

ELECTRONIC EVIDENCE GUIDE

A BASIC GUIDE FOR POLICE OFFICERS,
PROSECUTORS AND JUDGES

RESTRICTED



www.coe.int/cybercrime

Version 2.0

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

ELECTRONIC EVIDENCE GUIDE

A BASIC GUIDE FOR POLICE OFFICERS, PROSECUTORS AND JUDGES

Version 2.0

Cybercrime Division
Directorate General of Human Rights and Rule of Law
Strasbourg, France
15 December 2014

This guide is the result of the following projects:

CyberCrime@IPA

GLACY - Global Action on Cybercrime

Cybercrime@EAP

Cybercrime@Octopus

Acknowledgement

The first edition of this Guide was published in March 2013 under the CyberCrime@IPA joint project of the Council of Europe and the European Union on cooperation against cybercrime in South-eastern Europe. Work on this document was coordinated by Nigel Jones (United Kingdom). Valuable inputs were received from cybercrime experts from CyberCrime@IPA project countries and areas as well as a range of other international experts from Africa, Asia and Europe. Version 2.0 of the guide represents an update prepared by Victor Völzow (Germany) under the GLACY Project of the European Union and Council of Europe.

The authors are:

- Nigel Jones (United Kingdom)
- Esther George (United Kingdom)
- Fredesvinda Insa Mérida (Spain)
- Uwe Rasmussen (Denmark)
- Victor Völzow (Germany)

CONTACT

Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe, F-67075 Strasbourg Cedex
(France)

Tel +33 3 9021 4506
Fax +33 3 9021 5650
Email alexander.seger@coe.int

DISCLAIMER

The views expressed in this technical report do not necessarily reflect official positions of the Council of Europe, of the donors funding this project or of the Parties to the treaties referred to.

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 8 |
| 1.1 | The purpose of the Guide | 8 |
| 1.2 | Who is the Guide for? | 9 |
| 1.3 | How should the Guide be used? | 9 |
| 1.4 | Further tools | 10 |
| 1.5 | What is electronic evidence? | 11 |
| 1.5.1 | Characteristics of electronic evidence | 11 |
| 1.5.2 | Admissibility of electronic evidence | 13 |
| 1.6 | Why is it important? | 13 |
| 1.7 | Principles of electronic evidence | 14 |
| 1.7.1 | Principle 1 – Data Integrity | 14 |
| 1.7.2 | Principle 2 – Audit Trail | 14 |
| 1.7.3 | Principle 3 – Specialist Support | 14 |
| 1.7.4 | Principle 4 – Appropriate Training | 15 |
| 1.7.5 | Principle 5 - Legality | 15 |
| 2 | Sources of evidence | 16 |
| 2.1.1 | Storage devices | 17 |
| 2.1.2 | Tablet devices | 22 |
| 2.1.3 | Mobile telephones | 23 |
| 2.1.4 | Photo and video recording | 23 |
| 2.1.5 | Portable media players | 27 |
| 2.1.6 | Video games consoles | 27 |
| 2.1.7 | Potential evidence on these devices | 28 |
| 2.2 | Computer networks | 28 |
| 2.3 | Selecting which evidence to capture | 34 |
| 2.4 | What authorisation do you need? | 34 |
| 2.5 | Preparation and planning | 34 |
| 2.6 | Digital forensics specialists | 35 |
| 3 | Search and seizure | 38 |
| 3.1 | Who and what to take to the scene | 38 |
| 3.2 | Securing the scene | 41 |
| 3.3 | Documenting the Scene | 42 |
| 3.4 | Search and seizure in 'dead box' scenarios | 47 |
| 3.4.1 | Packaging, transport and storage | 47 |
| 3.4.2 | Computer system & electronic device collection | 49 |
| 3.4.3 | Checking the power status (on/off) | 51 |
| 3.4.4 | Computer network collection | 53 |
| 3.4.5 | Additional components | 54 |
| 3.4.6 | Digital storage media | 55 |
| 3.4.7 | Other electronic devices | 55 |
| 3.4.8 | General seizure instructions for electronic devices | 56 |
| 3.4.9 | Personal digital assistants (handheld computers) | 57 |
| 3.4.10 | Telephones, Smartphones and Tablet Devices | 58 |
| 3.4.11 | Smart cards and magnetic stripe cards | 59 |
| 3.4.12 | Answering machines | 60 |
| 3.4.13 | Digital cameras | 61 |

| | | |
|----------|---|------------|
| 3.4.14 | Facsimile (fax) machines | 61 |
| 3.4.15 | Printers | 62 |
| 3.4.16 | Scanners | 62 |
| 3.4.17 | Photocopiers (copy machines) | 62 |
| 3.4.18 | Multifunctional machines | 63 |
| 3.4.19 | Pagers | 63 |
| 3.4.20 | GPS devices and other satellite positioning devices | 63 |
| 3.4.21 | Wearables (e.g. smart watches, activity trackers) | 63 |
| 3.4.22 | Magnetic stripe readers | 64 |
| 3.5 | Search and seizure in live data scenarios | 64 |
| 3.5.1 | Volatile data | 65 |
| 3.5.2 | Physical access | 67 |
| 3.5.3 | Remote access | 79 |
| 3.5.4 | Administrator permission | 89 |
| 4 | Capturing evidence from the Internet | 91 |
| | A Web Service Taxonomy | 92 |
| 4.1 | Websites as a "Mashup" of Evidence | 92 |
| 4.2 | Virtual vs Physical location | 93 |
| 4.2.1 | IP (Internet Protocol) Address | 94 |
| 4.2.2 | Dynamic IP addresses vs static IP addresses | 95 |
| 4.2.3 | IPv6 | 96 |
| 4.2.4 | DNS for Domain Name System | 98 |
| 4.2.5 | Uniform Resource Identifier (URI) | 99 |
| 4.2.6 | IP & DNS records in your online investigations | 100 |
| 4.3 | Online sources of information | 101 |
| 4.3.1 | Websites | 103 |
| 4.3.2 | Social networking sites | 105 |
| 4.3.3 | Blogging and micro-blogging sites | 106 |
| 4.3.4 | Webmail services | 107 |
| 4.3.5 | URL-shorteners | 107 |
| 4.3.6 | Ad-networks | 107 |
| 4.3.7 | Content storage networks | 108 |
| 4.3.8 | File sharing Peer-to-Peer (P2P) networks | 108 |
| 4.3.9 | The 'Deep Web' and the 'Darknet' | 110 |
| 4.4 | Data v evidence | 113 |
| 4.4.1 | What do you want that data for? | 113 |
| 4.4.2 | Use the source | 114 |
| 4.4.3 | Classic approaches | 115 |
| 4.4.4 | High-tech classic approach | 116 |
| 4.4.5 | Taking it a step further | 119 |
| 4.4.6 | Time stamping | 120 |
| 4.4.7 | Creating a viewable duplicate of a website | 120 |
| 4.4.8 | Notary | 121 |
| 4.4.9 | Limitations on existing approaches | 121 |
| 4.4.10 | Adding it all up | 121 |
| 4.5 | Covert online investigations | 122 |
| 4.5.1 | Technical risks | 123 |
| 5 | Data held by third parties | 124 |
| 5.1 | Independent data holders | 124 |

| | | |
|----------|--|------------|
| 5.1.1 | Fostering cooperation between independent data holders and law enforcement | 125 |
| 5.1.2 | Data preservation | 126 |
| 5.2 | Receiving reports about cybercrime | 127 |
| 5.2.1 | Collating several victim reports to build a case | 129 |
| 5.2.2 | Witnesses to cybercrime | 129 |
| 6 | Analysing evidence | 131 |
| 6.1 | Digital Forensics | 131 |
| 6.2 | Digital Forensics process model | 133 |
| 6.3 | Common principles when analysing electronic evidence | 134 |
| 6.3.1 | Data integrity | 134 |
| 6.3.2 | Audit trail | 135 |
| 6.3.3 | Specialist support | 136 |
| 6.3.4 | Appropriate training | 136 |
| 6.3.5 | Legality | 138 |
| 6.4 | Digital traces | 138 |
| 6.5 | Types of forensic analysis | 139 |
| 6.5.1 | File system analysis | 139 |
| 6.5.2 | File recovery | 140 |
| 6.5.3 | Searching the file system | 141 |
| 6.5.4 | Dealing with file encryption | 142 |
| 6.5.5 | Document forensic analysis | 143 |
| 6.5.6 | Steganography | 144 |
| 6.5.7 | Log file forensic analysis | 144 |
| 6.5.8 | Network forensic analysis | 145 |
| 6.5.9 | IP addresses and the DNS | 145 |
| 6.6 | Connected services on seized devices | 148 |
| 7 | Preparation and presentation of the evidence | 149 |
| 7.1 | Use of electronic evidence in court proceedings | 149 |
| 7.2 | Evidence in criminal proceedings | 149 |
| 7.2.1 | Admissibility | 149 |
| 7.2.2 | Authenticity | 149 |
| 7.2.3 | Convincing | 150 |
| 7.3 | Explanation of the principles | 150 |
| 7.4 | Disclosure | 151 |
| 7.5 | Unused material | 151 |
| 7.6 | Care of victims and witnesses | 152 |
| 7.7 | Court presentation | 152 |
| 8 | Jurisdiction | 154 |
| 8.1 | The international dimension of cybercrime | 154 |
| 8.2 | International justice cooperation networks | 154 |
| 8.3 | Mutual Legal Assistance | 154 |
| 8.4 | Cross-border cases | 155 |
| 9 | Role specific considerations | 155 |
| 9.1 | LEAs, possibly all investigative authorities | 156 |
| 9.2 | Prosecutors | 156 |
| 9.2.1 | Management of investigations | 156 |

| | | |
|-----------|--|------------|
| 9.2.2 | Management of prosecutions | 156 |
| 9.2.3 | Disclosure to the defence | 157 |
| 9.2.4 | Admissibility of evidence | 157 |
| 9.3 | Judges | 158 |
| 9.3.1 | The investigative role of the judge | 158 |
| 9.3.2 | The role of the expert | 159 |
| 9.3.3 | Dealing with unused material | 159 |
| 9.3.4 | Jurisdiction | 159 |
| 9.4 | Non-criminal proceedings | 159 |
| 9.4.1 | Preparing the seizure of data | 160 |
| 9.4.2 | The data capturing process | 160 |
| 9.4.3 | Chain of custody of the seized data | 161 |
| 9.4.4 | Forensics analysis | 162 |
| 10 | Cases | 163 |
| 10.1 | Criminal cases | 163 |
| 10.1.1 | Admissibility of computer printout as evidence | 163 |
| 10.1.2 | Unauthorised modification of a computer | 164 |
| 10.1.3 | Employee obtained unauthorised access to a computer | 164 |
| 10.1.4 | Hacking computer systems | 166 |
| 10.1.5 | Possessing indecent photographs of children | 166 |
| 10.1.6 | Extraterritorial data seizure | 167 |
| 10.1.7 | Identity theft, password hijacking, social networks | 168 |
| 10.1.8 | Hacking computer systems (Qurban Ali) | 170 |
| 10.2 | Civil cases | 171 |
| 10.2.1 | Legal risk mitigation on a massive layoffs at pharmaceutical sector | 171 |
| 10.2.2 | Data forensics pursuant to a data breach | 171 |
| 10.2.3 | Investigations of a boycott of an online sales system | 172 |
| 10.2.4 | Electronic discovery for the legal risk analysis in a company buy out | 172 |
| 10.2.5 | Proving the authenticity of an email | 173 |
| 11 | Glossary | 174 |
| 12 | Further information | 195 |
| 12.1 | Books | 195 |
| 12.1.1 | Electronic evidence | 195 |
| 12.1.2 | United States of America | 195 |
| 12.1.3 | United Kingdom | 195 |
| 12.2 | Journals | 196 |
| 12.3 | About the authors | 196 |
| 13 | Appendices | 199 |
| | Incl. flowcharts and templates: forms, records, labels, questionnaires | |

1 Introduction

The Electronic Evidence Guide was originally prepared under the joint regional project Cybercrime@IPA of the European Union and the Council of Europe (CoE) on cooperation against cybercrime under the Instrument of Pre-Accession (IPA).

Under the CyberCrime@IPA Project, as well as during the Council of Europe's Octopus Conferences, counterparts have consistently identified the need for authoritative guidance and good practice on the handling of electronic evidence. The Electronic Evidence Guide was prepared in response to that need.

The concept of the Electronic Evidence Guide was developed through several workshops under the CyberCrime@IPA project and at an Octopus Conference in the course of 2012.

The first edition was published on 18th March 2013 and has since become a popular resource for law enforcement and judicial bodies in a variety of different countries. Some countries have even translated the guide into their domestic languages.

The changes to this, the second edition of the Guide are based on the feedback provided by readers. They include a completely revised section on analysing electronic evidence and digital forensics.

1.1 The purpose of the Guide

The purpose of the Guide is to provide support and guidance to criminal justice professionals on how to identify and handle electronic evidence in such ways 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 dealing with electronic evidence and offers advice on how to deal with them. Readers of this document should check if such advice already exists at the national level.

This Guide and the information contained in it are considered valid until 31 December 2016. 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 has been prepared for use by countries that are in the process of developing and establishing their own rules and protocols for dealing with electronic evidence. Most existing guides have been created for the law enforcement community, but this guide is for a wider audience including judges, prosecutors and others involved in the justice system who may need to know about electronic evidence (such as private sector investigators and defence attorneys). Although primarily a basic level document, some sections of the Guide are more detailed and provide practical advice that may be of interest to specialists.

1.3 How should the Guide be used?

This Guide should be seen as a template document that can be adapted and customized by countries according to their national legislation, practice and procedure. The overarching principles it describes are in accordance with generally accepted good practice for dealing with electronic evidence.

Readers should ensure that they are fully conversant with the laws of their own countries related to electronic evidence and its admissibility. 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.

The text is broken down into sections that follow every stage in an investigation chronologically from the initial identification of sources of potential evidence, to the search and seizure of data from the Internet, through to the analysis, preparation and reporting of evidence and its presentation in court. There then follow sections of particular interest to specific professional functions including law enforcement, prosecutors, judges, private sector investigators, attorneys, and other legal professionals.

A number of useful tools to assist the investigator appended to this document:

- Appendix A – Search and Seizure Flow Chart
- Appendix B – Live Forensics Flow Chart
- Appendix C – Private Sector Preparation Flow Chart
- Appendix D – Private Sector Search and Seizure Flow Chart
- Appendix E – Acquisition of Digital Evidence Flow Chart
- Appendix F – Chain of Custody Record
- Appendix G – Custodian Questionnaire
- Appendix H – Template Exhibit Labels
- Appendix I - Image Acquisition Worksheet

These may be used and adapted as required.

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 indicates specialised knowledge

Whenever readers are unsure what course of action to take, they should refer back to the overarching principles in section 1.7 for guidance. Readers should always seek specialist assistance when the situation confronting them goes beyond the scope of the Guide or of their training.

1.4 Further tools

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

- The Budapest Convention on Cybercrime¹ Parties to the Convention are 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);
 - Transborder access to data without the need for mutual assistance (Article 32).
- The proposal for law enforcement training strategies prepared under CyberCrime@IPA;
- The judicial training concept prepared by the Council of Europe and the training materials developed under CyberCrime@IPA;
- The typology study on criminal money flows on the internet prepared by MONEYVAL and the Global Project on Cybercrime of the Council of Europe;

¹ 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 The need for rule of law safeguards (Article 15 Budapest Convention) as documented under CyberCrime@IPA;
- The Octopus Cybercrime Community, a forum linking up the many hundred public and private sector cybercrime experts from all over the world.

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

1.5 What is electronic evidence?



All criminal proceedings depend on evidence to decide the guilt or innocence of an accused or to decide the merits of a case in civil proceedings. Traditionally and historically, evidence has been in a physical form (such as documents or photographs etc.) or the oral testimony of witnesses.

Electronic evidence is derived from electronic devices such as computers and their peripheral apparatus, computer networks, mobile telephones, digital cameras and other portable equipment (including data storage devices), as well as from the Internet. The information it contains does not possess an independent physical form.

However, in many ways, electronic evidence is no different from traditional evidence in that the party introducing it into legal proceedings must be able to demonstrate that it reflects the same set of circumstances and factual information as it did at the time of the offence. In other words, they must be able to show that no changes, deletions, additions or other alterations have (or might have) taken place.

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 be handled in a special way to ensure the integrity of the evidence it offers.

Given its special characteristics electronic evidence could be defined as:

Any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings.

1.5.1 Characteristics of electronic evidence

Electronic evidence shares most properties with traditional forms of evidence, but also possesses some unique characteristics:

It 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.

It 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.

It 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").

It 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.

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.

1.5.2 Admissibility of electronic evidence

Although the details may differ from jurisdiction to jurisdiction, 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).

1.6 Why is it important?



Criminals are predators and the mass use of digital media and Internet has provided new opportunities for them to perpetrate their crimes. They have evolved new strategies for traditional offences by exploiting these new channels of communication and novel categories of crime have evolved. Consequently it is imperative for all those involved in the legal system to be familiar with the different forms of electronic evidence and to know how to deal with them.

Almost any crime these days is likely to involve an electronic device that has a memory or some form of programming. Even where the crime itself has not used such a device, the actions of the perpetrator may well have been captured or recorded on a CCTV camera or through a Global Positioning System (GPS) device on a phone or in a vehicle. The securing of electronic evidence through digital forensic examination and investigation has become the primary tool in bringing criminals to justice.

The development of the Internet and its applications has led to evidence being found not only on personal computer devices, but also on websites, social networks, in emails and chat rooms. The development of “cloud” computing (where applications and data are stored remotely across national boundaries in non-specific locations) means that it is more important than ever for potential electronic evidence to be processed according to tried and trusted principles and practice.

1.7 Principles of electronic evidence

The following principles are provided to guide readers when dealing with electronic evidence. Much has changed in the world of technology in the decade since these principles were formulated so they have been amended to meet the challenges of today's operational environment.

Each country should take into account its own legal documents and regulations when interpreting the measures proposed in this document. This is such an important point, it will be repeated often!

1.7.1 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.

- Electronic devices and data must not be changed, either in relation to hardware or software. The person in charge of a crime scene or for collecting the evidence is responsible for maintaining the integrity of the material recovered and for ensuring the forensic chain of custody. Subsequent custodians of the devices and/or data must assume that responsibility.
- When data is accessed on a "live" computer system this must be done in the manner that causes the least impact on the data and by a person qualified to do so. Principles 2 to 5 apply if this course of action is found to be necessary.

1.7.2 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.

- It is imperative to record accurately all activity at the scene to enable a third party to reconstruct the first responder's actions if necessary. All activity relating to the search, seizure, access, storage or transfer of electronic evidence must be fully documented, preserved and available for review.
- Any subsequent action related to the processing and examination of electronic evidence should also be amenable to audit in the same way.

1.7.3 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.

- For investigations involving search and seizure of electronic evidence it is always desirable to involve electronic evidence specialists wherever possible. All such specialists, either

from within the organisation or as external contractors, should have the appropriate and objectively verifiable knowledge to deal with electronic evidence properly. Such a specialist should have:

- Sufficient specialist expertise and experience in the field;
- Sufficient knowledge and skills in conducting investigations;
- Sufficient knowledge of the matter at hand;
- Sufficient legal knowledge;
- Appropriate communication skills (for both oral and written explanations);
- Sufficient and appropriate language skills;
- Appropriate authorisation and/or legal justification for his/her involvement in the activity.

1.7.4 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.

- For those circumstances where only a first responder is available to collect electronic evidence and/or access original data held on an electronic device or digital storage media, s/he must be trained to do so according to legally sanctioned procedures and to be able to explain and justify the relevance and implications of his/her actions.

1.7.5 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.



2 Sources of evidence

Investigators should always consider the possibility that any electronic devices or equipment encountered during the investigation can potentially yield evidence. The presence of such items may not be obvious or in plain sight of the investigator.

The variation in devices containing electronic evidence increases almost daily. The following list of potential sources of evidence is not exhaustive, but contains examples of those most commonly found.

A computer system will be made up of a number of different components that are likely to include:

- An external case housing **circuit boards, microprocessors**, hard drives, **memory**, and connections for other devices;
- A monitor or other display device;
- A keyboard;
- A mouse;
- Externally connected drives;
- Peripheral devices;
- Software.

Computer systems can come in many different forms including desktops, laptops, tower computers, rack-mounted systems, minicomputers, and, mainframe computers. Other devices will commonly connect to these systems including printers, scanners, routers, external hard drives and other storage devices as well as docking stations (that allow multiple connections to be made).

Note the definition of "computer system" and "computer data" used in the Budapest Convention on Cybercrime:

Article 1 – Definitions

For the purposes of this Convention:

- a. "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;*
- b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;*

This definition covers tablets, smart phones and other devices described below.



Desktop / Tower



Laptop



Mainframe

Images of computer systems²



2.1.1 Storage devices

Storage devices also come in many shapes and sizes and vary in the manner in which they store and keep data. The following section provides details of some of these devices and their capabilities.

2.1.1.1 Hard disk drives and solid state disks

Hard disk drives (HDD) are the main storage devices within computer systems. They consist of a circuit board, data and power connections. Inside the hard disk drive there are magnetically-charged ceramic, metal or glass platters (i.e. plates or disks) that rotate at high speed. An arm travels across the surface of the platter like in old fashioned record players and 'writes' the data to the disk. It is not unusual to discover separate hard disk drives during a search that are not connected to or installed in a computer system. Usually a hard disk drive in desk top computers will measure 3.5 inches (8.9 cm) across and 2.5 inches (6.35 cm) across laptops.

Solid state disks (SSD) have a different structure to hard disks and are becoming more popular. Instead of storing data on platters, solid state disks store data using microchips and have no moving parts. As such they are less likely to be damaged when dropped or knocked and offer faster access to the data.

² Image Source:

- [1] computershopper.com/var/ezwebin_site/storage/images/desktops/product-profile/superior-699-pc-model-6173/38202-1-eng-US/superior-699-pc-model-61731_product_review_thumb.jpg
- [2] expresscomputing.info/siteimages/laptop1.jpg
- [3] prepare.icttrends.com/images/2012/06/mainframe-computer.jpg



Computer Hard Disk



Computer Hard Disk Interior



Solid State Disk

Photographs of different types of internal storage³

2.1.1.2 Removable media

Compact Disk (CD), Digital Video Disk⁴ (DVD) and Blu-ray Disks (BD) are typically used for storage of large video or audio files. They may, however, also hold large quantities of other kinds of data that can be of evidential value. Although they look very similar, the storage capacities vary greatly.



Compact Disk (CD)



Digital Video Disk (DVD)



Blu-ray Disk (BD)

Photographs of different types of removable optical storage⁵

³ Image Source

[8] [upload.wikimedia.org/wikipedia/commons/e/e6/Hard_disk_Western_Digital_WD1000_1_\(dark1\).jpg](https://upload.wikimedia.org/wikipedia/commons/e/e6/Hard_disk_Western_Digital_WD1000_1_(dark1).jpg)

[9] lh3.ggpht.com/_Kkg7XHt7mJA/TLHZioMTiBI/AAAAAAAAAow/FN4THI-QzNQ/s800/Storage-Hard-disk.jpg

[10] blog.mirchimart.com/wp-content/uploads/2012/06/1.jpg

⁴ Also called Digital Versatile Disk

⁵ Image Source:

[11] jetmedia.co.uk/cdmada80.jpg

[12] 3.bp.blogspot.com/_RzAQQvY1zGw/TPHH3KzB3rI/AAAAAAAAAWg/ctwmTTftGew/s1600/icon-DVD.png

[13] 4.bp.blogspot.com/_N3kyjbXGs0I/S3OK_6rfzLI/AAAAAAAAADY/S76APQ9wVPE/s320/sony-blu-ray-disc-format-us.jpg

2.1.1.3 Memory cards

Memory cards, also known as flash cards, are also devices for storing digital information. They are used in devices such as digital cameras, mobile phones, laptop computers, music players and games consoles. They retain data without power and can store huge amounts of data while being easy to conceal.



Secure Digital Card (SD)



Micro SD Card and Adaptor



Compact Flash Card (CF)

Types of memory cards⁶

2.1.1.4 USB data storage devices

Universal Serial Bus (USB) is the name given to a set of rules or 'protocol' used for communication, connection and power supply for devices that connected to computers. The range of devices using this protocol has grown enormously since it was introduced in the 1990s. Some examples of the more usual USB devices are shown below.



⁶ Image Source

[14] memorycardsforcameras.org/wp-content/uploads/memory-cards-for-cameras-sd.sdhc_.sdxc_.jpg

[15] portal.lynxmobility.com/images/Accessories/microSD_2GB_02.jpg

[16] heise.de/imgs/18/4/8/6/8/6/8/SP128GBCFC400V10.jpg-777a6b1cc6a3f2fc.jpeg

Restricted

Images of common USB devices⁷

However, not all devices are what they seem. Here are just a few of the ways in which USB storage devices can be disguised. It is important for anyone considering electronic evidence to be vigilant and aware of the possible novelty.



Images of unusual USB devices⁸

2.1.1.5 Data storage tape disks

Data stored on tape is more likely to be encountered in a business rather than a domestic setting. The most common type used now is the 'Linear Tape-Open' (LTO) technology developed in the

⁷ Image Source

[17] img.ehowcdn.com/article-new/ehow/images/a07/ph/ee/clean-usb-ports-laptop-computers-800x800.jpg

[18] s0.static.mymemory.co.uk/images/product_shots/large_16631_1297420753.jpg

[19] 1.bp.blogspot.com/_o801UUtSFEI/TPuVqLOz3qI/AAAAAAAAACM/-XvKYezjX-E/s1600/2edsfas.jpg

[20] merchadismania.co.uk/productimages/fullsize/XH21-Metal--USB-Flash-Drive-With-Clear-Ends-STR-CAP-OFF/Personalised-Printed--Metal--USB-Flash-Drive-With-Clear-Ends.jpg

[21] media.tecca.com/2010/11/03/630-usb-lexar-630w.jpg

[22] 1.pcmag.com/media/images/310963-verbatim-tuff-n-tiny-usb-drive.jpg?thumb=y

[23] 3.bp.blogspot.com/_zS2JDRBdNzk/THd83p8BZ8I/AAAAAAAAACKc/sgBaS8XLbbg/s1600/4mm+pico-usb-300x261.jpg

⁸ Image Source:

[24] ohgizmo.com/images/imation_4gb_micro_hard_drive.jpg

[25] media.gdgt.com/img/product/11/8ov/oakley-thump-i3m-800.jpg

[26] technabob.com/blog/wp-content/uploads/2006/09/imation_usb_wristbands.jpg

[27] pixelbeat.org/systems/laks/usb-watch-drive-uf1s.jpg

[28] cookingfor.us/catalog/images/Victorinox%20SwissMemory%20128%20MB%20USB%20Storage.jpg

[29] geeky-gadgets.com/wp-content/uploads/2008/01/domino_thumb_drive.jpg

1990s as an open-format⁹ standard. Tapes are normally used for backup and therefore may be useful in cases where an historical analysis is required or where the original computer is not available.



Images of data storage tape devices¹⁰

2.1.1.6 Peripheral devices

Peripherals are devices that are not an integral part of the computer, but connect to it to increase its range of functions. Examples of peripheral devices are: scanners; printers; tape drives; webcams; loudspeakers; microphones; calculators; fax machines; answering machines; and card readers. Many of these devices have their own data storage capacity and may be relevant to particular types of investigation (for example, the presence of a card reader may be relevant in a credit card cloning investigation). Here are some images of just a few of the types of peripherals that might be encountered:

⁹"open-format" means that users have access to multiple compatible sources of storage media. Source: <http://searchstorage.techtarget.com/definition/Linear-Tape-Open>

¹⁰ Image Source

[30] 2.imimg.com/data2/LO/TG/MY-3658176/fujifilm-linear-tape-open-lto5-250x250.jpg

[31] global.tdk.com/csr/ecolove/img/eco_med03.jpg

[32] 3000newswire.blogs.com/.a/6a00d83452e85869e20134809149c4970c-320wi

Images of Peripheral Devices¹¹

2.1.2 Tablet devices

A tablet computer is a device that is operated by touching the screen rather than using a keyboard or mouse. It is normally larger than a mobile phone or **Personal Digital Assistant (PDA)**. Tablets may store data in the form of a hard disk or flash memory, but , increasingly, user-generated data are stored in the cloud. Tablets have become very popular in recent years. They run their own operating systems and are often connected to the Internet via a Wireless Local Area Network (**WLAN**), Third Generation Mobile Telecommunications (**3G**) (now slowly becoming Fourth Generation or 4G) or Long Term Evolution (**LTE**)¹² networks.



¹¹ Image Source:

[33] softwaretutor.files.wordpress.com/2010/04/fax.jpg

[34] superwarehouse.com/images/products/hpQ3851AA2L.jpg

[35] static.bhphoto.com/images/images345x345/504534.jpg

[36] carolinabarcode.com/images/ArticleImages/RunMyStore/CreditCardReader.jpg

[37] xactcommunication.com/itempics/48_xlarge.jpg

[38] labelprinter.org.uk/wp-content/uploads/2009/03/dymo-labelwriter-400.jpg

¹² A kind of wireless 4G broadband network.



2.1.3 Mobile telephones

The time when a telephone was used simply for making and receiving calls is long past. Nowadays, mobile or 'cell' phones are used for many other tasks: sending and receiving text or multimedia messages; accessing the Internet and email; playing games; listening to music; and, taking photographs. Many modern mobile phones are really computers, although their connectivity requires them to be handled in a somewhat different manner. It is important to note that different phones have different capabilities and the way they connect (their 'connection interfaces') can require specialist equipment in order to capture evidence.



Images of Mobile Phones¹⁴



2.1.4 Photo and video recording

2.1.4.1 Digital cameras

Digital cameras take still or video photographs in the form of thousands of small dots of light called pixels. Most modern digital cameras can also record sound as well as pictures. Digital cameras can store thousands of images on small "memory cards" (see 2.1.1.3 above) or on the camera itself. For investigations involving photographs it may be possible to prove which camera took a specific photograph because certain metadata are often stored with the image¹⁵. Examples

¹³ Image Source:

[4] find-cool.net/wp-content/uploads/2012/09/Windows-8-Tablet-PC.jpg
 [5] vedainformatics.com/blogs/wp-content/uploads/2010/01/apple-ipad-tablet-pc.png
 [6] compartablets.co.uk/wp-content/uploads/2011/09/galaxy-tab-8.9.jpg
 [7] cache.gizmodo.com/assets/images/4/2007/12/delltablet.jpg

¹⁴ Image Source:

[39] lh5.googleusercontent.com/-RyY55_39t7o/T25v61iDZnI/AAAAAAAAADc/fw-gqm7QTR4/s0/phone.png
 [40] resources.envirofone.com/shared/media/images/news/articles/mobile_phone_recycling_could_be_boosted_by_iphone_4_deals_2059_19917932_0_0_7063723_300.jpg
 [41] fonesunlock.co.uk/images/P/Unlock_Blackberry_Storm_9500-01.jpg

¹⁵ For instance, using the Exchangeable Image Format (EXIF) standard.

of common types of digital camera are shown below, along with some cameras disguised as other devices.



Images of Digital Cameras¹⁶

2.1.4.2 Digital video cameras

A digital video camera also often stores its images on removable media, but can also record to a hard disk contained within the camera itself. In some cases these cameras look very similar to digital still cameras (bearing in mind that digital still cameras can usually also take video and a digital video camera can take still photographs). Some examples of video cameras are shown below.

¹⁶ Image Source

[42] [transcribe.co.uk/UserFiles/digital_camera_picture\(3\).jpg](http://transcribe.co.uk/UserFiles/digital_camera_picture(3).jpg)

[43] brain.pan.e-merchant.com/6/0/12305806/l_12305806.jpg

[44] cdn0.mos.techradar.futurecdn.net///classifications/gadgets/digital-cameras/images/canoneos1dmarkiiiangled-380-75.jpg

[45] bridgetoworld.com/images/l/201009/12834167310.jpg

[46] cdn2.bigcommerce.com/server1700/0a80b/products/60/images/291/Digital_spy_alarm_clock_3__74576.1282420400.1280.1280.gif

[47] wholesales-shopping.com/wp-content/uploads/2011/09/17.jpg

[48] images.madeinchina.com/p/520/3593520_0/On-sale-4GB-Spy-Camera-Watch-Video-Recorder-Mini_3593520_0.bak.jpg

Images of Digital Video Cameras¹⁷

2.1.4.3 Video recorders

Video recorders are usually found in the domestic setting and used to record TV programmes or other locally based activity. They are also used to playback prerecorded films, music and other data. The Video Home System (VHS) recorders were prominent from the 1970s until overtaken by digital versions. VHS was recorded and played back using large cassette tapes that may still be found under some circumstances. Certain kinds of optical discs were also produced, but did not become mainstream. Instead, the Digital Versatile Disk (DVD) became the standard. DVDs and their later evolution, Blu-ray discs, are still used today, but some modern video recorders store their recording on built-in hard drives. Where CCTV is present, images the cameras may be recorded in any of these formats.

Video Recording Formats¹⁸

2.1.4.4 Digital audio recorders

Digital audio recorders are small handheld devices used to record sound on a memory chip to play the recording back. They come in various capacities in terms of maximum recording time and quality. Some recorders have a USB capability that allows the recordings to be uploaded to a

¹⁷ Image Source:

[49] alpha.akihabaranews.com/wp-content/uploads/images/6/66/16666//1.jpg

[50] sils.unc.edu/sites/default/files/it/CanonGL2.jpg

[51] pembrokeshirefilmfestival.files.wordpress.com/2012/12/panasonic-hcv100.png

¹⁸ Image Source

[52] blogcdn.com/www.switched.com/media/2008/07/41113_4048.jpg

[53] totalsecuritywarehouse.com/images/catalog/category50.jpg

computer and may have associated speech recognition software allowing for the creation of automatic draft transcripts.



Images of Digital Audio Recorders¹⁹

2.1.4.5 CCTV cameras

Closed Circuit Television (CCTV) cameras are used by companies, governments and private individuals. CCTV cameras may be deployed continually or to monitor a particular activity. In some countries they have become a tool for surveillance in public places monitoring traffic or crowd flows, detecting public disorder or criminal activity. Some CCTV cameras record images onto storage media while others are only used for live monitoring. They can also be motion activated and operate in low light or under infrared conditions. They should always be considered as a potential source of electronic evidence wherever they are at or near a crime scene. Some examples of how CCTV cameras may look like are shown below.



Images of CCTV Cameras²⁰

¹⁹ Image source

[54] [i.ebayimg.com/t/8GB-Digital-Voice-Recorder-650Hr-Dictaphone-MP3-Player-w-U-Disk-Iron-gray-US-/00/s/MTAwMFgxMDAw/\\$\(KGrHqNHJEgFDTE6vHM3BQ7nlu,LGg~~60_35.JPG](http://i.ebayimg.com/t/8GB-Digital-Voice-Recorder-650Hr-Dictaphone-MP3-Player-w-U-Disk-Iron-gray-US-/00/s/MTAwMFgxMDAw/$(KGrHqNHJEgFDTE6vHM3BQ7nlu,LGg~~60_35.JPG)

[55] c773974.r74.cf2.rackcdn.com/0330731_617464.jpg

[56] fl12.shopmania.org/files/p/bg/t/472/m-audio-micro-track-ii~3964472.jpg

²⁰ Image Source

[57] newlonsoft.com/images/CCTV%20images/CCTV-Camera_2.jpg

[58] videos.cctvcamerapros.com/images/ptz-cameras/infrared-ptz-camera.jpg



2.1.5 Portable media players

Portable media players such as iPods or **MP3**²¹ players store and play digital media. These can include music and other audio, photographs or video as well as documents and other types of file. Once again, these devices have many similarities with computers. Some of these devices use removable flash storage while others have large hard disks capable of storing many thousands of files. Some examples of portable media players are provided below.



Images of Portable Media Players²²



2.1.6 Video games consoles

Video games consoles have existed since the early 1970s, but have developed greatly over the years. These devices use onboard or removable storage that allows the users not only to play games, but also to visit websites and to store and play videos, photos and music. For this reason, they should never be overlooked as sources of electronic evidence even if they seem innocuous at first sight. Major console producers include Sony, Nintendo and Microsoft and these companies currently hold the majority of the market for consoles and games.

[59] icode.co.uk/icatcher/cctvshop//images/Genie-VRD43-Dome-CCTV-Camera.jpg

[60] goldlinesecuritysystems.com/wp-content/uploads/2011/07/balajicctv_gif.jpg

²¹ 'Moving Picture Expert Group Audio Layer'³

²² Image source:

[61] newsongs2013.net/mp3-player-2010-images/best-mp3-player-2010-apple-ipod-touch.jpg

[62] butzgaskins.com/wp-content/uploads/2012/04/iPods-MP3-Players1.jpg

[63] geekalerts.com/u/cross-mp3-player.jpg

[64] images.highspeedbackbone.net/skuimages/large/Creative-Labs-Zen-Stone-1Mai.jpg

[65] ecodigital.co.uk/estore/images/sandisk-sansa-fuze.jpg



Images of Video Games Consoles²³

2.1.7 Potential evidence on these devices

Computer hardware and software, as well as the networks and systems to which a device is connected, can hold important data that have been created either automatically by the device itself or by the user. User-generated data would include documents, photos, image files, e-mails and their attachments, databases and financial information. Computer generated data would include the Internet browsing history, chat logs, event logs and data about other services, computers and networks to which the device has been connected.

Although this Guide is focused on electronic evidence, an investigator should never forget the important role played by traditional forensics (such as fingerprints, DNA and other traces) in linking a perpetrator to a device.

2.2 Computer networks

When two or more computers are linked by data cables or by wireless connectivity a 'network' is established. Computers in a network are able to share data and other resources between them and will often be connected to additional hardware components that extend their scope and the functions available. Computer networks can be limited such as those found in the home (e.g. where members of a family establish a network sharing an Internet modem) or as extensive as

²³ Image Source

[66] static1.thcdn.com/productimg/0/600/600/41/10179241-1279698066-442000.jpg

[67] gadgets.in.com/uploads/2011/01/sony_psp_2_codenamed_ngp_1.jpg

[68] galaxine.com/gifs/console.jpg

[69] ecx.images-amazon.com/images/I/41XM4A0DD6L._SL500_AA300_.jpg

[70] game-consoles.org/wp-content/uploads/2010/11/nintendo-3ds-video-game-console.jpg

[71] venturebeat.files.wordpress.com/2012/07/ouya-big.jpg?w=558&h=9999&crop=0

those used by major corporations or governments linking hundreds or even thousands of computers together.

Local Area Network (LAN) – A Local Area Network is a computer network covering a limited 'local' area like a home, an office, or a group of buildings (such as a school). Defining characteristic of LANs include the much higher speed they can achieve for transferring data between computers on the network, the limited geographic range and the fact that they do not need to rent lines from telecommunications companies.

Wide Area Network (WAN) – A Wide Area Network is a computer network that covers a broader area and will include any network that crosses metropolitan, regional, or national boundaries. The term implies a network that uses routers²⁴ and public communications links.

Contrast these with personal area networks (PANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area respectively. The largest and most well-known example of a WAN is the Internet.

Some of the terminology and devices that may be encountered when dealing with networks are:

Port – There are two types of ports: computer or hardware ports and network or internet ports. A computer port is a connection point between a computer and another device where information comes in and out (examples include USB, Ethernet and parallel ports by which devices can be attached). A network port is located in the software at the point where the software connects to internet or network services. A common analogy would be the doors and windows to a building. Each port is allocated a different number in computer programming. The number identifies the port's role and function and is set according to common standards.

Bandwidth – Like the diameter of a pipe, the size of the bandwidth indicates the maximum volume of information that can be carried along a phone line, cable line, satellite feed etc. The greater the bandwidth, the faster the potential speed for downloading and uploading data.

Media Access Control (MAC) address – The MAC address is a unique reference code assigned by the manufacturer to most network adaptors or network interface cards (NICs). MAC addresses function as an address on a network so that devices can be identified and the appropriate data can be forwarded to it.

Network Attached Storage (NAS) – A NAS is similar to an external hard-drive with the difference that it provides storage space for a whole network rather than just a single PC. NAS can often offer a lot more than just data storage. A NAS can be used as an automatic downloading server (e.g. uTorrent) and even as a small webserver. Many NAS devices house more than one hard drive and offer 'RAID' functionality.

²⁴ A router is a device that directs or 'routes' packets of data along a network or between networks.

Restricted

A so-called 'Redundant Array of Independent Disks' (**RAID**) is a way of arranging the storage of data (a data 'configuration') using multiple disk drives. Data is stored across the individual disks to ensure the best level of performance and/or data reliability. The operating system will access the RAID as though it were a single hard disk. The access is controlled and coordinated either by software or by a hardware RAID controller. Standalone RAIDs are commonly found in network configurations and may contain huge amounts of electronic evidence.



Images of NAS with RAID²⁵

Network Interface Controller (NIC) – is a circuit board or card installed in a computer that allows it to connect to a network.



Network Interface Controllers²⁶

²⁵ Image Source

[72] mpcomp.co.uk/5/graphics/import/105481.jpg

[73] resexcellence.com/wp-content/uploads/2013/01/5big_NAS_Pro_back_34_left.jpg

[74] gadgetreview.com/wp-content/uploads/2011/03/D-Link-DNS-321-Network-Attached-Storage-Enclosure.jpg

²⁶ Image source:

[75] ssos.com/nic.jpg

[76] ecx.images-amazon.com/images/I/41CAHWZY8LL._SL500_SS500_.jpg

[77] hexcs.com/assets/Uploads/TL-WN851N.jpg

Network Hub – A network hub or concentrator is a device for connecting multiple computers or Internet devices together so that they act together as a single part or 'segment' of a network. All computers in this segment are able to communicate with each other. A hub transmits any data received from the network and broadcasts it to all the other devices connected to it. For an investigator it can be hard to distinguish between hubs and switches because they basically look the same, but hubs have been largely replaced by network switches. The main difference is that a hub broadcasts all packets to all ports while a switch sends it only to the target port.



A Network Hub²⁷

Network Switch – A network switch is very similar to a hub. Switches are mainly used to connect groups of network devices to each other. In contrast to hubs they use internally stored databases to remember which MAC address has used which port of the switch. This allows a switch to route data packets to a specific device rather than to all devices.



A Network Switch²⁸

Router – A router is like a sorter in a post room. It is a device that identifies the destination to which a parcel or packet of data is addressed and then sends that packet on to the next point in the network nearest to where it needs to go. Although a router must be located at the gateway between networks it does not necessarily have to be linked to the Internet. Routers are commonly

²⁷ Image Source

[78] omnisecu.com/images/basic-networking/network-ethernet-hub.jpg

²⁸ Image source

[79] upload.wikimedia.org/wikipedia/commons/thumb/5/5f/Linksys48portswitch.jpg/220px-Linksys48portswitch.jpg

Restricted

used in the home to connect a house to a broadband connection. In such a situation it will often serve multiple purposes acting as a switch, access point, firewall, router and gateway all together.



Image of a Router²⁹

Server – A server is a computer or device that provides information and/or services to other computers on a network. Given the right software, any network-connected computer can be configured as a server. In most cases, a server will be a dedicated powerful computer designed to be “always available”. One computer server can run several services (e.g. web server, email server, file server, print server etc.). In business it often makes sense to run different services on different machines for reasons of security and to minimise the impact of any failure.



Images of Servers³⁰

Firewall – A firewall is a hardware device or software service that is used to increase the security of a network by preventing unauthorised access. For instance a firewall may be configured (set up) to detect and block any attempt to enter a network using multiple ports except for those ports that have been configured to allow incoming traffic. In homes, it is more common to find a software firewall, but in business settings the investigator is more likely to come across hardware firewalls.

²⁹ Image Source:

[80] trendnet.com/image/products/photo/TW100-BRV204_d3_2.jpg

³⁰ Image Source:

[81] x3me.info/wp-content/uploads/2011/10/server.jpg

[82] chost.pl/templates/whm/images/servers.png

[83] electroguardpaint.com/images/computerServerRoom.jpg

Restricted



Images of Hardware Firewalls³¹

Wireless Access Point – Wireless Access Points connect Wireless LAN devices to the rest to the network. In every WLAN infrastructure an access point is necessary whenever there are more than two devices. Modern routers can often function as an Access Point. A computer's NIC or even a mobile phone can also be configured to act as an Access Point.



Images of Access Points³²



While the network devices listed above can be standalone devices as shown in the photographs, it is very likely that a single device will serve multiple purposes. Routers in the home often function as a modem, firewall, switch and access point and a Networked Attached Storage (NAS) system may also serve as a Virtual Private Network, E-Mail and Webserver with switching as well as access point capabilities.

³¹ Image Source

[84] hacker10.com/wp-content/uploads/2011/04/Hardware-firewall-WatchGuard-XTM-2Series.jpg

[85] plug.4aero.com/Members/lmarzke/talks/plug_utm/screenshot1.png/image_preview

[86] cloverline-guardline.com/images/firewall.jpg

³² Image Source :

[87] solwise.co.uk/images/imageswifi/net-el-ecb3500-1.jpg

[88] zdtronic.com/images/WNDAP330.jpg

[89] amlabels.co.uk/files/images/products/5397.jpg

2.3 Selecting which evidence to capture

Selecting which device to seize and which evidence to collect or capture at a crime scene may be less easy than it first appears. The factors to consider are dealt with in more detail in the section on search and seizure. However, careful planning and advance preparation will help to avoid difficulties on site and here are some preliminary considerations to take into account.

2.4 What authorisation do you need?

The first consideration in planning for any coercive activity is to ascertain the nature and level of legal permission and/or authorisation required. That authorisation may take a number of forms. The simplest of these is to obtain consent from the person in charge of the equipment or the data to be captured. Such consent should always be obtained in writing and investigators should ensure that the person giving consent fully understands his or her rights as well as the implications and possible consequences. National legislation and guidelines must, of course, be satisfied.

Other levels of authorisation will be prescribed by law. They will depend on the nature of the investigation and whether those seeking authorisation are from a competent authority or working on a private civil matter. In most cases some kind of judicial orders or warrant will be required.

Absolutely no coercive activity involving the seizure of equipment or the capture of data should be undertaken without obtaining the requisite level of authorisation.

2.5 Preparation and planning

In planning an operation, certain questions need to be considered in advance.

Where is the data hosted (i.e. actually stored)?

It is not unusual for data to be hosted in a location other than where the equipment is present. If you arrive at a search without first considering this possibility you may find that further legal authorisation may be required (especially if the data is stored in a different jurisdiction) or additional technical skills or equipment may be necessary.

How sophisticated is the suspect?

It is wise to gather as much intelligence about the suspect as possible. A suspect skilled in computers may have implemented anti-forensic procedures to interfere with the seizure of equipment or the capture of data (for example they may have encrypted all their data storage devices or installed single key data wiping on their computers). If this is the case, it will be necessary to have countermeasures pre-prepared. The suspect may also have stored data in the cloud or using some other online resource so that no data will be found on their equipment.

Are there alternative or complementary sources of evidence?

Before embarking on any action that may involve direct contact with a suspect, seizure of their equipment or capture of his or her data, it should be considered during the planning phase whether there are other, more preferable, sources from which the same information might be obtained. For example, you might consider contacting other parties to an online transaction (such as an exchange of email), a third party such as an Internet Service Provider (ISP) or an online service provider. With greater use of the cloud, the same data may be recoverable from such a third party source.

It is a tactical decision whether to recover data from the suspect or from the alternative data holder. In some jurisdictions, third parties are required by law to notify their customer of any request for data access which may inconveniently alert a suspect and prompt him or her to conceal or destroy evidence. The investigator or prosecutor in charge will have to consider how the procedure for recovering data from third parties might impact on the effectiveness of an investigation (especially if the data are held in another jurisdiction). It will also be important to decide which source of evidence is best for the purposes of the investigation and most valuable for its eventual outcome.

2.6 Digital forensics specialists

Because digital forensics are so complex and so many different disciplines are involved, a digital forensics examiner tends to specialise in one area of electronic evidence. This means an investigator or prosecutor may sometimes need to retain the services of a digital specialist to assist with particular technical situations.

When selecting a specialist it can be helpful to see some form of formal accreditation awarded by a respected academic or professional body. Accreditation represents a certain level of educational attainment and provides an independent assessment of his or her credentials when his or her expertise is scrutinised in court. Similarly, a track record of publication in recognised peer reviewed journals, experience in previous cases and a professional reputation, all help to enhance that confidence.

The process of selection should not be haphazard, but active and structured from the start. Computer crime units may be able to offer additional advice on the criteria for selection, however, the following criteria may help to establish the value and reputation of an independent consulting witness.

Specialist skills

- a. Relevant academic and professional qualifications and accreditation;
- b. Specific skills that he or she possesses relevant to the case in hand;
- c. Involvement in any relevant specialist professional institutes or associations;
- d. An acknowledged reputation for his or her activity in the required area of expertise (for

instance does the specialist hold any awards for his or her work?).

Specialist experience

- a. The length and nature of experience of this type of work;
- b. Level and seniority attained;
- c. The number of court cases in which he or she has been involved;
- d. The type and complexity of cases in which the specialist was involved;
- e. Evidence to prove level and quality of experience (for instance participation as an invited speaker at reputable events; publications in respected peer review journals, official and honorary appointments relevant to the specialism).

Knowledge of investigation

An understanding of the nature and needs of an investigation in terms of confidentiality, relevance and the distinction between information, intelligence and evidence.

Contextual knowledge

An understanding of the difference between the approaches, language, philosophies, practices and roles of the police and the law, and the requisite technical knowledge of Information Technology as well as familiarity with the concept of probability in its broadest sense and knowing the difference between scientific and legal standards of proof.

Legal knowledge

An understanding of relevant aspects of the law in relation to:

- a. Statements;
- b. Continuity;
- c. Rules of evidence;
- d. Court procedures (including the differences in the roles of the defence and prosecution);
- e. A clear understanding of the roles and responsibilities of the expert witness.


Communication skills

The ability to express and explain in ordinary language:

- a. The nature of the specialism;
- b. The techniques and equipment used in the examination;
- c. The methods of interpretation used;
- d. The strengths and weaknesses of the evidence;
- e. Any possible alternative explanations for the facts uncovered.

General

- a. The expert may need to be security cleared to the appropriate security level to handle the evidential material;
- b. The expert should sign a Non-Disclosure Agreement (to ensure whatever knowledge acquired during the examination remains confidential);
- c. Where relevant, the expert should be made aware of any relevant guidelines on material related to paedophilia including the effect of such material on others involved and be required to risk assess the same appropriately;
- d. The specialist should have no conflict of interest and should be required to make a declaration to that effect.



3 Search and seizure

This section deals with the actions to be taken when recovering sources of potential electronic evidence from premises controlled by a suspect.



3.1 Who and what to take to the scene

The planning and preparation process should be sufficiently rigorous to identify the level of forensic support that will be required at the scene. Where the need for digital forensic expertise has been identified the person in charge of the search should inform the local forensic unit and/or external specialists as soon as possible to ensure the necessary support is available.

The first decision in relation to potential electronic evidence in a planned operation will be the nature of the search location and the type(s) of seizure that may be required; either the seizure and removal of equipment that is not being used at the time (i.e. 'dead box') or the capture of live data from devices that are switched on and in operation or a combination of both.

Such decisions may well need to be revised at the scene once circumstances become clear, but, as much information as possible about the IT system used should be collected in advance. Where required by national law, such details may be required for the search warrant.

Questions for the planning process would include:

- What computer hardware/operating system/software/applications and storage media, communication and network related equipment (ISP, phone, facsimile, modem, LAN network equipment, etc.) is likely to be found?
- Who is responsible for the computer system and/or network (e.g. is there a local administrator or is the system administered by an external company)?
- How much equipment is there likely to be?
- How much data may need to be copied? And,
- Is there a system backup available on storage media?

Once the initial planning and thinking has been done, the preparation for the actual entry and search should include the following steps:

- Check that the entry to the premises and seizure of e-evidence has been properly authorised in law (e.g. obtain a search warrant or other authorisation in accordance with applicable laws);
- Ensure that rapid and safe means of entry are available and have been arranged;
- Choose the team members (including external specialists if necessary);
- Assign individual tasks to the team members;
- Brief the team members about how to perform their tasks (they should have passed the corresponding basic training); and,
- Supply the necessary seizure tools and equipment.

Remember that all activities should be in compliance with state and local laws as well as agency policy.

If it is known or suspected that e-evidence might be found at the scene, the search team should include members specially trained in that function as well as an independent specialist if necessary. If the system is administered or maintained by an external company or administrator, the investigator might consider involving them as an expert witness (of course if he/she is not considered a suspect and has no other conflict of interest).

At a minimum those dealing with electronic evidence (and ideally everyone present) should have received basic training in identifying and collecting potential sources of such evidence. Where possible each group tasked with seizing electronic evidence should consist of at least two officers so that there can be two witnesses for every action.

All team members should know the principles to apply when handling e-evidence as well as those used for handling other physical evidence. They should be aware of any special measures required (e.g. not to use aluminium powder for collecting fingerprints from electronic devices). They should also know that in certain situations they must contact a specialist unit and should have this contact information ready if they have not involved specialists in the search.

Special tools and equipment are sometimes needed to collect e-evidence and, although advances in technology may require additions to any equipment used previously, the following basic toolkit will assist in many cases.

- Disassembly and removal tools:
 - Screwdrivers (flathead and crosshead, and manufacturer-specific, (e.g. Hewlett Packard, Apple));
 - Spanners (hex-nut, star-type nut and secure-bit);
 - Pliers (standard and needle-nose);
 - Wire cutters (for removal of cable ties);
 - Small tweezers;
- Documentation:
 - Search and seizure record (property register - see Appendix of this guide);
 - Labels and tape (to mark and identify component parts of the system, including leads and sockets);
 - Cable tags;
 - Exhibit labels (tie-on and adhesive - see Appendix to this guide);
 - Other necessary forms and documents for completion at the scene (see Appendix to this guide);
 - Indelible coloured marker pens (to code and identify removed items);
 - Camera and/or video camera (to photograph scene and any on-screen displays);

- Package and transport supplies:
 - Antistatic bags (for protection of equipment being removed such as circuit boards). Any materials (such as polythene bags) that can produce static electricity should be avoided;
 - Faraday bags and/or aluminium foil;
 - Antistatic bubble wrap;
 - Cable ties (for securing cables);
 - Evidence bags and tape;
 - Boxes for packaging external storage media such as USB devices DVDs, or CDs;
 - Packing materials (materials that can produce static electricity such as styrofoam or styrofoam peanuts should also be avoided);
 - Flat pack assembly boxes or sturdy boxes of various sizes (original packaging should be used whenever available);
- Communication tools:
 - Mobile phone or other communication devices for obtaining advice (should not be used in the proximity of computer equipment);
 - Contact information for assistance (e.g. phone numbers of the specialist unit)
- Other items:
 - Small torch with a bracket;
 - Gloves;
 - Hand truck (i.e. a sack barrow or 2 wheeled dolly);
 - Large rubber bands;
 - Magnifying glass;
 - Printer paper;
 - A laptop computer loaded with all standard forensics tools;
 - Network cables (Twisted Pair and Crossover);
 - Sufficient Hard-Drive capacity (e.g., some Terabyte external Hard Disk Drives);
 - Hardware Write-Blockers (for on-site imaging and triaging purposes);
 - Forensic Boot-DVDs (for when officers are trained in their use, for forensic purposes);
 - Live Data forensics tools (when officers are trained in their use, for forensic purposes);
 - Transport (to and from the scene, for team members, seizure tools and equipment and the seized evidence).

3.2 Securing the scene



The person in charge of the search should ensure the safety of all persons at the scene and the integrity of all evidence, both traditional and electronic. Remember that potential evidence on computers and other electronic devices can be easily altered, deleted, or destroyed, but traditional forensic evidence also has a role to play and is susceptible to cross contamination.

Securing the scene involves the following steps:

- Follow standard policy and procedure in your jurisdiction to secure the crime scene:
- Move all persons away from the proximity of any evidence to be collected (including equipment and power supply);
- Secure all electronic devices including personal and portable devices;
- Refuse offers of help or technical assistance from any unauthorised persons.
- Leave a computer or electronic device off if it is already turned off.
- If a computer is on or the state cannot be determined, the investigator should follow the steps described in section 3.4.3.
- Protect volatile data physically and electronically by following the steps described in section 3.5.
- Identify and document related electronic components that will not be collected;
- Identify telephone and network lines attached to devices, document and label them;
- Decide if any other evidence is required from a device to be seized (e.g. DNA, fingerprints, drugs, accelerants);
 - If so, follow the general handling procedures for that evidence type laid out in the relevant handbook;
 - Postpone destructive techniques until **after** electronic evidence recovery is done;
 - Collect latent prints **after** e-evidence recovery is complete (since keyboards, computer mouse, diskettes, CDs, or other components may have latent fingerprints or other physical evidence that should be preserved);
 - **Do not** use aluminium powder to collect fingerprints from the scene as this may damage equipment and data.
- Search the scene for non-electronic, but related evidence, such as:
 - written passwords and other handwritten notes;
 - blank pads of paper with indented writing (but do not shade with graphite pencil);
 - hardware and software manuals;
 - calendars or diaries;
 - text or graphical computer printouts;
 - photographs; or,

- information about personal interests that may be useful for later password /passphrase cracking (most passwords are directly related to the personal environment, such as licence plates, partners/children, phone numbers, hobbies, etc.);
- (Don't forget traditional physical evidence such as fingerprints and DNA).
- Conduct preliminary interviews;
 - Separate and identify all persons (witnesses, subjects, or others) at the scene and record their location at time of entry;
 - Use a checklist to collect and record information from these individuals;
 - Consistent with agency policy and applicable law (for instance in the requirement to provide a caution against self incrimination or list of rights), obtain information from these individuals such as:
 - Purpose of the device/system (e.g. bookkeeping);
 - Owners and/or users of devices/systems found at the scene, as well as passwords (see below), user names, and Internet Service Provider;
 - Any passwords required to access the system, software, or data. An individual may have multiple passwords (e.g. BIOS, system login, network or ISP, application files, encryption pass phrase such as for PGP or Truecrypt, e-mail, access token, scheduler, or contact list);
 - Any unique security schemes or destructive devices;
 - MySpace, Facebook, or other online social networking Website account information.
 - Any offsite data storage; and
 - Any documentation explaining the hardware or software installed on the system;
 - Any other relevant information.

3.3 Documenting the Scene



Documenting the scene is an ongoing process **throughout the entire seizure procedure**. It is of crucial importance to document accurately the location and condition of computers, storage media and other electronic and conventional devices. This section gives only a summary of the information to be documented.

In general, the following must be documented, but additional documentation may be created during the collection phase:

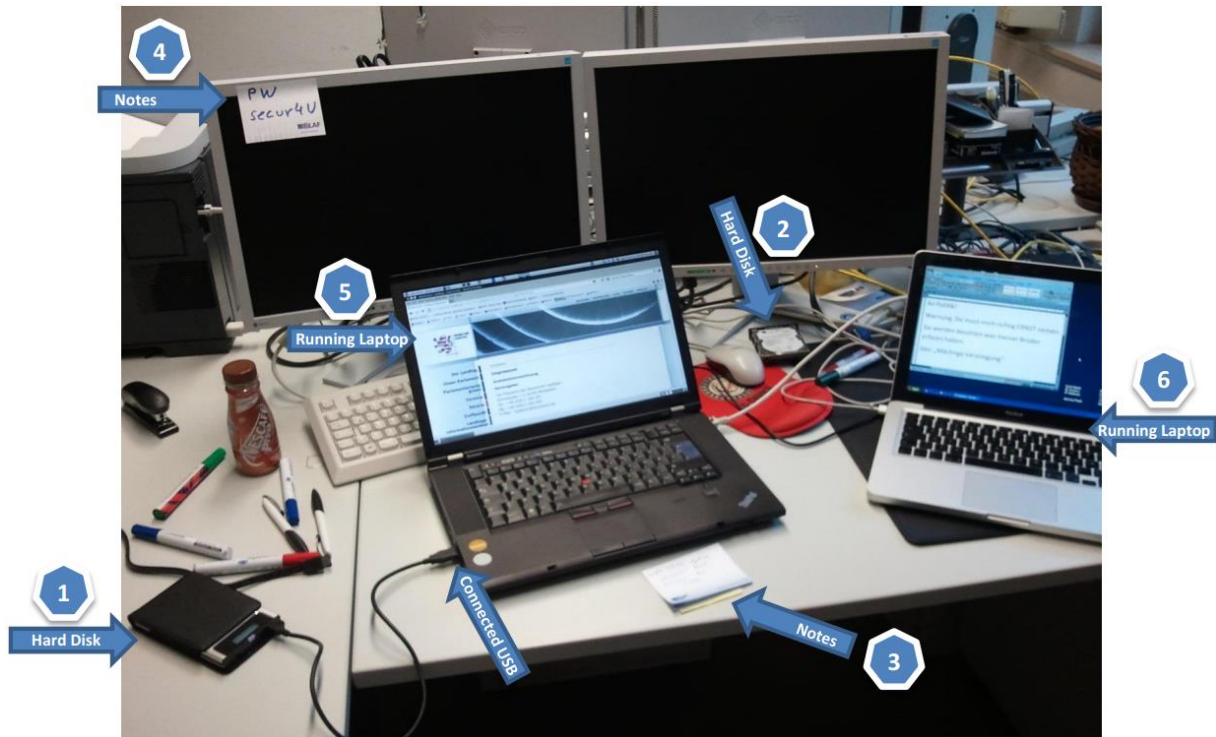
- Physical scene;

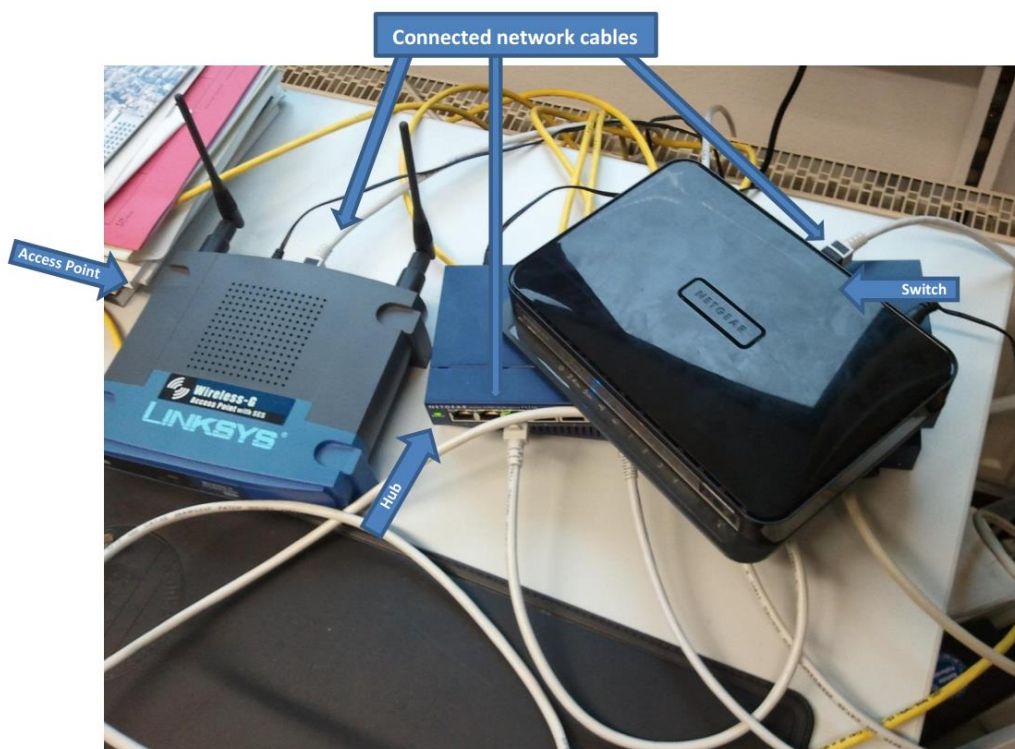
Restricted

- Draw a sketch plan of the system (including details such as the position of the mouse and the location of the components);
 - Photograph/video/document the entire scene (360 degrees of coverage, if possible);
 - Locate computer systems and electronic components/devices/equipment and how they are connected.
- Document the following:
 - Details of all relevant equipment found (including make, model and serial number);
 - Condition and location of each computer system containing or presenting electronic evidence, including the power status of the computer (on, off, or in sleep mode);
 - Document all connections (cable or wireless) to and from the computer system or other devices;
 - Label all ports and cables (including connections to peripheral devices) to allow for exact reassembly at a later time; Label unused connection ports as "unused";
 - Identify laptop computer docking stations in an effort to identify other storage media;
 - Document the details of the monitor at the time of intervention;
 - Photograph the front of the computer as well as the monitor screen and other components;
 - Make written notes of what appears on the monitor screen;
 - Video active programs or create more extensive documentation of monitor screen activity;
 - Document relevant electronic components that will not be collected;
 - Information from the persons found at the scene;
 - Interview the persons and document their answers completing the forms;
 - Document the following:
 - Details of all persons present on the premises searched;
 - Details of all persons who used the relevant computer system and equipment;
 - Remarks, comments and information offered by the computer users/owners/witnesses;
 - All actions taken at the scene;
 - Create audit trail/seizure log with the description of the action taken and the exact time.

Here are some examples of what an investigator might encounter in a search and seizure scenario and how he can document the scene:

Overview pictures:

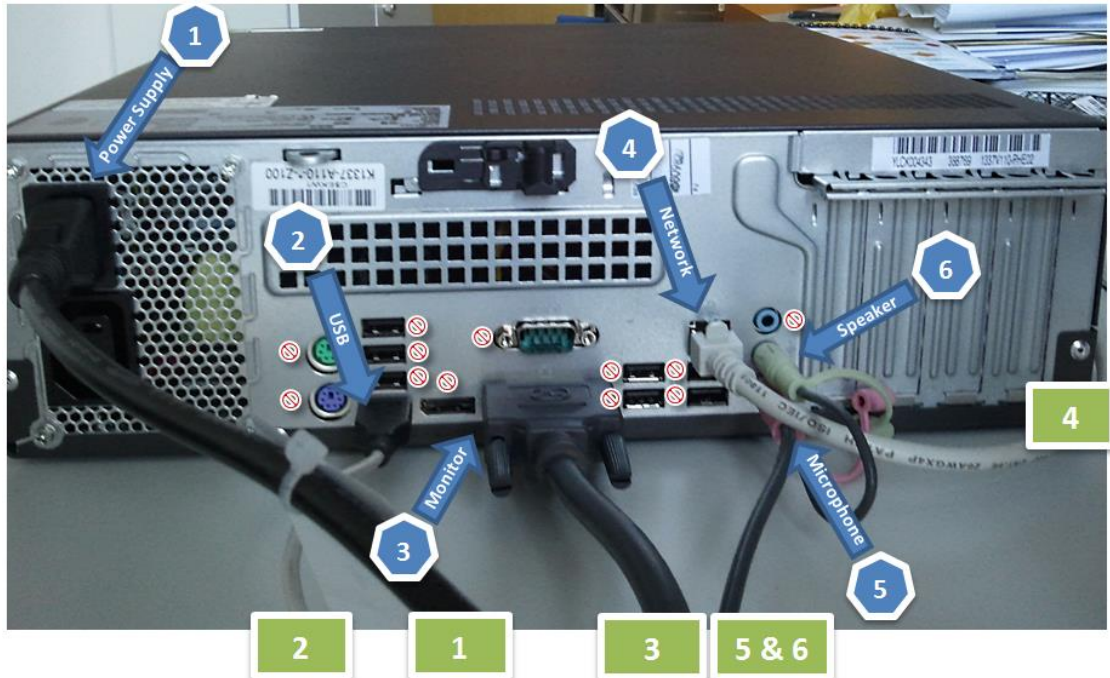




Details:



Detailed Connection Status of a wired Desktop Computer:





3.4 Search and seizure in 'dead box' scenarios

An IT system should not be seized as evidence just because it happens to be found at the scene. Such a measure must be justified and in proportion to the corresponding offence, therefore the person who ordered the search should make a conscious decision whether an item is to be taken. S/he should have a reasonable suspicion or enough evidence to justify the seizure.

A 'dead box' scenario refers to equipment that has been found during the search to be turned off. Dead box devices will be removed from the scene and examined later at a law enforcement or digital forensic laboratory.

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 e-evidence will require special collection, packaging, and transportation. E-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.

Recovery of **non-electronic evidence** (or conventional evidence) may also be crucial in the investigation and proper care should be taken to ensure that such evidence is recovered and preserved. Other items relevant to the investigation are frequently found in close proximity to the computer or related hardware items and should also be seized. As always, all item of evidence should be identified, secured, packaged and preserved in compliance with agency policies and applicable laws.



3.4.1 Packaging, transport and storage

Computers and related devices are fragile electronic instruments that are sensitive to temperature, humidity, physical shock, static electricity, magnetic sources, and even to some operational function (e.g. switching on/off). Special precautions should therefore be taken when packaging, transporting, and storing e-evidence. To maintain the chain of custody, the packaging, transportation, and storage should be recorded and any change of custody or condition of the seized property should be timed and noted.

Inexpert handling can cause damage or destruction of e-evidence and the following precautions should be taken:

- Packaging:
 - Ensure that all collected e-evidence is properly documented and labelled before packaging;
 - Whenever possible, transport the collected e-evidence in the original packaging;

Restricted

- If no original packaging is available, use antistatic packaging (e.g. paper or antistatic plastic bags). Avoid using materials that can produce static electricity, such as standard plastic bags;
 - **Do not** fold, bend, or scratch storage media such as diskettes, CD-ROMs, and tapes;
 - **Do not** affix adhesive labels on the surface of the storage media. Use boxes or envelopes for packaging storage media whenever possible;
 - Ensure that all containers holding evidence are properly labelled;
 - If multiple computer systems are collected, label each system so that it can be reassembled as found.
- Leave cellular, mobile, or smart phone(s) in the power state (on or off) in which they were found.
 - Package mobile or smart phone(s) in signal-blocking material such as Faraday isolation bags, radio frequency-shielding material, or wrapped in aluminum foil to prevent data messages from being sent or received by the devices. If incorrectly packaged or removed from shielded packaging the device may be able to send and receive data messages. Be aware that keeping devices in signal-blocking packaging may reduce battery life significantly. In cases of low battery power consider putting devices into "flight-mode" instead.
- Transport:
 - Keep electronic evidence away from magnetic sources. Radio transmitters, speaker magnets and heated seats are examples of items that could damage e-evidence;
 - Ensure that the equipment is protected from shock and bumps (i.e. mechanical damage), heat, and humidity;
 - Ensure that computers and other devices that are not packaged in containers are secured during transport to avoid shock and excessive vibrations. For example, computers should be placed on the vehicle floor and monitors placed on the seat with the screen down and secured by a seat belt;
 - **Do not** put heavy objects on top of smaller pieces of equipment/storage media;
 - Whenever possible, **do not** store electronic evidence in vehicles for long periods of time;
 - Document the transportation of the digital evidence and maintain the chain of custody for all evidence transported.
- Storage:
 - Ensure evidence is inventoried in accordance with the relevant policies;
 - Store evidence in a secure area, away from extreme temperatures and humidity;

- Protect it from magnetic sources, moisture, dust and other harmful particles or contaminants;
- Use an adequately secure store room with appropriate:
 - access control;
 - fire protection and suppression systems (e.g. alarm, fire extinguishers, no smoking in the storage area or in the vicinity);
 - temperature and humidity control; and,
 - protection from magnetic sources (e.g. isolated from directional radio devices).
- **Do not** store any inflammable items in the same room or in the vicinity (e.g. cleaning chemicals, or stacks of paper);
- Use suitable floor covering to avoid static charges;
- **Do not** store e-evidence in rooms with water-pipes, especially along the ceiling;
- Be aware that potential evidence such as date, time, and system configuration may be lost as a result of prolonged storage. Since batteries have a limited life, data could be lost if they fail. Appropriate personnel should be informed that a device powered by batteries (e.g. a PDA, or PC/CMOS³³) requires immediate attention.

3.4.2 Computer system & electronic device collection



There are many different types of computer systems including laptops/notebooks, desktops, tower systems, modular rack-mounted systems, mini-computers, and mainframe computers. On these, potential evidence is most commonly found in files that are stored on internal (e.g. memory, hard disks) and external (e.g. CD, diskette, USB token) storage devices and media.

A computer system typically consists of the following components that should be considered for collection in case of seizure:

- a main unit (a plastic or metal housing containing a motherboard, the CPU, memory, and possibly expansion boards);
- a monitor (usually attached to the main unit);
- a keyboard (usually attached to the main unit);
- a mouse;
- cables;
- power supply units (e.g. power packs, and spare batteries);
- possibly additional components (e.g. modems, printers, scanners, docking stations, port replicators, card readers, dongles, smart cards, and external data storage devices); and,
- network devices.

³³ The complementary metal-oxide-semiconductor (CMOS) battery is used to power the BIOS (basic input output system) that enables a computer to start up.

Personal computers (PC) have various types and numbers of ports (i.e. in this case physical outlets like USB ports) for connecting external storage, display screens, keyboards, printers, mice and other peripheral devices. Devices can also be connected to a PC over a wireless connection (e.g. WLAN, Bluetooth, infrared).

PCs tend to use the following operating systems: Microsoft Windows, Unix, Linux or Mac OS. A computer system may be a standalone or it may be connected to a network. In a computer network, additional network components are also usually to be found (e.g. network cables, routers, hubs, and switches), which may provide a wireless connectivity.

As we have seen, storage media and other electronic devices are not always readily identifiable as such. They might be hidden in wristwatches jewellery, keys, toys, etc.

Digital storage devices are frequently not stored near the computer system, but in a separate room or even in a different building. In some cases the media may be locked up in special boxes or cupboards (e.g. data security safes)

Finally, the following items may also be considered for collection and might provide additional help when examining a computer system:

- Hardware and software manuals (including original CD ROMs);
- Notes, diaries, calendars, and similar items, on which passwords or other related information may be noted;
- Blank pads of paper with indented writing;
- Computer related literature;
- Computer printouts;
- Relevant photographs; and
- Computer related keys.

This following section describes the necessary steps in seizing a computer. Some of the initial steps have already been described in previous sections.



Remember:

- **Document** the scene continuously and record all actions you take and any changes that you observe in the monitor, computer, printer, or other devices as a result of your actions.
- **Do not follow any unverified advice from a potential suspect.**
- If a **computer network** is encountered, **contact a forensic computer specialist** in your agency or an external expert identified by your agency for assistance.
- **Beware** that some devices may be connected over a **wireless** connection (e.g. WLAN, Bluetooth, infrared);

- **Beware** that if there is any **network connection**, the computer system may be accessed and manipulated during the seizure (i.e. whenever switched on and within the reach of the network connection).

Steps to follow to secure the scene and seize the equipment:

- Search the area for the following components/items;
 - the computer system components;
 - digital storage media;
 - additional components;
 - other electronic devices; and,
 - non-electronic evidence.
- Conduct preliminary interviews;
- Observe the computer system and determine whether it is on or off (**see below**);
- Document all connections and components and put labels on each connection and device:
 - Photograph and/or sketch a diagram of the connections to/from the computer and the corresponding cables;
 - Record the evidence according to your agency's procedures.
- Carefully remove the equipment and record any serial or identification numbers. Allow the equipment to cool down before packaging and removal.
- If transport is required, package the components.

The charts in Appendices A and B provide an easy to follow flow chart for dealing with seized devices. Users are responsible for ensuring that the procedures set out in these charts are in compliance with any national legislation or procedural guidelines.



3.4.3 Checking the power status (on/off)

This section offers some advice related to the seizure of computer equipment and storage media.

Determine whether the computer system is off or on.

Most computers have status lights that indicate when the computer is on. If fan noise is heard, the system is probably on. If the computer housing is warm, that may also indicate that it is on or was only recently switched off.

N.B. Some portable devices get activated by opening the lid.

Always consider removing the battery from portable computers and devices.

Portable computers (e.g. notebooks or laptops) usually have a battery pack in addition to the main supply. Some even have a second battery in the multipurpose bay instead of a floppy drive or CD

drive. Batteries for such devices are charged when the portable computer is connected to a power supply and, if fully charged, can last several hours. It is often hard to determine whether a portable computer is turned on or off when it is in standby mode.

A computer system that appears to be switched off may be in sleep mode. If so, it could be activated and accessed remotely allowing alteration or deletion of files.

Some screen savers give the impression that the computer is switched off. Observe the monitor and try to determine whether it is on, off, or in sleep mode.

You may encounter one of the following situations:

Situation 1: Monitor is on and work product and/or desktop is visible.

- Document the details of the monitor at the time of intervention
- Proceed to "Setting B" as described below.

Situation 2: Monitor is on and screen is blank (sleep mode) or screen saver (e.g. a picture) is visible.

- Move the mouse slightly (without pushing buttons). The screen should change and show work product or request a password.
- If mouse movement does not cause a change in the screen, do not perform any other keystrokes or mouse operations.
- Document the details of the monitor at the time of intervention
- Proceed to "Setting B" as described below.

Situation 3: Monitor is off.

- Make a note of "off" status.
- Turn the monitor on, then determine if the monitor status is as described in either Situation 1 or 2 above and follow those steps.

Once you have determined whether the computer is on or off, you will need to undertake one of the following:

Setting A: You have determined that system is switched off; **do not** switch it on!

- Remove the power supply cable from the target equipment (**do not** switch it off at the wall socket) and record the time of doing so.
- If dealing with a portable device, also remove the battery pack. Remove any additional battery packs, if applicable (some portable devices have a second battery in the multipurpose bay instead of a floppy drive or CD drive).

Restricted

If the computer system is off, leave it off because the startup process will modify the computer data and potentially destroy the evidence.

Setting B: You have determined that the system is switched on; **do not** switch it off!

- Try to contact a specialist:
 - If a specialist is available, follow their advice;
 - If no specialist is available, continue with the next instruction.
- **Do not** touch the keyboard or other input devices.
- Proceed with steps described in 3.5.



Remember: Removing the power supply cable from the computer system will affect all currently running programs and all data currently stored in the RAM of the computer (including relevant data, such as passwords) will be lost. This would include any connection to the Internet, printing, or encryption.



Remember: When a system is turned on, it is crucial to have the suspect secured and away from fuse boxes, power switches as well as mobile communication devices. There have been cases where running systems with full-disk encryption have been powered-off during the search just because the suspect was able to reach the fuse box or to send a signal to a remotely controllable power adapter.

Setting C: You cannot determine whether the system is switched on or off.

- Assume that it is switched off. **Do not** press the power switch.
- Remove the power supply cable from the target equipment (**do not** switch it off at the wall socket) and record the time of doing so.
- If dealing with a portable device, also remove the battery pack. Remove any additional battery packs if applicable (some portable devices have a second battery in the multipurpose bay instead of a floppy drive or CD drive).

3.4.4 Computer network collection



Remember - If you have a good reason to believe that there is a network in place contact a computer network specialist before attending the scene. If no specialist is available, the information provided in this section may help you when seizing the relevant equipment.

A computer network can be indicated by:

- The presence of multiple computer systems;
- The presence of network components such as:

- Network interface cards (NIC, or network cards) and associated cables (if not wireless);
 - Wireless Local Area Network (WLAN) devices (e.g. wireless access point);
 - Routers, hubs, and switches;
 - Servers; and,
 - Network cables running between computers or central devices such as hubs.
- Information provided by informants or individuals at the scene.



Remember: If you encounter a computer network, contact a forensic computer specialist in your agency or an external specialist recommended by your agency for assistance.



3.4.5 Additional components

As mentioned above, a computer system may include some additional components such as:

- External storage devices connected by cables or other interfaces;
 - External hard drives,
 - External optical drives (e.g. CD, DVD or Blu-ray burners),
 - Floppy drives,
 - Magnetic tape drives.
- Drive duplicators;
- MP3 players;
- Dongles;
- Smart cards and smart card readers;
- Printers;
- Scanners;
- Docking stations;
- Port replicators;
- PC cards and PC card readers;
- Web cameras (see digital cameras);
- Modems (internal or external, dialup/analogue or cable, DSL, ISDN, wireless modems);
- Wireless devices:
 - Infrared-adapters (USB, serial, mainboard);
 - Infrared-enabled devices (wireless LANs, links between notebooks and PCs, cordless modems, intrusion detectors);
 - Bluetooth-enabling devices (e.g. Bluetooth USB dongles for PDAs and PCs, PC cards for notebooks); and,
 - Bluetooth-enabled devices (e.g. headsets, PDAs, notebooks, phones, GPS receivers).



Remember: Some components may appear to have a different function (e.g. pens, watches, jewellery).

Please refer to the information above for the general seizure, packaging, transport and storage instructions.



3.4.6 Digital storage media

The following media are frequently not stored near the computer, but either in a separate room or in a different building (As mentioned in 3.4.2 above, in some cases the media might be locked up in special boxes so-called data security closets):

- Floppy disks;
- Backup media (e.g. magnetic tapes);
- CDs and DVDs;
- Hard drives not connected to the computer;
- PC cards;
- Magnetic stripe card;
- Memory cards;
- USB memory pens/keys/sticks;
- Dongles;
- Solid state disks.

Please refer to the information above for the general seizure, packaging, transport and storage instructions.



3.4.7 Other electronic devices

- Personal digital assistants (PDA or handheld computers), such as:
 - Electronic organiser;
 - Communicator; or,
 - Smart phone.
- Video equipment (video camera, video cassette recorder (VCR) or player);
- Audio recorders;
- Chips;
- Circuit boards;
- Expansion boards;
- Digital cameras;
- Access tokens (for identification/authentication information of the card and the user, level of access, configurations, permissions, or the device itself), e.g.
 - Smart cards;
 - Dongles (security dongle), also called hardware keys; or,

- Biometric scanners.
- Telephones;
- Answering machines;
- Facsimile machines;
- Dictating machines/voice recorders (see also answering machines);
- Pagers;
- Games consoles with memory cards, gameboys with cartridges, Xboxes, gamecubes, etc.;
- GPS devices and other satellite positioning devices;
- Digital watches;
- Credit card skimmers or magnetic stripe readers;
- Copiers.

3.4.8 General seizure instructions for electronic devices

The following should be considered when seizing an electronic device (the same advice as already offered under Section 3.4.3 regarding computers.):

- If the device is switched on, do not switch it off because switching it off may activate a lock mechanism:
 - Photograph the display (if applicable) and record the information displayed;
 - Remove all power supply cables (usually it is better to remove them from the target equipment and not from the wall socket);
 - Do not try to access the internal memory or any storage media.
- If it is switched off, do not switch it on because that could modify/destroy evidence (as in computer systems);
- Disconnect each telephone line from the wall rather than the device and then document and label it;
- Collect/record important information:
 - Collect manuals and other instructions if available;
 - Record the relevant data (e.g. phone number).
- Please refer to the information above for the general packaging, transport and storage instructions:
 - Since batteries have a limited life, data could be lost if they fail. Therefore, appropriate personnel should be informed that a phone powered by batteries is in need of immediate attention;
 - After seizure, hand the device to an expert as soon as possible. In the case of PDAs and mobile phones this has to be done immediately.



Remember: After seizure the device should be handed to a specialist as soon as possible. In the case of PDAs and mobile phones this should be done immediately.



3.4.9 Personal digital assistants (handheld computers)

Even though personal digital assistants (PDA, or handheld computer) are not as popular today as they were in the past, they might still be found at the scene. A PDA is a small device that can be used for computing, telephone/fax, paging, networking, and other things. It is (was) typically used as a personal organiser (or electronic organiser). A handheld computer approaches the full functionality of a desktop computer system. Some PDAs contain disk drives, and some have PC card slots that can hold a modem, hard drive, or other device. They usually include a mechanism to synchronize their data with other computer systems, most commonly by a connection in a cradle. If a cradle is found at the scene, attempt to locate the associated handheld device. A PDA may contain potential e-evidence in the same way as a computer system.

PDAs contain a small microcomputer with a real or virtual miniature keyboard and a liquid crystal display together with memory chips in which all the information is stored. The amount of working memory (i.e. RAM) is often indicated in the name of the PDA (e.g. 2Gb, 16Gb, or 32Gb). The memory is kept active by batteries and if these fail all information contained in the PDA may be lost. Often there are two sets of batteries: a main set which is designed to run the display and keyboard when the PDA is switched on; and, a backup battery which maintains information in the memory if and when the main batteries fail.

Some PDAs have a single rechargeable battery, which is normally kept topped up by keeping the PDA in its cradle connected to a PC. This battery tends to fail very quickly (a matter of a few days) when not kept charged. Special measures need to be taken to maintain the evidence in this kind of device.

Most PDAs will use one of the following operating systems: Palm OS, Symbian, Linux, Android, the Psion EPOC, or the Windows operating systems. Use of the Windows operating system makes the PDA fully compatible with Windows based PCs

When seizing PDAs as e-evidence the following should be considered;

Collecting:

- If a **computer network** is encountered **contact a forensic computer specialist** in your agency or an external expert identified by your agency for assistance.
 - Beware that some PDAs may be connected over a wireless connection (e.g. Bluetooth, infrared);

- Beware that if there is any network connection, the PDA may be accessed and manipulated during the seizure (i.e. whenever switched on and within reach of the network connection).
- If a switched-on PDA is found at the scene, **do not** press the RESET button and **do not** remove batteries because it can result in complete loss of the data stored in the PDA.
- **Do not** switch on or open PDAs upon collection;
- Seize power leads and peripherals including memory extensions or items that connect the PDA to the PC (e.g. cradle, cable, charging set);
- PDAs usually have an automatic switch-off function that may activate a lock or encryption mechanism (they can be activated by switching it off as well):
 - **Avoid** encryption activation by keeping the PDA in running mode (e.g. by tapping on a blank section of the screen) until expert advice is available.
- Packaging, transport and storage;
- Set PDA in cradle pending examination.

Please refer to the information above for the general seizure, packaging, transport and storage instructions.



3.4.10 Telephones, Smartphones and Tablet Devices

A telephone is a handset that is found either:

- On its own (as with mobile phones);
- With a remote base station (cordless), or
- Connected directly to the landline system.

A mobile phone may have some additional functionality (for instance the ability to take digital photographs). Modern mobile phones often have an operating system (such as the iOS, Android, Windows Phone) that allows the user to carry out tasks that are typically associated with traditional computer systems including receiving and sending e-mails, surfing the Internet, chatting, playing games, etc. Mobile phones with such expanded functionality are called smartphones.

A telephone may draw power from an internal battery, electrical plug-in, or directly from the telephone system. Two-way communication is established from one handset to another by using land lines, radio transmission, cellular systems, or a combination of systems. Many telephones can store names, phone numbers, and caller identification information. Many mobile telephones can also store names, addresses, calendar information, details about incoming calls, receive e-mail, send texts, act as a voice recorder and may be used to access the Internet (so they contain Internet access data). Access to many mobile phones will require PINs, passwords or other access codes,

Tablet devices are very similar to smartphones, but have a larger screen. They come with their own operating systems based on the mobile phone versions of the operating systems. Like smartphones they offer a near endless variety of functionality and allow the user to install his or her own applications (apps).

Please refer to the information above for the general seizure, packaging, transport and storage instructions. Also see section 3.4.



3.4.11 Smart cards and magnetic stripe cards

A smart card is a small handheld device that contains a microprocessor (i.e. a "chip". It is sometimes referred to as a chip card) that is capable of storing a monetary value, encryption key or authentication information (password), digital certificate, or other information. Some smart cards are actually small computers because they also have an operating system (i.e. a smart card operating system).

Smart cards may be used for different purposes and applications for example:

- As key cards allowing physical access to restricted areas/buildings/rooms;
- Providing access control for computers or programs or functions (e.g. as an encryption key);
- Allowing cash withdrawal at ATMs;
- Acting as an electronic purse/wallet;
- As a customer loyalty card or bank card;
- As a social security or government identification card;
- As authorisation for accessing certain government services;
- For creating digital signatures;
- As a payphone card; or,
- For otherwise storing personal data, addresses, access codes.

Because of these various uses and the information that it may contain a smart card can contain potential evidence in much the same way as a computer system.

According to international standards a smart card should be 85.6 x 54 x 0.76mm (i.e. format ID-1, the so-called "ATM card size") with an electrical contact plate on the front side of the card. Smart cards will also often carry a magnetic stripe on the reverse side.

Other standards of chip cards also exist. For instance the ID-0 format (size 25x15x0.76mm) which are used in mobile phones (full size SIM card).

USB tokens³⁴ contain both a chip (based on the same standards as a chip in a smart card) and chip card reader functionality. This means they are becoming more and more popular for two step authentication for obtaining computerised services.

Some smart cards exist that use induction technology instead of a contact plate. These cards do not require physical contact with the card reader, but need only to be placed in close proximity to the reading device. "Super" smart cards have also been developed which have an internal battery, a small LCD display and an integrated keypad. These cards have a significantly enhanced level of security.

Most smart cards data and functions are usually protected by a secret personal code (called a personal identification number or PIN) and data on the card become accessible after the correct code has been entered on the computer keyboard, on the card reader keyboard (or on the super smart card itself).

There are some rules for handling smart cards:

- Do not fold it;
- Do not expose it to extreme temperatures;
- Do not touch the electrical contact plate;
- Protect from scratches, liquids, magnetic influences, etc;
- Try to find out the PIN (look for kept with the card or ask the trustworthy user(s)).
- Do not attempt to gain access to the data/functions on the card, even when a potential suspect claims to have told you the PIN. Several attempts to enter a false PIN can result in irrevocable loss of data and the card being blocked (in some cases it is possible to unblock the card by another secret personal code called a personal unblocking key or PUK).
- Photograph/note/copy the information printed on the card (e.g. cardholder identification, account numbers, credit card companies, business contacts, etc.).
- If present, also seize any smart card readers found.

3.4.12 Answering machines

An answering machine is an electronic device that is part of a telephone or connected between a telephone and the landline connection. Older models use micro magnetic cassette tapes, while modern machine will use an electronic (digital) recording system. An answering machine records voice messages from callers when the called party is unavailable or chooses not to answer a telephone call. It usually plays a message recorded by the telephone owner requesting the caller to leave a message.

³⁴ In computing a token is something that allows a particular action to be done. Very often it will be a physical object that provides electronic access to a protected system or program or some kind of computer service.

Answering machines can store voice messages and, in some cases, time and date information about when messages were left. They may also contain other voice recordings.

Potential evidence from an answering machine can include:

- Caller identification information;
- Deleted messages;
- Last number called;
- Voice memos;
- Phone numbers and names; and,
- Micro cassette tapes.

Please also refer to the information above on the general seizure, packaging, transport and storage instructions.

3.4.13 Digital cameras

As already discussed, a digital camera is a device for capturing images and video. It has an internal memory, related storage media and conversion hardware capable of transferring images and video to computers.

Potential evidence may be found from;

- The camera itself;
- Images (including Exif-Metadata³⁵);
- Removable memory cards;
- Sound;
- Time and date stamp; and,
- Video.

Please also refer to the information above for the general seizure, packaging, transport and storage instructions.

3.4.14 Facsimile (fax) machines

A facsimile (or fax) machine is a device for scanning images and text and sending them over the telephone line. This functionality is available for computers as well (e.g. fax/modem PC cards). Facsimile machines can contain the following evidence:

- Film cartridge;
- Pre-programmed phone numbers (i.e. short dial lists);
- History of transmitted and received documents;

³⁵ The Exchangeable Image File Format (EXIF) is a standard format for images, sound, cameras and scanners etc. Devices that use EXIF will often mark images with certain data about the taking of the image. Many modern devices also add GPS data (so-called "geotagging").

- Memory allowing multiple-page outgoing faxes to be scanned, stored and sent at a later time or incoming faxes to be stored and printed later;
- Fax transmission protocol (i.e. send/receive log);
- Header; and,
- Clock adjustment.

Please also refer to the information above for the general seizure, packaging, transport and storage instructions.

3.4.15 Printers

Printers may maintain usage logs, time and date information, and, if attached to a network, they may store network identity information. In addition, unique characteristics in a print out may allow a particular printer to be identified.

Potential evidence from a printer includes;

- Documents;
- Hard drive/flash storage;
- Ink cartridges;
- Network identity/information;
- Superimposed images on the roller;
- Time and date stamp; and,
- User usage log.

Please refer to the information above for the general seizure, packaging, transport and storage instructions.

3.4.16 Scanners

Scanners are digital devices that scan text documents and hard copy images and store them in digital format. The device itself may be evidence. In addition, imperfections in the scanner that are reproduced in the scanned copies may allow a particular scanner to be identified as the one involved in an illegal act.

Please refer to the information above for the general seizure, packaging, transport and storage instructions.

3.4.17 Photocopiers (copy machines)

Some photocopiers maintain user access records and a history of any copies made. Copiers with a 'scan once/print many' feature save the scanned document to memory for later printing. Potential evidence from copiers includes documents, time and date stamp, and usage log.

Please refer to the information above for the general seizure, packaging, transport and storage instructions.



3.4.18 Multifunctional machines

The devices described in the three previous paragraphs may be combined into one device (e.g. a copy machine, a scanner and a fax machine). Several physically separated devices may also function together as one multifunctional machine if connected over a network.



3.4.19 Pagers

A pager is a device that may be used for sending and receiving numeric (e.g. phone numbers) and alphanumeric (text, often including e-mail) messages.

Mobile computing devices and mobile phones can also be used as pagers.

Please refer to the information above for the general seizure, packaging, transport and storage instructions.



3.4.20 GPS devices and other satellite positioning devices

Global Positioning Systems (GPS) devices can provide information on previous locations and travel logs including destination information, way points, and routes. Some GPS devices automatically store this information. Potential evidence found in a GPS device could be as follows:

- Home location;
- Previous destinations;
- Points of Interest;
- Travel logs;
- Tracing/route information;
- Way point coordinates; and,
- Way point name.

Please refer to the information above for the general seizure, packaging, transport and storage instructions.



3.4.21 Wearables (e.g. smart watches, activity trackers)

There are several types of wearable devices that incorporate very small computer systems integrated into clothes or accessories. They typically have a set of sensors (e.g. GPS, gyro sensor, heart rate sensor) and communication functionality (e.g. WLAN, Bluetooth). Such devices may store messages and additional information such as address books, appointments, calendars, user activity, geographical information and notes. They also have the capability of synchronizing information with a smart phone or a computer. Potential evidence to be considered includes:

- Address book

- Appointment calendars
- E-mail
- Geo information
- Activity events
- Notes and,
- Phone numbers.

Some wearables may contain a storage device, such as flash memory, a USB token, or even a camera.

Please refer to the information above for the general seizure, packaging, transport and storage instructions.



3.4.22 Magnetic stripe readers

Magnetic stripe readers (e.g. credit card skimmers) read information contained on the magnetic stripe on plastic cards. Potential evidence contained on the magnetic stripe include:

- Cardholder details;
- Card expiration date and credit card numbers; and,
- Security information.

Please refer to the information above for the general seizure, packaging, transport and storage instruction.



3.5 Search and seizure in live data scenarios

Live Data Forensics are likely to be necessary when a crime scene has computers and electronic devices switched on and operating. In the early years of computer forensics whenever an investigator found a running system during a search and seizure process, the advice was to “Pull the plug”! Since then, the volume of volatile data held in memory, the use of remote connections and encryption software has increased enormously. Pulling the plug means all the volatile data will be lost to the investigation, the remote connections will drop and open files may be locked and encrypted. Such data and information can be of high evidential value and the need to capture live data has led to a revised set of procedures and guidance. The possibility of altering or even overwriting evidence is very high and live data forensics require a much higher level of technical knowledge and expertise. .

For Live Data Forensics the principles 1 and 2 defined in the introduction to this Guide are particularly relevant. Investigators must be qualified and competent to conduct the necessary steps and use techniques that will minimise the impact on the system. A detailed audit trail of all the actions taken together with the times they were taken is vital.

Forensic examination of a live system requires specific training, hands-on practical experience, and a set of validated forensic tools. If no examiner with this skillset is present at the scene, a

specialist unit should be immediately asked for support. However, if nobody can be reached, pulling the plug and losing the volatile data may make more sense than risking possible contamination of the evidence by uninformed attempts at capturing live data .

Before going into detail on how to acquire different kinds of volatile data we should define volatile data and what kind of evidence they can provide.



3.5.1 Volatile data

For the purposes of this Guide 'Volatile Data' is defined as follows:

Volatile data are data that are digitally stored in a way that the probability is very high that they will be deleted, overwritten or altered within a short space of time due to human or automated interaction.

Volatile Data are highly fragile and will be lost if not saved quickly and correctly. In modern IT systems the amount of information held in the volatile Random Access Memory (RAM) can be as large as 12 GB or 16 GB of data (the equivalent of about 55.000 pictures with an average size of 300 KB) and it is not just data stored in RAM that can be lost. Data in modern IT environments is not always stored and processed locally. A wide range of services offer cheap and even free storage and powerful processing resources on remote systems (i.e. the Cloud). Access to this data will be governed by the legislation of the country hosting the data and access might not be possible other than during the search. Indeed, in some countries national laws may prohibit access to or acquisition of such data even on a live system.

There are different kinds of volatile data with which the investigator needs to be familiar:

1. **Volatile data on the physical computer** like open network connections, running processes and services, ARP³⁶ and DNS³⁷ caches.
2. **Transient data** that are not volatile by nature, but are only accessible at the scene. Encrypted volumes as well as remote resources are examples of this kind of data. These data can become inaccessible, altered or deleted if the investigator is unable to acquire them at the time of the search.

Both of these categories are explored further below.

³⁶ ARP means Address Resolution Protocol. It is a commonly accepted set of rules and standards used to convert an IP Address into a physical hardware address so that messages on a network are sent to the correct device.

³⁷ DNS stands for Domain Name System. DNS is a kind of database that links the series of numbers used as an IP Address to the more user friendly domain names.



This table by Farmer and Venema³⁸ describes the possible time frame for obtaining different types of data:

| Type of Data | Degree of Volatility |
|--|----------------------|
| Registers, peripheral memory, caches, etc. | Nanoseconds |
| Main memory | Ten nanoseconds |
| Network state | Milliseconds |
| Running processes | Seconds |
| Disk | Minutes |
| Floppies, backup media etc. | Years |
| CD-ROMs, printouts, etc | Tens of Years |

Volatile Data can be rich sources of evidence. A 'live' computer can show the processes currently running (i.e. show what operations the computer is undertaking), caches (where data is temporarily stored), network connections and reveal any data stored in memory. Memory can also contain useful information such as passwords or decrypted applications (useful if a machine has encryption software installed) and sometimes even malicious code that has not been saved to disk. If the traditional approach of 'pulling the plug' were to be followed such useful information would be lost. However, if the data are captured before removing the power, an investigator will have a wealth of additional information to add to the evidence on the hard disk.

The following are likely to be stored in volatile memory:

- Running processes;
- Running services;
- System information;
- Logged on users;
- Listening and open ports;
- ARP (address resolution protocol) cache;
- DNS cache;
- Auto-start information;
- Registry information not yet written to the disk;

³⁸ D. Farmer and W. Venema (2006), Forensic Discovery, Addison & Wesley, ISBN 0-201-63497-X

- Unsaved documents;
- Binaries of process, services including those of Malware only residing in memory.

In a search and seizure scenario, an investigator can preserve volatile data in the following way:

- Identify, secure, document and photograph each device containing volatile data;
- Observe and isolate potential suspects and other persons from the equipment and prevent them from altering or destroying the evidence;
- Monitor IT components and prevent any automated alteration or destruction of evidence.



3.5.2 Physical access

When involved in a search it may be difficult to determine easily whether a computer is turned on or not. In addition to the steps provided in Section 3.4, here are some hints on what to do under such circumstances.

- Document the status of the computer by taking a photograph.
- Look and listen for signs that the computer is powered on. Listen for the sound of fans running, drives spinning, or check to see if light emitting diodes (LEDs) are on.
- Try to move the mouse, but do not push any buttons.
- Observe the screen for any indications of a screensaver or login screen.
- Document the status of the screen by taking a photograph.

If the computer turns out to be on, but a screensaver is appearing, the first things to do are:

- Observe the screen while moving the mouse;
- If a screensaver disappears and you get access to the system without being prompted for a password you can proceed with the next Live Data Forensics steps (if you are fully trained and competent to do so);
- If the screensaver is locked with a password ask the suspect, check if the password hint is activated in the screensaver interface, look for notes or other clues. If the password is obtained, then disable and proceed with the next Live Data Forensics steps.
- If you do not discover the password, there are techniques to acquire the RAM via FireWire and Thunderbolt interfaces or with the 'cold boot' method. These techniques should only be used by Live Data Forensics specialists.
- **In any of these cases: Document the status of the screen by taking a photograph.**

If the computer is turned on, but not protected by a screensaver or authentication screen or you were able to obtain the password:

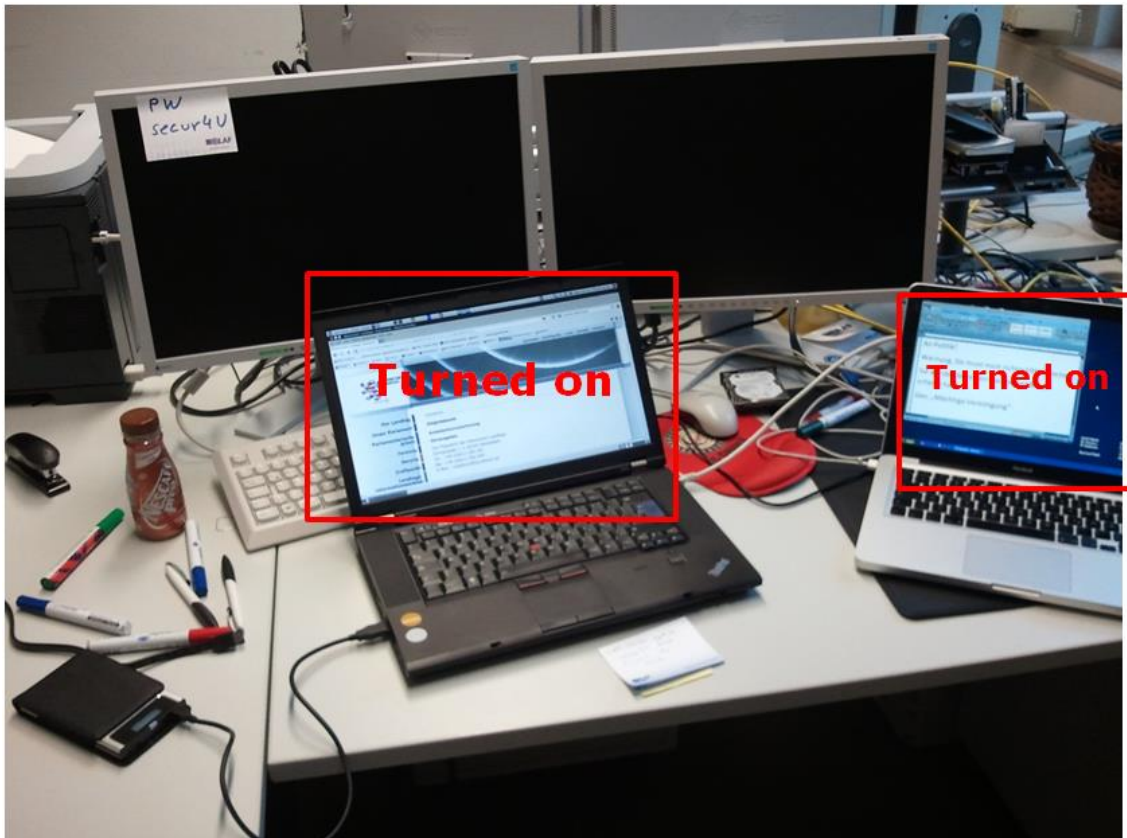
- Check the display screen for signs that digital evidence is being destroyed. Words to look out for include "delete," "format," "remove," "copy," "move," "cut," or "wipe";
- Look for signs of encryption being used (described later on);

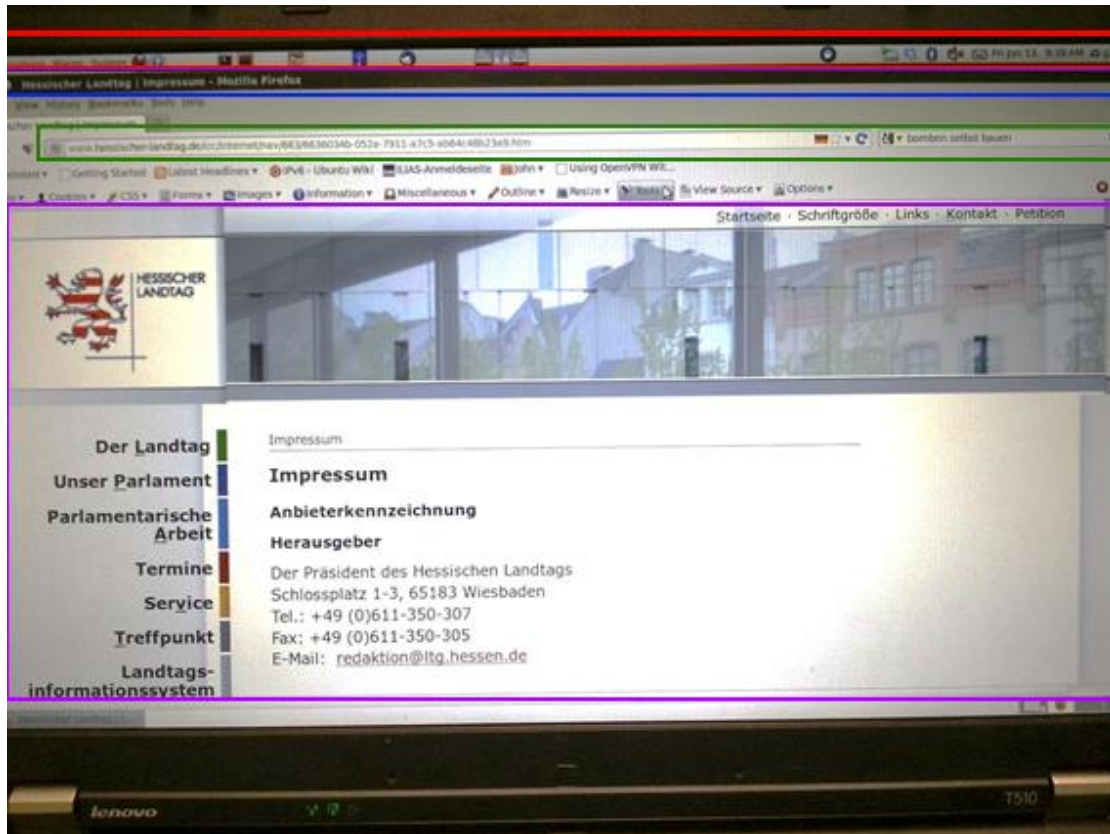
Restricted


- Look for signs that the computer is being accessed from a remote computer or device;
- Look for signs that cloud services are being used (described in 3.5.3.1.);
- Look for signs of active or ongoing communications with other computers or users such as instant messaging windows or chat rooms;
- Look for signs that cameras or web cameras (web cams) are active;
- Keep moving the mouse to avoid a screensaver or lock becoming activated;
- Look for signs of virtual machines being powered on and perhaps being in full screen mode;
- **In all of these cases: Document the status of the screen by taking a photograph.**

There is no Standard Operation Procedure for Live Data Forensics that covers each and every situation. As each search is different the experienced examiner will have to choose appropriate measures based on the circumstances. A flowchart on some of the basic procedures can be found in **Appendix B**:

To aid a better understanding of what might be seen on a computer screen, here are some photographs from simulated search and seizure scenarios.





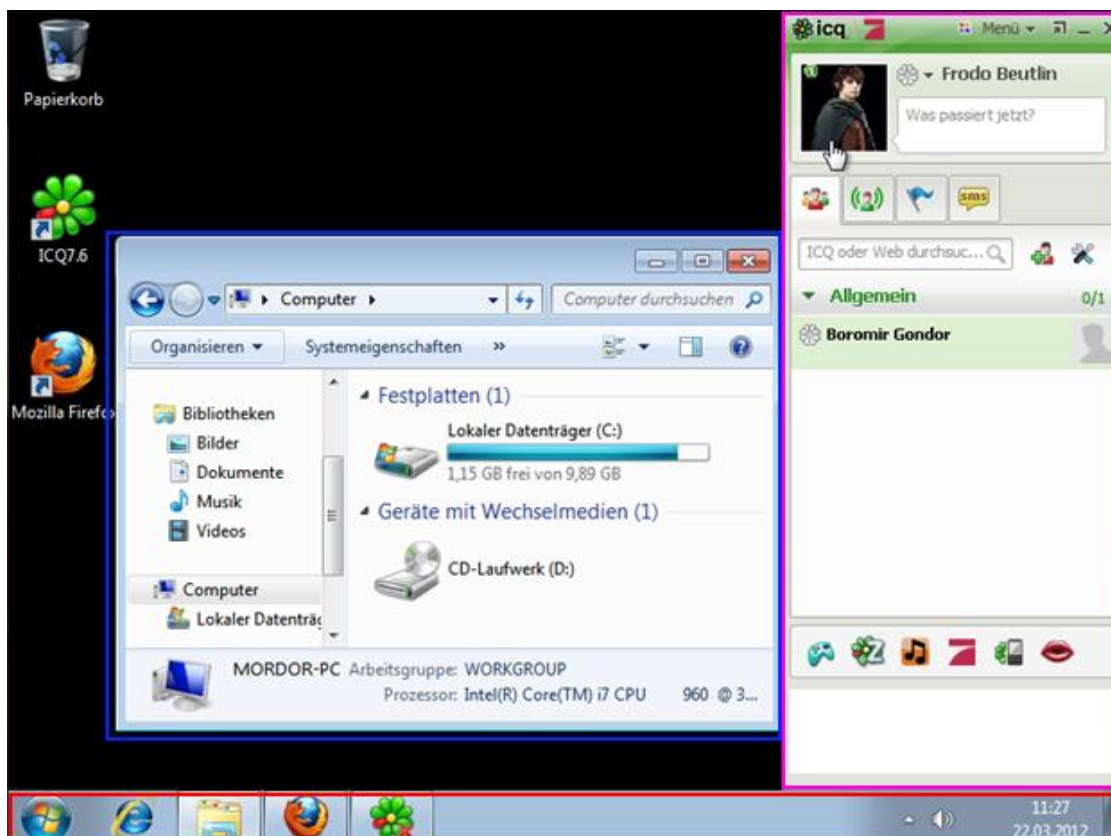
This is a laptop running the "Ubuntu" Linux operating system with the "Gnome" Graphical User Interface (GUI)³⁹. The red rectangle at the top of the image shows the task bar with a program menu (on the left), shortcuts (in the centre) and tray icons and clock (on the right). Although hard to see in the image, an attentive investigator might have noticed the small TrueCrypt icon  in the middle of the shortcuts.

The blue rectangle shows the title bar of the currently opened window. In this case it shows the currently opened webpage and that "Mozilla Firefox", an Internet browser, is open!

The green rectangle shows the URL (Uniform Resource Locator) on the left and the search box for Google search on the right. The search box might be of interest. Normally these data are also stored on disk and might not appear to be part of Live Forensics, but modern browsers can be configured to delete or even not to record search history or other browser information.

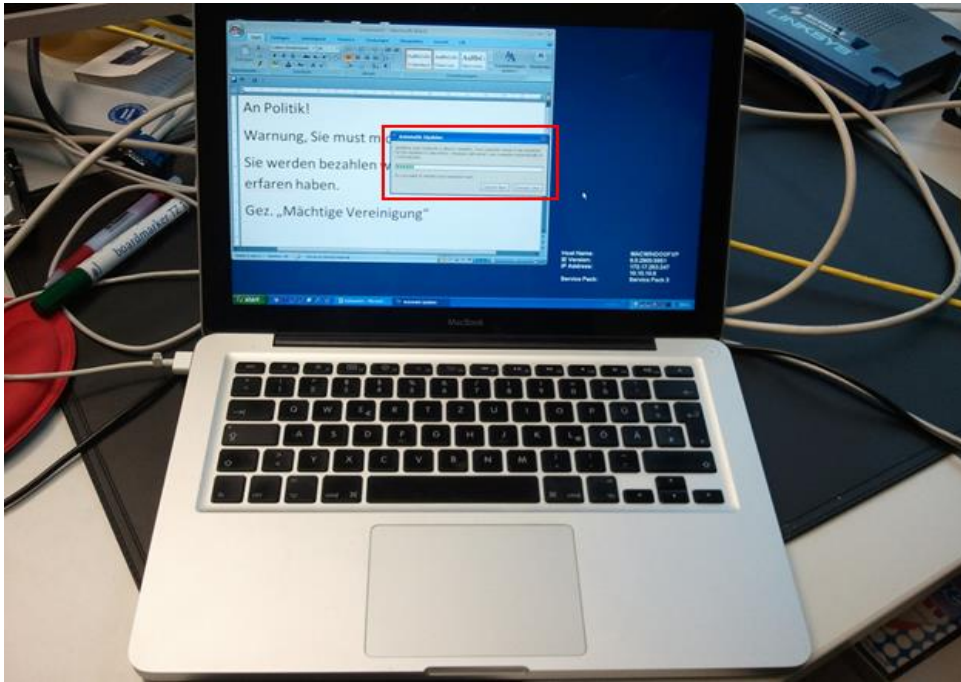
The purple rectangle shows a website has been opened.

³⁹ A Graphical User Interface or GUI is the name given to the user friendly representation on a computer screen of how the user interacts with the computer through images and icons.

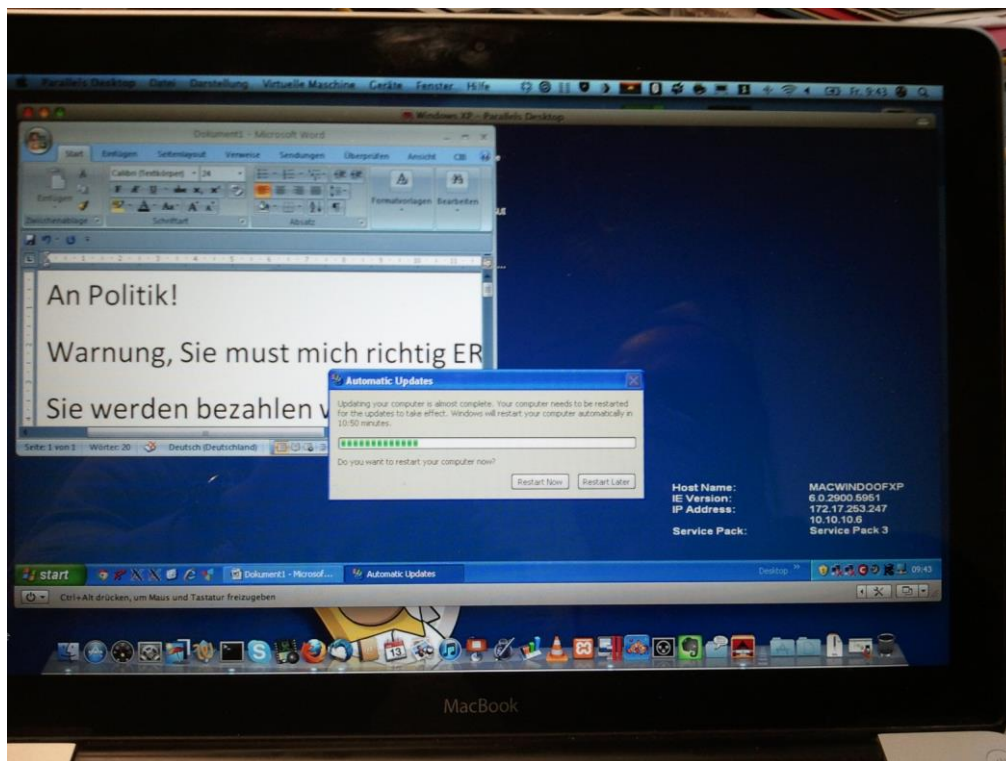


This Computer is running Windows 7. The red rectangle shows the task bar with a program menu and shortcuts (on the left), the active windows (centre) and tray icons and clock (right). The active programs from the shortcuts can easily be identified as they are highlighted. In this case, Windows Explorer (blue rectangle), Mozilla Firefox and ICQ⁴⁰ (pink rectangle) are open, although Firefox cannot be seen on screen.

⁴⁰ ICQ is an instant messaging application.



This picture shows a laptop, which appears to be a MacBook. On a MacBook an investigator would expect the MAC OS X operating system to run, but in this case the machine appears to be running Windows XP. Particular attention should be given to the progress bar in the middle of the screen. A progress bar indicates that there might be a process running. In this case it is a normal Windows update process that would restart the computer if the investigator did not react promptly. This could mean that the document shown in the screen, but which has not yet been saved to the disk could be lost forever.



A closer look at the laptop reveals that it is actually running Windows XP inside a virtual machine, so the chances of recovering that document would even be worse. Of course, having realised this, an investigator would perform live data forensics on both machines, the virtual one and the MacBook 'host'.

When conducting live data forensics in scenarios like those in the photographs, changes to the system are unavoidable. Live examination involves using tools on the live system that will inevitably make changes to it. The examiner must, however, seek to capture as much of the volatile data as possible while leaving as small a footprint of his or her actions as possible.

The order in which data capture is undertaken could also be crucial and the examiner should carefully consider the order of data collection. Although every search and seizure scenario will entail case-specific considerations, a predefined methodology based on the order of volatility is recommended.

Writing a simple program (e.g. in Bash (Linux), Batch (Windows) or Python) can be used to establish a standardised workflow. Existing frameworks with additional functionality like Microsoft COFEE (available via Interpol) can support an investigator if he is not trained in programming.

Restricted

For investigators searching for the right tools to acquire volatile data Kuhlee and Voelzow⁴¹ have created a list of program fragments and tools to help:



| Volatile fragment | Windows Tools | Linux Tools |
|---|---|---|
| Contents of computer memory (RAM) | Dumpit, Winen, Mdd | dd, fmem |
| Routing-Tables, ARP caches, Kernel statistics | Route PRINT, arp -a, netstat | netstat -r -n route arp -a |
| DNS Cache | Ipconfig /displaydns | rndc dumpdb (if installed) |
| Process lists | PsList, ListDLLs, CurrProcess, tasklist | ps -ef, lsof |
| Active network connections (sockets) | netstat -a | netstat -a, ifconfig |
| Programs/services using network connections | sc queryex, netstat -ab | netstat -tunp |
| Open files | Handle, PsFile, Openfiles, net file | lsof, fuser |
| Network shares | Net share, Dumpsec | showmount -e, showmount -a smbclient -L |
| Open ports | OpenPorts, ports, netstat -an | netstat -an, lsof |
| Currently logged-in users | Psloggedon, whoami, ntlast, netusers /l | w, who -T, last |
| Mounted encrypted filesystems | Manage-bde (Bitlocker), efsinfo (EFS) | mount -v, ls /media |
| Temporarily connected filesystems | Fsinfo, reg (Mounted Devices) | mount -v, ls /media |
| Remote logging- and monitoring data | psloglist | /etc/syslog.conf Port UDP 514 |
| Physical configuration, network topology | Systeminfo, msinfo32, ipconfig /all | ifconfig -a netstat -in |
| Storage media | reg (Mounted Devices), Net | mount -v, |

⁴¹ Kuhlee and Voelzow (2012), *Computer Forensik Hacks*, O'Reilly, ISBN 978-3-86899-121-5, <http://www.forensikhacks.de>

Restricted

| Volatile fragment | Windows Tools | Linux Tools |
|---|------------------------------------|-----------------------------|
| | share, netstat -a | ls /media |
| System clock (to determine the offset to radio clock) | time /T, date /T, uptime | time, date, uptime |
| Environment variables | cmd /c set | env, set |
| Clipboard | Pclip | |
| Contents of disks | FTK Imager, EnCase, Tableau Imager | Dc3dd, ewfacquire, Guymager |

Many of these tools can be found either in the Sysinternals⁴² suite by Microsoft or for Linux in the CERT repository.⁴³ The list is by no means exhaustive. On Linux systems for example the investigator should always consider also acquiring the volatile information stored in the virtual /proc filesystem.

When composing a set of live data forensics tools the investigator should consider the following:

- Only select tools with least impact on the system. For acquiring RAM for example a small tool like "WinPMem⁴⁴" is to be preferred to a heavyweight graphical tool like "FTK Imager".
- The tool should come with its own executables so that the investigator can run the tool without using untrusted binaries⁴⁵ from the system. The investigator should also only use tools and scripts functionality of which s/he can explain in court.
- The tool/script should be automated and not require a lot of user interaction. The investigator will not remember all options for all commands nor will s/he be able to monitor every process across multiple devices.
- In company environments the tools should include a triage functionality providing the investigator with enough information to determine if an incident has occurred.
- The tool should only gather data that are volatile. It is not necessary to acquire data that can also be found on the hard drive of the computer once it has been analysed.

There are also some preconfigured Forensics DVDs available which come with a broad range of live forensics tools. Although it is highly recommended that the investigator create his or her own set of tools adapted to his or her personal needs, cases and legislation, these DVDs can provide a good idea of which tools to incorporate into his or her personal toolbox and may also be a good alternative for investigators starting out in the field of Live Data Forensics.

⁴² <http://technet.microsoft.com/en-gb/sysinternals>

⁴³ <http://www.cert.org/forensics/tools/>

⁴⁴ <https://code.google.com/p/volatility/source/browse/branches/scudette/tools/windows/winpmem/>

⁴⁵ A 'binary' file is a computer program that can be executed by the computer.

PALADIN Live-CD, Sumuri Forensics, <http://sumuri.com/index.php/joomla/weblinks>



Raptor Live-CD, Forward Discovery, <http://forwarddiscovery.com/Raptor>



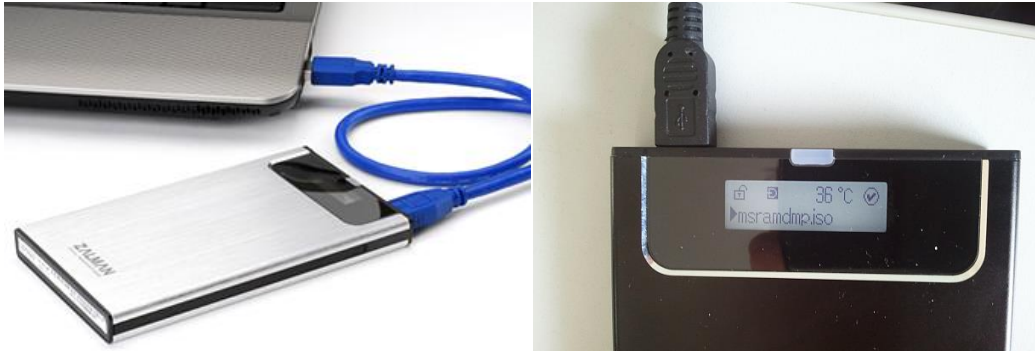
Further Advice

When investigators conduct live data forensics on a system they should never store the acquired data on the storage media of the target computer, but should connect forensically prepared external storage media. In addition to ensuring a reserve of this external storage media, other devices containing live data forensics tools should be prepared and ready for use.

Options for storage devices include:

- **USB Sticks:** These are very fast and reliable, but USB sticks with a memory capacities equivalent to the amount of RAM are needed;
- **External Hard Disk Drives (HDDs):** This kind of option should be chosen whenever large volumes of memory are to be copied. Models with a range of possible connectors (USB/eSATA/FW) are more flexible.
- **DVDs:** Ideal for live data forensics tools to be used on the target system. The write protection of DVD-Rs protects the trusted binaries (programs) from being altered.

- **External HDDs with virtual DVDs:** These combine the advantages of both with the fast accessible, reliable storage of the external hard-drive and the write protection of DVD-ROM. An investigator can save his or her forensic boot disks as ISO⁴⁶ files in a special folder and mount⁴⁷ them as a virtual DVD-ROM without the risk of affecting validated binaries.⁴⁸ One example of such a device is the Zalman ZM-VE300 (USB 3.0).



In preparing the acquisition media and live data forensics tools the investigator should consider the following:

- Format your media with NTFS⁴⁹ (due to filesize and amount-limitations of the FAT⁵⁰ file system);
- Consider preparing a second set of media with a different filesystem format (e.g. EXT4 for systems that do not have support of NTFS);
- Expect and prepare for multiple operation systems like Windows, Mac and Linux;
- Validate your trusted binaries beforehand⁵¹;
- Test the proper functionality of your boot-DVD⁵²/ HDD setup;
- Be sure you know your tools BEFORE you search the premises;
- Bring enough storage space;
- Avoid cross-contamination by wiping your destination drives before every search;
- Use a flat folder structure to limit impact on RAM.



3.5.2.1 Encryption

Encryption, especially 'full disk encryption' is becoming more popular not only for people wanting to hide criminal activities, but also for companies with commercially sensitive or proprietary

⁴⁶ An ISO file is like a box that contains a complete copy, archive or image of a disk.

⁴⁷ i.e. make them accessible to the system.

⁴⁸ Kinds of programs that are guaranteed not to have been corrupted.

⁴⁹ NTFS stands for New Technology File System and is a way of filing and arranging Windows files.

⁵⁰ FAT stands for File Allocation System for keeping track of files stored on a hard drive.

⁵¹ In other words, make sure the software tools you will be using have been tested and are accurate.

⁵² A boot-DVD is the DVD that you use to 'boot' or load an operating system or utility (useful) program..

Restricted

information and the need to protect personal data. Often company policies will require all mobile devices including (external media and laptops) to be encrypted using software like Microsoft Bitlocker, Steganos, PGP, etc. Nowadays hardware vendors will also include encryption options in their laptops and hard drives.

Once the encryption on a hard drive has been activated it may be too late for the investigation. Strong encryption needs specialized crypto clusters and a lot of time to be able to decrypt and even then it may not be possible. In the worst case, encryption will prevent any data from being analysed rendering even the biggest hard drives, with terabytes of information, worthless.

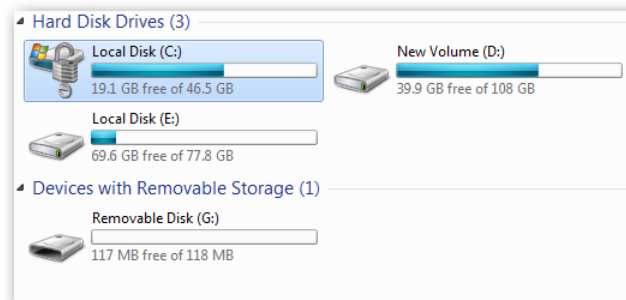
So how would the investigator prevent a disk from being encrypted? How can encryption be detected and what should be done when encryption is encountered?

A good starting point is to look for visible signs of encryption software being used. Typical software names are, as mentioned above, Microsoft Bitlocker, Truecrypt, Steganos, PGP and their icons might be seen.



Example of tray items of encryption software

Traces of encryption software can also be found in the running processes, in the installed software dialog, the registry (e.g. mounted devices, installed software, associated file extensions) and also in the Windows Explorer.



Microsoft Bitlocker encrypted disk in Windows Explorer view



When Microsoft Bitlocker has been used the operating system can give the investigator information about mounted encrypted drives by entering the following command⁵³:

manage-bde -status

If the investigator sees clues that encryption is being used s/he should proceed as follows:

⁵³ A command is an instruction direct to the operating system of a computer.

- If you find that encrypted disks or containers are still mounted in the system, copy them while you still have access to that live system;
- In case of Bitlocker being used to mount an encrypted volume, save the 48-digit Recovery Key by using the command:

manage-bde -protectors -get <volume name>

- After that, copy the files. If the encrypted volumes or containers are not mounted and are still encrypted, ask the suspect for the password, the decryption keys/media and how on how to decrypt the files (remembering that a suspect may attempt to give false information);
- If questioning is successful, decrypt the data and copy them;
- Be sure that no screensaver, low battery or energy saving feature interrupts and interferes with the saving of the encrypted files.



Important: Successful decryption may not only depend on passwords, but also on Trusted Platform Module (TPM) chips within the systems hardware, on keyfiles stored locally or on external media (such as a USB Key). If two step authentication has been used, having the password will be pointless unless the second component is found. That is why it is so important to seize all sources of digital evidence at the premises.



Important: In the case of TrueCrypt⁵⁴ Full Disk Encryption it is possible to split the hard drive into two parts with two different passwords - one part containing all the secret data, the other part containing only unimportant data. The developers included this feature to cater for the situation in which the user is forced to give out his password against his will. To show his cooperation and avoid punishment the user should reveal the password to the outer part only containing the unimportant data. The investigator should always check if the size of all the volumes shown matches the full size of the media.

The procedures described above can be found in **Appendix B**.



3.5.3 Remote access

As mentioned before, an investigator conducting a search with running systems does not only have to deal with volatile data stored locally within the components of the computer, but also with transient data that might be stored outside of the running PC. In corporate environments in particular it is possible to find network infrastructures with user data hosted (stored) on centralized servers shared between different entities in the network group. Most of the time the company's servers cannot be shut down and hardware cannot be seized due to the company's operational constraints and commercial liabilities. There may also be a privacy constraint. Most of the time a warrant or court order permitting the search will only cover the acquisition of data that belong to the suspect or the data to which the suspect had access. Imaging the whole server or on a shared system would include data not covered in the judicial permission would not be an option.

⁵⁴ TrueCrypt has now been discontinued, but may still be encountered.

A good way to approach such commercial scenarios is to seek the cooperation and consent of those responsible (as long as they are not in any way implicated in the investigation). When searching the systems of bigger companies it is good practice for the lead investigator to organize a meeting with the head of the company, a representative of the legal department and a representative from the company's IT infrastructure department. In these meetings the next step involving a search warrant should be planned with the cooperation of all parties involved. Subsection 3.5.4 covers the value of a system administrator's permission in more detail.

In most situations the investigator will be dealing with either dwellings or small to medium-sized enterprises. In such cases, the network may comprise of some single computers in a network and a server containing the central database for the company's accounting software, allocation of shares for workgroups, some home directories⁵⁵ and perhaps an exchange server for emails.

An investigator conducting Live Data Forensics in such an environment should always ask for the cooperation of the person responsible for the network infrastructure (if that person is not a suspect). The bigger the network the more this kind of support is needed because the person who has set up the infrastructure and administers it on a daily basis knows best which resources to which the suspect might have had access. However the investigator needs to stay sceptical and make his or her own decisions and conclusions. He or she must bear in mind that the person from whom they have asked help might be a friend of the suspect.

The routers and firewalls can give the investigator an insight into network configuration through their Access Control Lists (ACLs) or security rule sets.⁵⁶ This may be achieved by viewing the configuration screens as an administrator of the device, but will require the user names and passwords previously found or obtained at the time of seizure. The Tool DVDs mentioned in the preceding section also include a variety of network reconnaissance tools. It is good practice to draw a diagram of the network infrastructure. This will help the investigator to understand and remember more effectively connections between the computer and the rest of the network.

If the suspect's computer is turned on and other volatile data have been captured, the investigator should look for any clues that data is being stored remotely. This can include:

- Shared folders on other network computers;
- Mapped network drives from a server;⁵⁷
- E-Mails stored on an IMAP or Exchange server;
- Cloud services and online storage.

⁵⁵ A place where files are stored for particular users.

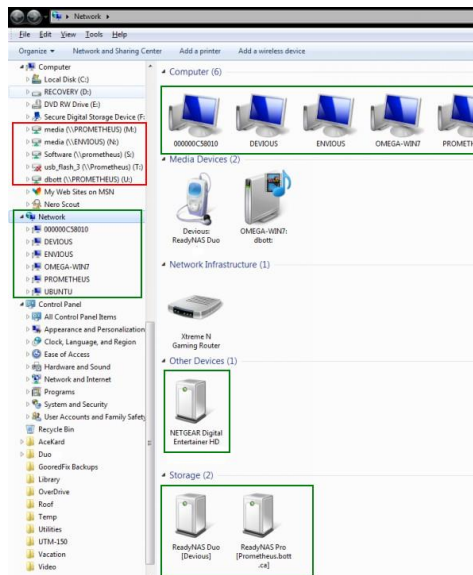
⁵⁶ The set of rules established for securing the network and governing its range of use.

⁵⁷ Drive mapping is the way a network assigns drives (reserved space) across a network to different computers sharing storage.

Restricted



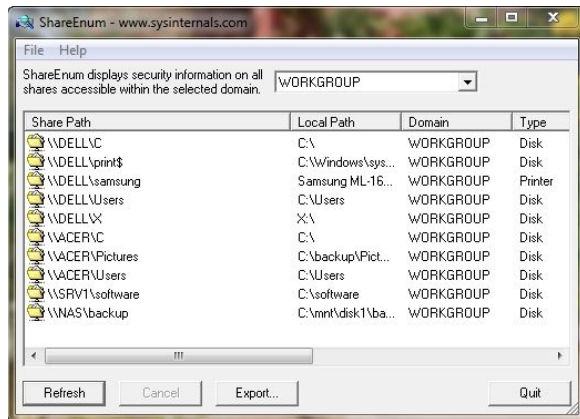
Shared folders on other network computers and also mapped network drives from a server can be investigated either by simply looking for them in Windows Explorer or by using the free tool ShareEnum from the Sysinternals suite.⁵⁸ Both approaches can be seen below:



Windows Explorer view:

Green: Network Devices with Shares,

Red: Mapped Network Drives



ShareEnum from SysInternals

When such an arrangement has been discovered, the investigator should copy these shares. Indeed, if possible, the investigator should think about making an image (i.e. an exact clone) of the computers where these shares are located because an ordinary copy will not include deleted files nor the unallocated 'slack space' on the drive.

E-Mails stored remotely on an IMAP⁵⁹ or Exchange Server can be located by analysing the account settings of the corresponding e-mail clients. For POP3 and even for IMAP accounts – depending on the settings – there will be local databases. Such databases are not volatile and do not need to be seized in live forensics. If there is no local database file the investigator should try to save the contents of the e-mail account directly from the exchange server or assign the host of the account to do so.

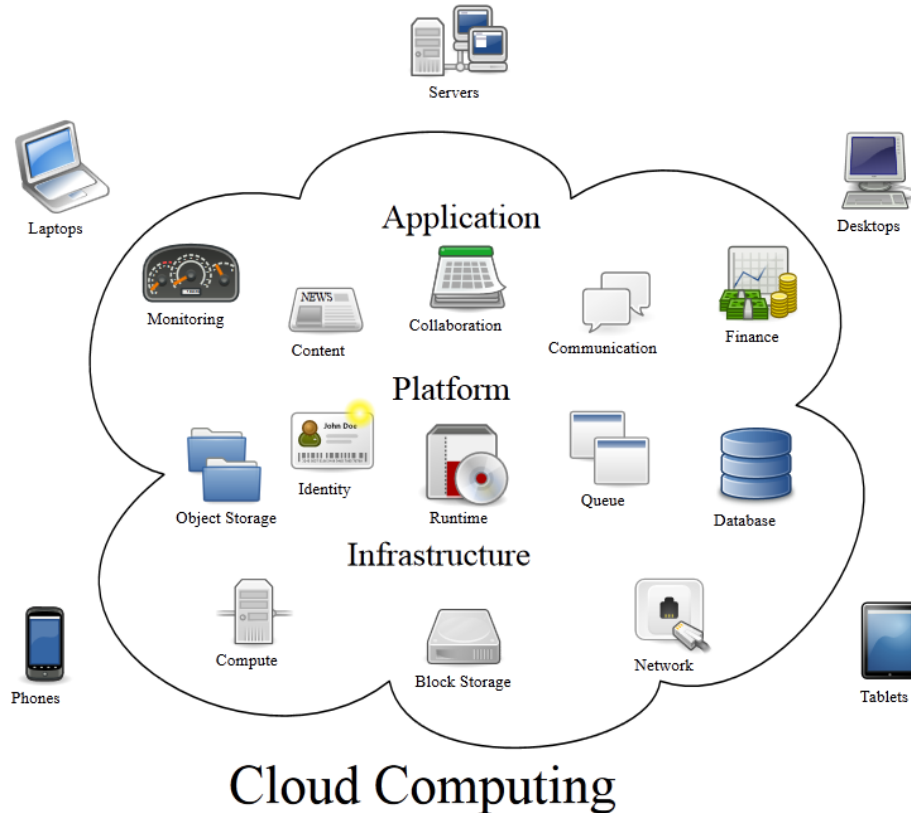
⁵⁸ <http://technet.microsoft.com/de-de/sysinternals/bb897442>

⁵⁹ IMAP stands for Internet Message Access Protocol



3.5.3.1 Cloud Computing

Cloud services and online storage is a topic that is becoming of significant importance. To be able to recognize and understand these services the investigator needs to know what cloud computing is, which kinds of services are available and how they work. The following graphic and definition give a useful overview.



Graphic source: Sam Johnston, Wikipedia.com

Definition of Cloud Computing

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.⁶⁰

Mell and Grance from the National Institute of Standards and Technology (NIST) identify three service models for Cloud Computing.⁶¹

Software as a Service (SaaS): The consumer is provided with the capability of using the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure (including the network, servers, operating systems or storage) or even individual applications, with the possible exception of limited user-specific application settings.


Platform as a Service (PaaS): The consumer is provided with the capability of deploying consumer-created or acquired applications onto the cloud infrastructure created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure (including the network, servers, operating systems, or storage), but does have control over the applications deployed and possibly over the configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS): The consumer is provided with processing, storage, network, and other fundamental computing resources and is able to deploy and run arbitrary software (including operating systems and applications). The consumer does not manage or control the underlying cloud infrastructure, but has 'broad freedom to choose' operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g. host firewalls).

⁶⁰ Mell and Grance, NIST, 2011, <http://csrc.nist.gov/publications/PubsSPs.html#800-145>


⁶¹ Mell and Grance, NIST, 2011, <http://csrc.nist.gov/publications/PubsSPs.html#800-145>

Some examples of cloud and online storage services:



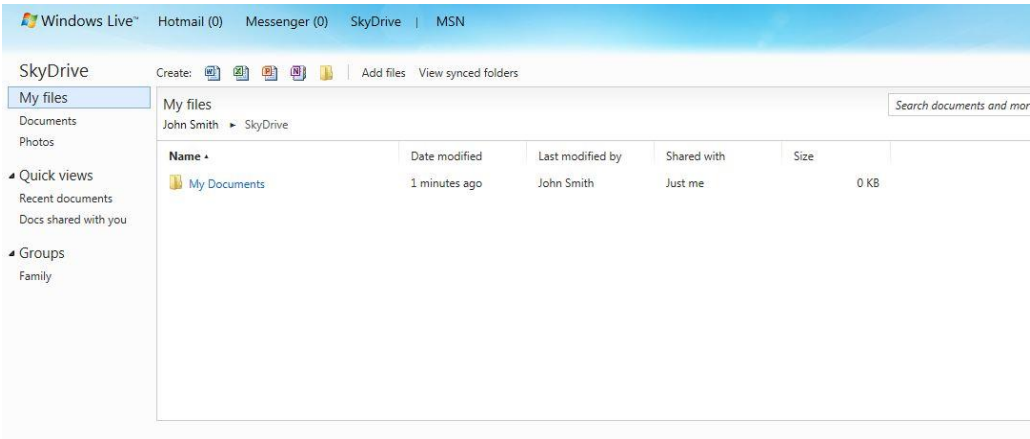
Amazon offers a wide variety of web services. Their Elastic Compute Cloud (EC2) is one of the biggest cloud services world-wide. They offer typical IaaS services. <http://aws.amazon.com/en/ec2/>

| Region: | | Linux/UNIX Usage | Windows Usage |
|----------------------------------|--|------------------|------------------|
| US East (Virginia) | | | |
| US East (Virginia) | | | |
| US West (Oregon) | | | |
| US West (Northern California) | | | |
| EU (Ireland) | | | |
| Asia Pacific (Singapore) | | | |
| Asia Pacific (Tokyo) | | | |
| South America (Sao Paulo) | | | |
| Standard | | | |
| Small (Default) | | \$0.080 per Hour | \$0.115 per Hour |
| Medium | | \$0.160 per Hour | \$0.230 per Hour |
| Large | | \$0.320 per Hour | \$0.460 per Hour |
| Extra Large | | \$0.640 per Hour | \$0.920 per Hour |
| Micro On-Demand Instances | | | |
| Micro | | \$0.020 per Hour | \$0.030 per Hour |



Microsoft OneDrive offers their customers large amounts of online storage with Microsoft Office integration.

URL: <https://onedrive.live.com>





Google Docs offers large amounts of free online storage for documents. They offer multi-user Wysiwyg (what you see is what you get) editors for creating spreadsheets, text-documents, presentations etc., within the browser.

URL: <https://docs.google.com/>



Docs

Create and share your work online

Upload your files from your desktop: It's easy to get started and it's free!

Access anywhere: Edit and view your docs from any computer or smart phone.

Share your work: Real-time collaboration means work gets done more quickly.



Google drive offers a limited amount of free online storage amounts of free online storage that can be upgraded by paying a monthly fee. The user can upload, sync and share all kinds of data as well as access his or her Google docs documents.

URL: <https://drive.google.com/>





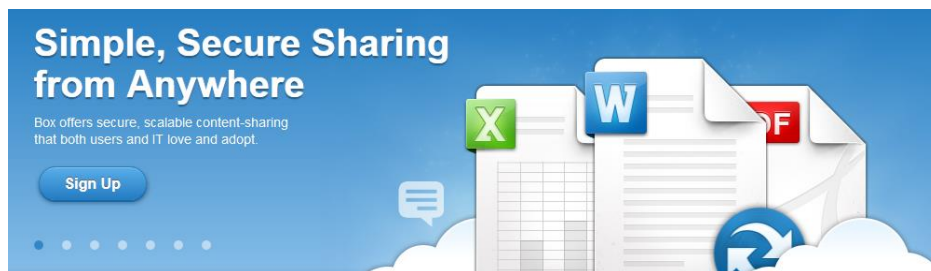
Dropbox offers a limited amount of free online storage that can be expanded by purchasing professional plans. Their specialty is the synchronization of files among a wide range of different devices operation systems such as Windows, Linux, Mac OS X, iOS, Android, etc.

URL: <https://www.dropbox.com>



Box is similar to Dropbox offering a limited online storage capacity that can be extended by purchasing professional plans. They also offer strong synchronization possibilities as well as collaboration features.

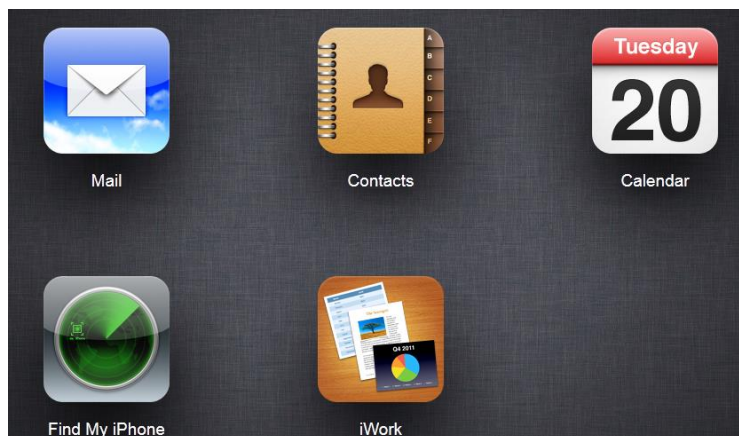
URL: <https://www.box.com>





Apple offers its customers free limited, extendible storage in the iCloud. This service is able to synchronize data among Apple devices and computers running the iTunes software.

URL: <https://www.icloud.com>



The strength of Sugarsync is in the synchronization among a range of different devices. They also offer a free limited storage space that can be extended by purchasing professional plans.

URL: <https://www.sugarsync.com/>



A full list of online storage providers and cloud providers can be found on Wikipedia:

Restricted

62

The interesting aspect about cloud computing for the investigator is that data is not stored on a single physical computer, but on multiple servers. Most of the time even the provider of a cloud service cannot tell where certain data are stored. The other interesting aspect is that cloud services are able to replace almost every part of a company's IT infrastructure, starting with software services like word-processing or accounting software through to the complete replacement of all employee workstations.

Consequently there will be situations where not a single byte of data can be retrieved from a company's computers because they will merely be 'thin clients'⁶³ without any storage 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.

If an investigator is confronted by a running system with network access and suspects that cloud computing is involved, s/he should:

- Look for tray icons that look anything like the logos of the services mentioned above;
- Check installed software for cloud services;
- Look in the process list for names of cloud services;
- Look for network shares and mapped network drives;

⁶² http://en.wikipedia.org/wiki/Comparison_of_online_backup_services.

⁶³ A 'thin client' is effectively just a portal for accessing computer programs that are operating in another remote location. Nothing actually happens on the computer itself.

- Observe the network traffic;
- Monitor the list of open or listening sockets for suspicious activity;
- Acquire any data that appear to be stored remotely. Even though an online storage service might synchronise data to the hard drive of the computer, that synchronisation should never be trusted.

After the investigator has acquired all volatile data and transient data, s/he can proceed in the following way:

- Remove the power supply cable from the target equipment and record the time of doing so (**do not** switch it off at the wall socket because the computer system may have an uninterruptible power supply (UPS)).
- Remove the storage media from the corresponding drives; place the media in their original boxes/jackets and label them accordingly. Insert either a seizure disk/CD or a blank floppy disk if available. **Do not** remove DVDs or touch any button on the DVD drive.
- Disconnect any modem attached (merely switching it off may not always be sufficient).
- If dealing with a portable device, also remove the battery pack. Remove the additional battery packs if applicable (N.B. Some portable devices have a second battery in the multipurpose bay instead of a DVD drive).



3.5.4 Administrator permission

Sometimes some or even all of a company's network resources will be managed by external companies and are hosted in remote locations. One problem with remote storage is that the investigator may not have the possibility to get there personally or be able to send other investigators to the other location. In such cases the cooperation of the remote system administrator can be invaluable. Depending on the circumstances it can be a good idea to organize a telephone/voice conference with the remote administrator and the head of the company and a representative of the legal department (if they are not thought to be involved in the matter under investigation).

In many cases administrators are not sure whether they are allowed to cooperate in an investigation. In law enforcement cases where the request has been made in compliance with the law, this can only be a problem if the remote location is in a different country with different legal rules and procedure. Things can be made easier if the head of the company owning the data is able to get clearance from the legal department and authorises the administrator to cooperate with the investigation.

"Cooperation" in such cases does not mean that the remote administrator will do all the acquisition work. The opposite is the case: the administrator should be allowed as little access to the system as necessary while the investigators should search and acquire all evidential data themselves. The administrator's cooperation is only needed for information about the infrastructure and to grant

Restricted

access rights to certain areas of a server, workstation or software functions. A big enterprise might also have e-discovery solutions in place. The investigator should specifically ask for this because it will allow him or her undetected remote searches and access to acquire certain or all company systems (even including the volatile data).



4 Capturing evidence from the Internet

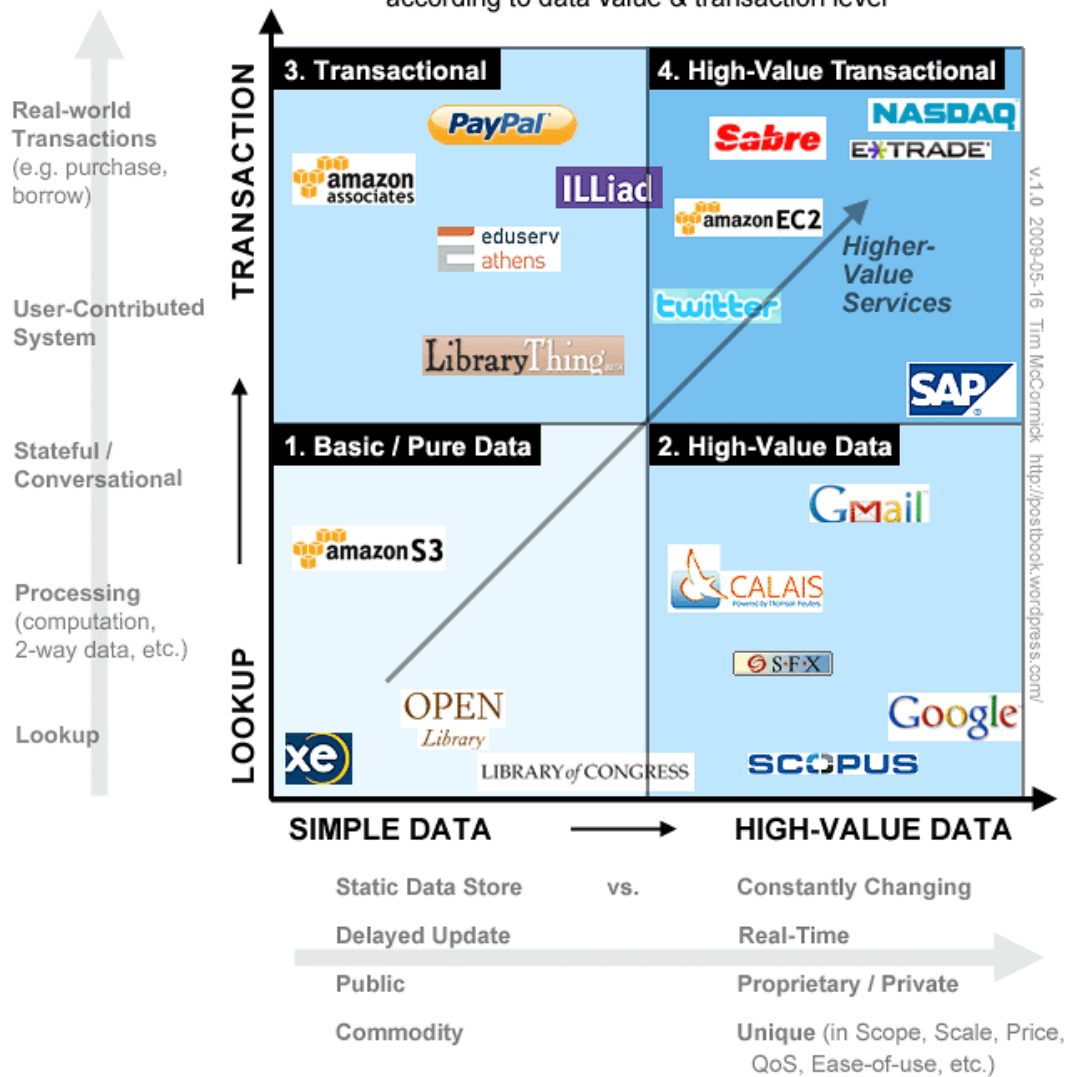
In this chapter we will delve into the technical and methodological procedures involved in the acquisition of online evidence. We will stress aspects such as the “transparency” and “quality” of acquired evidence as those characteristics will eventually play a major role later on as the admissibility of your evidence becomes questioned. The chapter deals with the acquisition of evidence from publicly available information on the Internet as well as issues involved in covert Internet investigations. The latter is much more complicated because legislation and practice varies significantly between jurisdictions. Conducting such investigations requires additional knowledge and skill sets than those required to conduct the activities outlined in Chapter 3.

Regarding the admissibility of evidence, this document will not assume a given legal framework of reference and will not, therefore, rely on a particular regime of legal regulation. The general approach will allow readers to understand the reasoning behind the acquisition process, which, in turn, should enable them to adapt the general concepts to available resources and relevant legislation. The investigator should be especially conscious that any evidence acquired today for intended use in a given country and legal framework, might well be required elsewhere in the future.

Last, but not least, the reader is advised that this chapter will require a slightly higher technical background than the previous chapters on this Guide. Those with little technical background are nonetheless invited to read this material to grasp its general concepts. This will enable them to expect and ensure that other technical specialists on the team will use a valid acquisition methodology.

A Web Services Taxonomy

according to data value & transaction level



A Web Service Taxonomy⁶⁴

4.1 Websites as a “Mashup” of Evidence

According to a current Wikipedia article:

“The main characteristics of the mashup are combination, visualization, and aggregation... [...] In the past years [sic], more and more Web applications have published APIs⁶⁵ that enable software developers to easily integrate data and functions instead of building them by themselves.”

⁶⁴ Chart by Tim McCormick http://tjm.org/wp-content/uploads/2009/05/web-services-taxonomy-chart_23.gif

⁶⁵ Application Program Interface (API) is a set of commands, functions, and protocols which programmers can use when building software for a specific operating system. Source: www.techterms.com/definition/api

To apply this mashup concept to Internet investigations, the investigator could consider a web service that stores raw data on Amazon S3⁶⁶, uses Facebook authentication, payments through PayPal⁶⁷ and provides realtime “push” information on relevant activity through Twitter to its subscribed users. Such an online service would “mash-up” a broad range of sub-services (or related websites). What is even more important for us, online evidence would also be scattered across these sub-service/providers/companies. Welcome to the real world scenario of online evidence gathering!

This “mashing-up” example is extremely common on the Internet and although it might seem at first sight hard work to have to “harvest” evidence from all those different sources, it can sometimes turn out that it provides the investigator with data of greater evidentiary value: there is no single source of evidence (company) with vested interests in the potential outcome of your investigation. The mashup quality of many online services can in turn produce many “third parties” involved in any given transaction, this, as well see later, will help the investigator produce evidence with a greater chance of being relied upon.

On other occasions the investigator will find that different online providers are able to corroborate a given fact from different and independent sources (although given the nature of the Internet, care must be taken that the facts are not all quoting a single source). Take for example an insider trading scenario in which Gmail receives a user name and password for ETrade Inc.⁶⁸ (an online trading company) which gets read from a machine with the IP address ‘X’. Minutes later XE.com (a currency exchange information portal) receives queries from that same IP address ‘X’ requesting certain exchange rates involved in your investigation. ETrade Inc. then starts to receive purchase orders again from that same IP address ‘X’. The investigator can now call upon ETrade logs, Gmail logs, and XE.com logs which will all corroborate each other with links to the same IP address.

All of this “Online Evidence” requires special procedures on acquisition to guarantee the admissibility of the resulting evidence.

4.2 Virtual vs Physical location



The Internet is a global network that connects computers throughout the world by means of devices and protocols. Although there are several organizations that establish regulations and standards, every single node in the global network can be an independent sub-network, whose design and maintenance is not dependent on any organization. The Internet can be accessed through many types of technologies and this broadens the horizon of services that can be offered through it.

⁶⁶ Amazon Simple Storage Service.

⁶⁷ A secure online payment system.

⁶⁸ This is an imaginary name used for the purposes of this document and has no connection to any real legal or natural person.

When dealing with online evidence the investigator must clearly differentiate and be able to translate the “*virtual*” world into the “*physical*” world and vice-versa. In the virtual world a “location” (*where* is my evidence?) is usually translated into something called a URI/URL⁶⁹ or ultimately an IP address. For those readers who require it, a simple and straightforward review of the technical background of things such as URL, DNS, and IP addresses follows. The technical reader may wish to skip this section.



4.2.1 IP (Internet Protocol) Address

The IP is the most established set of standard and rules used for sending or receiving data across the Internet. The IP Address is the most fundamental type of source of information available on the Internet. They show where data packages are to be delivered. There are two types of IP addresses, IPv4 (IP version 4, commonly referred to just as “IP”) and IPv6 (IP version 6) addresses. An IPv4 address consists of a sequence of four numbers separated by a dot “.”. Each number might take a value between 0 and 255. (Ex.: 192.168.1.252). An IPv6 address, on the other hand, consists of eight groups of four hexadecimal digits. Each group is separated by a colon (i.e. 2001:0db8:85a3:0042:0000:8a2e:0370:7334).

The Internet Assigned Numbers Authority (IANA) regulates IP addresses and coordinates the allocation of IP addresses through regional entities known as Regional Internet Registries (RIR):

- RIPE (Europe and some parts of Asia)
- APNIC (Asia, and the Pacific Region)
- ARIN (North America)
- LACNIC (Latin America and the Caribbean)
- AfriNIC (Africa)

The IANA has also defined address spaces to be allocated to private networks (i.e. local area networks). These spaces are:

10.0.0.0 to 10.255.255.255 – Class A

172.16.0.0 to 172.31.255.255 – Class B

192.168.0.0 to 192.168.255.255 – Class C

The process for assigning an IP address to an Internet Service Provider is fairly straightforward. IANA informs each regional entity about which IP addresses are available for applicants in their region. The Internet Service Providers (ISP) then request the assignment of IP addresses from their regional entity. Once an ISP has received a range of IP addresses, it can then proceed to distribute them among his customers (the end user) and the ISP will build the network for which it will be responsible.

⁶⁹ The Uniform Resource Identifier or Uniform Resource Locator is the string of characters that acts as a name for or address of a location on the World Wide Web.

In other words, IANA cuts the “cake” into big chunks, regional entities cut their piece again into multiple slices to distribute it among ISPs and ISPs then reduce their slice of the “cake” into teh crumbs which are individually leased to clients.

It is not possible to have two identical public IP addresses connected to the Internet at the exact same time. Like postal address in the real world, each participating machine has to be uniquely identified in order to send and receive data effectively. When a connection is made to the Internet by a computer at home, the ISP leases a unique IP address to that computer for the time of connection. This means that IP address will be associated with all Internet activities undertaken by that computer during that period of time. When the connection is cancelled, the IP address is reallocated to another computer.



4.2.2 Dynamic IP addresses vs static IP addresses

If some mathematics are applied to the concept of IPv4 addresses it becomes clear that there is a finite number of IPv4 addresses available. IPv4 addresses consist of a set of four numbers, and each number can only take a value between 0 and 255. This means that *only* 4.294.967.296 different combinations of unique IPv4 addresses are available globally. Since there are millions of computers, devices and people connecting to the Internet, 4 billion addresses are clearly going to be insufficient. This is why Internet Service Providers manage their IP-address pools using something called dynamic IPv4 addressing or by something called Carrier-grade NAT⁷⁰ (CGN) (i.e. making use of additional port addresses for each IP address). On the other hand, the IPv6 address format with its eight groups of four hexadecimal numbers means that there are enough IP addresses not only for each person on the world, but also for each and every device in their household (see section 4.2.3).

As mentioned before, each Internet Service Provider has been assigned a range of IP addresses. In some cases, the number of IP addresses assigned to an ISP is smaller than the number of its customers. However, since it would not make commercial sense to restrict the number of clients to match their number of available addresses, technologies and protocols have been developed to solve this issue. The most common one is the Dynamic Host Configuration Protocol (DHCP).

DHCP is a protocol⁷¹ used to automatically assign a pool of IP addresses to a group of devices. The inner workings of this protocol are quite “simple”. When a device wants to connect to the Internet, it requests an IP address from its ISP. The ISP then consults its “available IP addresses list”. It checks which IP addresses are not assigned at that moment to another device and allocate one of those ‘free’ IP addresses to the requesting client (device). In doing so, the ISP registers the date and time and the client’s identity. As soon as the client logs off the Internet, that IP address goes back onto the “available IP addresses list” for allocation to another device. This means that a client or device may get a different IP address every time a connection is made to the Internet. On some occasions the IP address might even change a couple of times during a single session.

⁷⁰ This is a mechanism for maximizing the limited IPv4 addresses available.

⁷¹ i.e. A set of rules for devices to communicate with each other.

If a person's address were to change continuously in the real world, sending a letter to that person would be almost impossible as the post office would not know where to deliver it. On the Internet there are certain types of devices for which the IP address must be known at all times. In these cases, "Static IP addresses" are used. This means that the ISP assigns a specific IP address to a single device (customer) for as long as that the owner of that device stays as a client with that ISP.

Most ISPs keep a range of IP addresses to be used as Static IP addresses, and another range for Dynamic IP addresses. Either way, they always know to whom an IP address was assigned at a given time. Note that although most contracts for Internet access will be made with an organization or a person, IP addresses are assigned to devices and not to individuals.



When during an Internet investigation an IP address is detected, the investigators can ask the ISP (usually with an order from the court) the details of the device and service contract to which that IP address was assigned at the relevant time. It should be stressed that the investigator must be able to pinpoint with absolute precision the exact moment in which a given IP address becomes relevant for his investigation. Take a look at the following:

| When? | Pitfalls... |
|---|---|
| IP X.X.X.X on 24/05/2012 | During that single day, many different users could have been assigned that IP address |
| IP X.X.X.X on 24/05/2012 16:30:12h | Looks ok, but when is exactly "16:30:12h"? |
| IP X.X.X.X on 24/05/2012 16:30:12h (UTC-10) | This is the precise time. |

"UTC-10" pinpoints what is called the "time zone" which in this case translates to "**Coordinated Universal Time minus 10 hours**" (i.e. Hawaii). Requests to ISPs for IP addresses should always show the time zone.



4.2.3 IPv6

As seen above, the number of available IPv4 addresses is limited. We have been using IPv4 since 1982, but very recently IPv4 officially exhausted its unallocated address space. In other words, there are no more IPv4 addresses available. Thankfully IPv6 comes to the rescue! IPv6 does not have unlimited address space, but it is certainly extremely large:

340 undecillion, which is 340 trillion, trillion, trillion addresses (or 340,000,000,000,000,000,000,000,000,000,000,000,000,000,000).

IPv6 addresses are represented by a 128-bit number split up into blocks of 16-bit hexadecimal values each separated by a colon ":". Letters are not case sensitive and leading 0s (zeros) in a block can be omitted. For example, one of Google's IPv6 addresses is shown as:

2001:4860:b002::68, but when written in full the PI address is actually 2001:4860:b002:0000:0000:0000:0000:0068.

Each device or computer can now have its own unique IP address and this is likely to make an investigator's life easier. One of the most discussed benefits on IPv6 is the integration of Internet Protocol Security (IPSec)⁷² into the IPv6 standard. Specifically IPv6 provides (amongst other things) the following features: data confidentiality, data integrity, data origin authentication. All of this will sound like good or bad news depending on where you stand. For example, "data confidentiality" sounds good until it provides a freely encrypted channel for a suspect to send data, or until your NIDS (*Network Intrusion Detection System*) decides it can't do its job because most of the new IPv6 network is point-to-point encrypted.

The basic problems you'll encounter will be:

Those who delay IPv6 deployment. Some organizations are delaying the inevitable full-scale deployment of IPv6. In these cases the use of DHCP and Carrier-grade NAT technologies is growing rapidly. This can be a bad thing from a traceability point of view if there's not enough "book-keeping" done at the DHCP/NAT implementation level.

Those who are "testing" IPv6. Many ISPs have setup testing platforms for IPv6 as part of a controlled "roll-out" of the new system. These platforms usually connect the new IPv6 testing facility to a core network which runs in IPv4. Since the platform is only in a testing/partial roll-out, the record keeping is incomplete so that LEAs are only able to trace IP addresses up to where IPv4 meets IPv6.

Lazy ISPs. The Regional Internet Registries (RIR) have been putting some informal pressure on ISPs to keep their Whois⁷³ databases up to date. Assigning huge blocks of IPv6 addresses has limited the pressure that RIR have been able to bring. This means that Whois data may not be as reliable or easy to obtain as in the past.

New technology/old problems. As with any new system IPv6 is raising new security problems. For examples, there are new vulnerabilities in IPv6 stacks, firewalls are suddenly wide open because of incorrect IPv6 arrangements and configuration, IDSs (Intrusion Detection Systems) have not been updated to process IPv6, etc...

Digging out the trenches. Until IPv6 has been fully implemented, an investigator might be faced with IPv6 tunnelled through IPv4 or vice-versa! That is to say, an IPv6 packet might be encapsulated ("stuffed inside of") in one or more IPv4 packets or the other way round. Of course this will mix with every other tunnelling technology available out there so it's possible you find that IPv6 is riding on IPv4 which, in turn, rides over a VPN tunnel which might itself be further encapsulated onto other transport protocols. In other words,

⁷² Internet Protocol Security (IPSec) is a security framework allowing authentication and encryption over the internet.

⁷³ This is a database containing the ownership details of domain (website) addresses.

during the transition period, IP addresses may become masked and confused because of their interactions and therefore be difficult to trace.



4.2.4 DNS for Domain Name System

As previously discussed, in order to communicate with a certain node on the Internet, knowledge about its IP address is necessary. The problem is that humans are not very good at remembering combinations of four numbers separated by dots. If each device had a human-friendly address instead of a string of numbers, it would certainly make things easier for us. A protocol named DNS was created to allow this to happen.

Human-friendly addresses are usually known as Fully Qualified Domain Names (FQDNs) or 'domain names' for short and consist of an alphanumeric sequence in a particular format (for example, www.coe.int).

The Domain Name System (DNS) is a system that acts like a large dynamic phonebook and keeps track of which IP address (or addresses) has been assigned to which "name" and vice versa. The relationship is not always one name to one IP address (for instance, one name can be assigned to multiple IP addresses and the other way around).

Let us imagine an Internet service that needs to be always available. (Such services would include Internet search engines, online banking, webmail, etc.). To make sure that users can always connect to the service, the service provider creates multiple replicas of a website in different computers. Each one of these computers has a different IP address, but all of them can answer to a common name. On the other hand, there are also scenarios in which one single IP address answers to several domain names. Web hosting companies use this mechanism to reduce costs and management in preference to hosting every single domain on a different computer (i.e. with different IP addresses).

Domain names are managed by Registrars accredited by the Internet Corporation for Assigned Names and Numbers (ICANN; <http://www.icann.org/>) or by Registries listed by IANA (Internet Assigned Numbers Authority). For the Generic Top Level Domains (gTLDs) such as .com, .net, .org, .biz, etc the ICANN accredits Registrars themselves while for Country Code Top Level Domains (ccTLDs) like .us, .uk, .de, .ie, etc. IANA delegates the registration to local Registries like Nominet UK, Denic eG, IE Domain Registry Limited, etc.

If a domain name is not registered by a privacy protection company these Registries can reveal valuable information about the owner of a domain name. A list of the ICANN Registrars can be found on the ICANN website (<http://www.icann.org/registrar-reports/accredited-list.html>) while a list of all ccTLDs Registries can be found on the IANA website (<https://www.iana.org/domains/root/db/>).

As one can imagine there are millions of FQDNs out there and managing this huge database is an impossible task for one single machine. To simplify this task, the Domain Name System uses a tree structure to perform name resolutions (link the domains to the number of the IP address).

Each segment of a FQDN refers to a different “domain”. The last segment of a FQDN, after the full stop, is called the “Top Level Domain”. In the case of www.coe.int the “top level domain” is “int”. The next segment (the middle one) is known as the “second level domain” (i.e. “coe”) and finally the very front part of the string before the first full stop, is the hostname label of the machine (“www” in this case).

Taking this into account, the DNS is a very rich source of information for Internet-related investigations for two reasons:

- A registration contract is necessary for an FQDN to exist. Every contract must contain contact details of an administrator. Therefore, it is possible to find out which organization or person is in charge of that certain FQDN. Of course, this information might be false or protected by the domain registrar.
- Since FQDNs are later translated into IP addresses, it is also possible to link that IP address with an Internet access contract (because of the way IP addresses are distributed, as explained in the previous paragraph).



4.2.5 Uniform Resource Identifier (URI)

The URI is the label used to identify the location of a ‘resource’ or component in a computer system. URIs provide a way for a resource to be accessed by other devices on the same network. The most common URI is a webpage address and allows interaction across the World Wide Web.

The World Wide Web (WWW) is a system of linked documents (webpages) that can be accessed through the Internet (it is a network that uses the Internet, but is not synonymous with the Internet). Webpages use something called ‘hypertext’ that makes it possible to link or jump to other objects and pages (i.e. navigate the World Wide Web) and are usually written in HyperText Markup Language (HTML) code. Webpages are usually grouped together in what are known as Websites.

Using a software application known as a web browser (such as Microsoft’s Internet Explorer, Mozilla’s Firefox or Google Chrome) one can access the World Wide Web and, if the domain name or URL (see below) is known retrieve a particular webpage. These are usually hosted on Web Servers that can be located anywhere in the world.

When referring to website addresses, the FQDN is known as a Uniform Resource Locator (URL). The main difference between an FQDN and a URL is that the URL includes the information needed to access a specific resource and specifies exactly what it is you want to have access to on that resource (or server).

Since the HTTP (or HTTPS) protocol is used to access and transfer hypertext documents, the structure of the URL for any given website will look like this:

`http://www.name-of-the-website.com/name-of-the-webpage.htm`

4.2.5.1 URL vs URI

A Uniform Resource Locator (URL) is the most common and well known subtype of Uniform Resource Identifier. The main difference is that a URI can be applied to access resources other than web pages or websites.

Here are some examples of what a URI looks like:

P2P networks:

`ed2k://file|Galactic_Council_Show.avi|14997504|345c013e991ee123d63d45ea71954d4d|/`

Skype:

`callto:<screenname>`

FaceTime:

`facetime://<address>|<MSISDN>|<mobile number>`

Spotify:

`spotify:track:2jCnn1QPQ3E8ExtLe6INsx`

4.2.6 IP & DNS records in your online investigations



Now that readers know about how IP addresses are assigned and how DNS names are registered, they are ready to start their most basic online investigations. They know how to request contact information from DNS registrars and know how to resolve (link) DNS to IP addresses and obtain information about who had those IP addresses assigned to them during the timeframe of their investigation.

In addition to the official channels used to query DNS records and resolve DNS to IP addresses there are plenty of tools and websites designed to automate and help the investigator on this front. Some of the most well-known are: DnsStuff (www.dnsstuff.com), DomainTools (www.domaintools.com) and CentralOps (www.centralops.net), but there are many others.

While these sites are useful, it is important to remember that it is best practice to obtain data from the originating registrars (see section 4.2.4).

4.2.6.1 Whois lookup

Whois records can help an investigator discover the owner of a specific domain name. The records contain information about *who* owns a domain, their name, surname, email address and physical address, their phone number, and some other information which might be relevant. The investigator should be aware that there is no quality or accuracy check conducted on this data.

4.2.6.2 Reverse Whois

This type of service will list all DNS/IP records (known to the site/tool) registered under the identity provided. The investigator can usually search by name, email, phone number or physical address.

4.2.6.3 IP lookup

IP lookup can help the investigator find all available information associated with a given IP address. The investigator may find out who the Registrar is and the Reverse DNS and IP block range to which it belongs. Most tools/sites will also identify the country in which it is to be found and even provide the Geo-Location, city or even latitude and longitude coordinates. The investigator should know that Geo-Location techniques are not fool proof (to say the least) and should never be relied on without further corroboration.

4.2.6.4 Whois, Reverse Whois and IP Lookup Time Machine

The investigator should be aware that DNS records change from time to time or may not be accurate. A DNS record can change its owner, for example, or an owner of a domain may falsify his information on DNS records and relocate the website to a remote country before undertaking some illegal activity. What we call "Time Machine" is basically an interface which allows the investigator to retrieve historical data from DNS records.

4.3 Online sources of information



There are many sources of online information available that might be useful to an investigation. In this section the most common types of online sources are listed together with the types of evidence they might yield.

Restricted

| Source | Example of Available Evidence |
|---------------------------------|--|
| Plain Website | <ul style="list-style-type: none"> ❑ Source Code ❑ Code Comments ❑ Hidden Fields ❑ External site references ❑ Online Ads ❑ Domain Authentication Codes ❑ WebSense / AdSense / SearchSense Codes ❑ Metadata (ex. creation / last modification) ❑ Previous versions at archive.org |
| Social Networking Sites | <ul style="list-style-type: none"> ❑ Source Code ❑ Internal IDs ❑ Chat Subsystem ❑ WebSense / AdSense / SearchSense Codes ❑ Metadata (ex. creation / last modification) |
| Blogging Sites | <ul style="list-style-type: none"> ❑ Internal IDs (blogID, userID, threadID...) ❑ Domain Authentication Codes ❑ Mashup: Twitter ❑ Mashup: FaceBook ❑ Mashup: Twitter ❑ Mashup: Picasa / Flickr ❑ Mashup: URL-Shortners ❑ WebSense / AdSense / SearchSense Codes ❑ Metadata (ex. creation / last modification) |
| WebMail Sites | <ul style="list-style-type: none"> ❑ Chat Subsystem ❑ Voice Sybsystem ❑ Internal IDs |
| URL-Shortners | <ul style="list-style-type: none"> ❑ Public Statistic Services ❑ Creation Date |
| Ad-Networks | <ul style="list-style-type: none"> ❑ Internal IDs ❑ Money Trail |
| Content Storage Networks | <ul style="list-style-type: none"> ❑ Internal IDs (fileID, bucketID, userID, ...) ❑ Hashed content |

Restricted

| | |
|---------------------|--|
| | <ul style="list-style-type: none">❑ Data Versioning Controls❑ Money Trail |
| P2P Networks | <ul style="list-style-type: none">❑ DNS records❑ Assigned IPs❑ Used Ports❑ Chunk/Shard Hashes |



4.3.1 Websites

Websites are the most fundamental source of information available on the Internet. The first piece of potential evidence is the actual “visible” content of the site. The second one is, obviously, the “invisible” content associated with these sites. Invisible content here is basically the “programming language” (HTML, CSS, Javascript, etc.) used to create the webpage, the actual content that the server sends to the browser and which the browser interprets and uses to construct the webpage seen on the screen.

The nice thing here is that more information is usually available than that which actually appears on the screen. Here follows an example of a simple logon web page and a partial dump (or extraction) of the underlying “source code” for that same logon webpage.

A screenshot of a web login form. It contains two input fields: the first is labeled "Login:" and contains the text "jbs"; the second is labeled "Password:" and contains three dots "...". Below these fields is a green button with the text "Login".

```

<HTML>
<HEAD>
<META http-equiv="Content-Type" content="text/html; charset=UTF-8">
<META content="text/css" http-equiv="Content-Style-Type">
<LINK href="/AB3Web/theme/Master.css" rel="stylesheet" type="text/css">
<TITLE>AB3 xsl stylesheet</TITLE>
</HEAD>

<BODY>

<H1>Please Login to AB3</H1>

<form action="/AB3Web/servlet/jbs.ab3.control.AB3" method="post">

<table border="0" cellpadding="0" cellspacing="0" width="100%">

<TBODY>

<tr>
<td align="right" width="30%"><b>Login: </b></td>
<td align="left" width="60%"><INPUT name="loginName" type="" value="jbs"></td>
</tr>

<tr>
<td align="right" width="30%"><b>Password: </b></td>
<td align="left" width="60%"><INPUT name="loginPassword" type="password" value="jbs"></td>
</tr>

```

As can be seen, there is more information there and some of it might be very useful. Some nice examples of data that may be obtained this way are:

- User/developer comments (passwords, identity or location references are extremely easy to find and sometimes very enlightening);
- Hidden fields;
- References to external sites which might provide an independent source of evidence (see Content Networks later for an example).

The source code of a site can help the “deadbox” forensic specialist to prove that a computer has accessed it even if the suspect has cleared his Internet History records and emptied his cache.

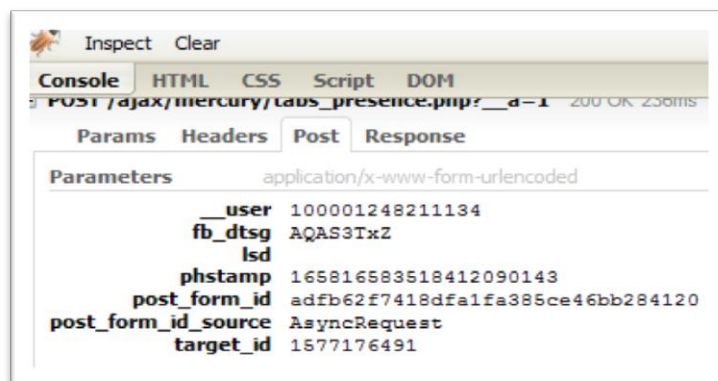
Last, but not least, there are “meta-data” that can provide high level technical information about the webpage itself. A simple example of this point is the Last Modification date for a given web resource (web page, image, etc). Here is a snapshot of such information extracted using an open source tool called FireBug running on Google Chrome. FireBug plus many other similar tools (as well as Google Chrome developers’ extensions) are available that will easily provide even more information from a simple webpage.



4.3.2 Social networking sites

Social networking sites started off as ordinary webpages and have evolved tremendously in their complexity. Complexity is good for digital investigators because it tends to increase the available lines of inquiry. Generic things the investigator should watch out for in Social Networking Sites include:

- Internal IDs.** These sites make extensive use of 'identifiers' (IDs) to track everything (users, pictures, chats, sessions, groups, likes/dislikes, etc.) and these IDs relate most of the time to internal IDs available to the service provider. Facebook makes extensive use of "fbid" (Facebook ID) (e.g. <http://www.facebook.com/photo.php?fbid=389359417758298>). Having a snapshot of the Facebook profile/user/picture, etc, of a person of interest is helpful, but having its internal ID on Facebook's database can be much more interesting.
- Chat.** These sites offer services by which users hold video, audio or text dialogues with other known or unknown users. They can provide information of great quality if processed adequately. The key element for the investigator in all web-interactive elements is to gather as much data as possible and not just what is shown on screen by the web browser. As an example, here is a peek at the information being interchanged with Facebook's servers simply by opening a chat window to talk to a friend. The "target_id" shown corresponds to Facebook's internal ID for the user who is of interest to the investigator.



- **Pictures.** Even though high profile sites have been introducing “cleaning” filters to images uploaded to them, the investigator may still come across some social sites and other types of websites that directly publish uploaded pictures. They should be aware of metadata attached to the images (mainly EXIF⁷⁴ encoded) including: date and time of shot, focal distance, latitude and longitude when the photograph was taken. Programs exist, or can easily be created, to search for and download large numbers of pictures from specific sites and to extract all relevant EXIF metadata in a matter of minutes.



4.3.3 Blogging and micro-blogging sites



In the past there multiple blogging sites powered by many different engines (i.e. types of software). Some were good, and some were bad. One of the more popular engines used to tag the IP address from which each post (entry) had been added. An investigator could easily obtain the IP address just by looking at the webpage’s “source code”. Those days are long gone (although the investigator might still stumble upon an old blogging framework yet). Today there are few blogging engines and almost everyone goes a lot of trouble to protect the bloggers’ privacy. On the other hand blogging platforms now usually require a more rigorous authentication process before the blogger can post to the site.



The blogger service from Google (former Blogspot) requires the user to authenticate their domain (if using their own) by uploading something like this to their main site:

```
<meta name="verify-v1" content="h+kBXIgekCCDbSWyZ+jVGQ4LXeZbGnUZOIyZeQTQB04=" >
```

This piece of HTML metadata code is then used by Google to establish a direct link between a Google email account and the domain used by the Blogger. The user is able to remove that metadata from the web once the link has been made, but almost no one does and this information stays there forever. Sites such as Twitter, Facebook, Google Analytics and AdSense all provide additional lines of inquiry to determine who is actually behind a given blog.



Similar user verification is required for Google WebMaster Tools:

```
<meta name="google-site-verification" content="abcdefghijklmnopqrstuvwxyz0123456789"/>
```

It is well known that Google derives its Site ID from the site’s URL and the email used to validate that site.



Last but not least, although “serious” blogging platforms are quite secure today, certain platforms still allow the possibility to post limited active content which might be useful.

⁷⁴ Ref. http://en.wikipedia.org/wiki/Exchangeable_image_file_format

As well as using established blogging service providers, the skilled web developer can setup a blog on his or her own web space by using a content management system (CMS) designed for blogging. Wordpress is probably the most famous example of such a CMS. Where the investigator needs to get information about a blog hosted on a private web space s/he can refer to the provider hosting that web space, the corresponding Network Interface Card (NIC) and also from the source code (such as the WebMaster Tools or Google Analytics snippets shown in this section).

4.3.4 Webmail services



Most webmail platforms insert the sender's IP address as an additional header on emails sent through them. Gmail, on the other hand, does not reveal this information citing the need to protect the privacy of their users. Several chapters could be spent on each of the big webmail platforms, but that would be too technical and beyond the scope of this Guide. However, the investigator should watch out when dealing with evidence related to these sites since there is plenty of potential for uncovering evidence.



As real case⁷⁵ a example the following URL link file was found on a suspect's hard drive which suddenly became relevant:

```
https://mail.google.com/mail/h/1fghjf56gshi2/?view=att&th=35hydfghdfgdfgwe67tid=0.1&dis
p=attd&realattid=f_gnt1i7j37&zw
```

After doing some research it was discovered that the last part of that URI⁷⁶ "realattid" stands for "Real Attachment ID". Since Google stores only one copy of attachments on its servers no matter how many different emails are associated with that same file, this allowed investigators to determine what the attachment contained and to tie the suspect into the events under investigation.



4.3.5 URL-shorteners

These are becoming extremely common on the Twitter landscape. Apart from the fact that there logs about Twitter connections are being maintained (*which is good for evidentiary purposes*), the investigator should also be aware that some services provide open link tracking statistics. This means that anyone can find the available statistics about the use of a specific shortened URL. Some services even provide these statistics against a timeline which can indicate when the shortened link was created.



4.3.6 Ad-networks

Online ads are one of those sources of information which are usually overlooked. When they appear on a suspect website, ads will lead to an ad-network such as Google AdSense, AdBrite,

⁷⁵ Tweaked and anonymized for privacy

⁷⁶ Uniform Resource Identifier

24/7 RealMedia, Microsoft PubCenter/adCenter, etc. These in turn can provide an ID (which will be more or less reliable depending on the ad-network) and lead to a “money-trail”.



As a side note, and not strictly Ad-related, Google Analytics codes can be found embedded in the code of many, many websites. Their format looks something like “UA-17576257-1” and they are used for gathering business intelligence and user preferences. Criminals also use them to track the effectiveness of all sorts of attacks and scams. IDs linked to a Google Analytics account, are in turn usually linked to a Google account which can then lead to a mobile phone number.



4.3.7 Content storage networks

Content storage networks are services that allow the storing and sharing of material on-line and are part of the Cloud Computing phenomenon.

The investigator will probably consider these networks as an underlying and invisible technology. However, the investigator should be aware of their existence since they can provide additional information or leads into the investigation that might be overlooked if not properly acquainted with this technology. Amazon has S3, Google has a content storage network for Google Apps and Microsoft has one for Azure. Many other applications use the same technology. One of the best-known examples is the cloud storing and sharing facility called DropBox which internally relies on Amazon S3.⁷⁷



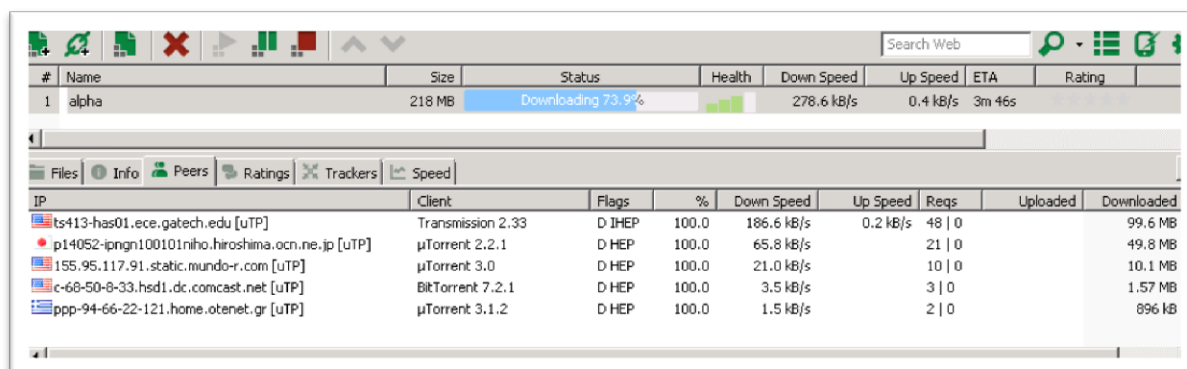
4.3.8 File sharing Peer-to-Peer (P2P) networks

In Peer to Peer (P2P) networks, computers (i.e. ‘peers’) are connected to each other without a central server. Each computer acts as both a client and a server and can share files with any other computer (peers) linked to the same network. Files being shared or downloaded through most P2P networks can be obtained simply by joining the P2P network and by logging appropriate P2P transactions. A user can configure most P2P clients to log transactions and automatically save the results in a file. Depending on national laws, that file may be used as evidence.

Here is a snapshot of a uTorrent client in action. Peers are shown downloading the same torrent (file) simultaneously.

⁷⁷ If they are able to request data formally from these service providers, investigators may find a treasure trove of evidence. For instance, Amazon S3 can provide hashed objects, full access logs and even file/object/shard versioning!

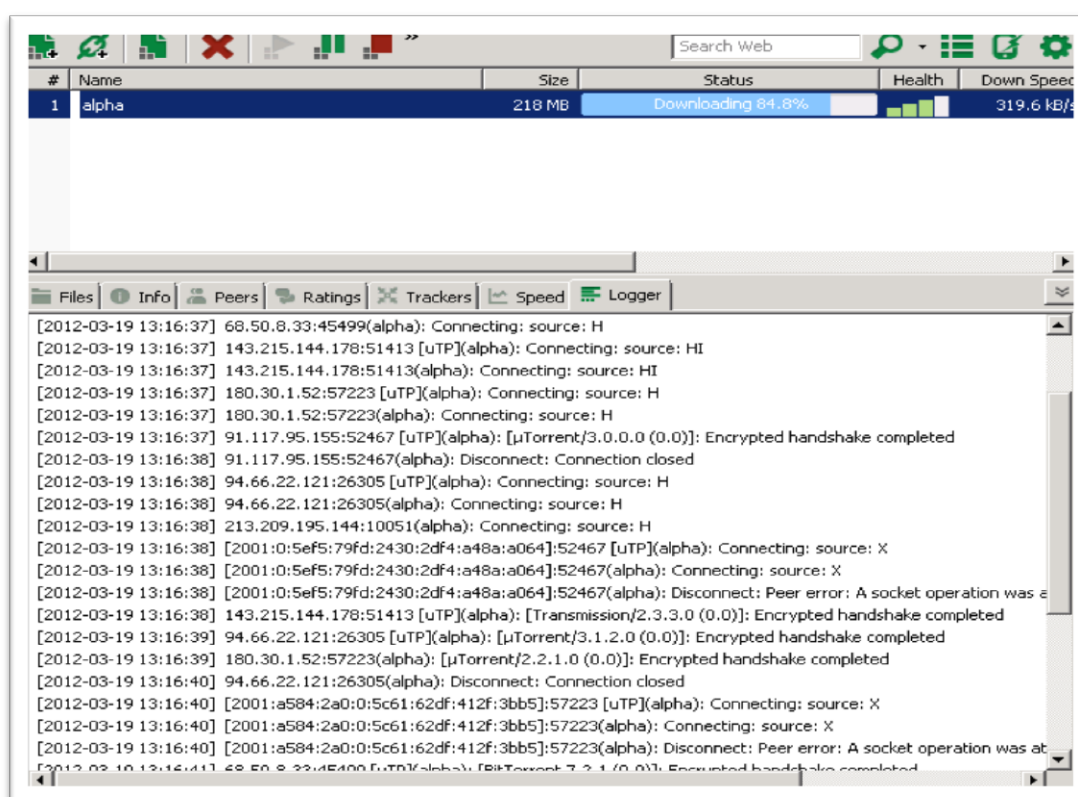
Restricted



| # | Name | Size | Status | Health | Down Speed | Up Speed | ETA | Rating |
|---|-------|--------|-------------------|--------|------------|----------|--------|--------|
| 1 | alpha | 218 MB | Downloading 73.9% | | 278.6 kB/s | 0.4 kB/s | 3m 46s | |

| IP | Client | Flags | % | Down Speed | Up Speed | Reqs | Uploaded | Downloaded |
|--|-------------------|--------|-------|------------|----------|--------|----------|------------|
| ts413-has01.ece.gatech.edu [uTP] | Transmission 2.33 | D IHEP | 100.0 | 186.6 kB/s | 0.2 kB/s | 48 0 | | 99.6 MB |
| p14052-ipcgn100101niho.hiroshima.ocn.ne.jp [uTP] | µTorrent 2.2.1 | D HEP | 100.0 | 65.8 kB/s | | 21 0 | | 49.8 MB |
| 155.95.117.91.static.mundo-r.com [uTP] | µTorrent 3.0 | D HEP | 100.0 | 21.0 kB/s | | 10 0 | | 10.1 MB |
| c-68-50-8-33.hsd1.dc.comcast.net [uTP] | BitTorrent 7.2.1 | D HEP | 100.0 | 3.5 kB/s | | 3 0 | | 1.57 MB |
| ppp-94-66-22-121.home.otenet.gr [uTP] | µTorrent 3.1.2 | D HEP | 100.0 | 1.5 kB/s | | 2 0 | | 896 kB |

If logging is turned on for this client, all the necessary details (IP, ports, timestamps, operations) will be logged straight into a file. In this example, the process has resulted in a file showing who actively downloaded the shmoo.com rainbow cracking files⁷⁸ for alphanumeric passwords.



| # | Name | Size | Status | Health | Down Speed |
|---|-------|--------|-------------------|--------|------------|
| 1 | alpha | 218 MB | Downloading 84.8% | | 319.6 kB/s |

| Timestamp | Log Entry |
|-----------------------|---|
| [2012-03-19 13:16:37] | 68.50.8.33:45499(alpha): Connecting: source: H |
| [2012-03-19 13:16:37] | 143.215.144.178:51413 [uTP](alpha): Connecting: source: HI |
| [2012-03-19 13:16:37] | 143.215.144.178:51413(alpha): Connecting: source: HI |
| [2012-03-19 13:16:37] | 180.30.1.52:57223 [uTP](alpha): Connecting: source: H |
| [2012-03-19 13:16:37] | 180.30.1.52:57223(alpha): Connecting: source: H |
| [2012-03-19 13:16:37] | 91.117.95.155:52467 [uTP](alpha): [µTorrent/3.0.0.0 (0.0)]: Encrypted handshake completed |
| [2012-03-19 13:16:38] | 91.117.95.155:52467(alpha): Disconnect: Connection closed |
| [2012-03-19 13:16:38] | 94.66.22.121:26305 [uTP](alpha): Connecting: source: H |
| [2012-03-19 13:16:38] | 94.66.22.121:26305(alpha): Connecting: source: H |
| [2012-03-19 13:16:38] | 213.209.195.144:10051(alpha): Connecting: source: H |
| [2012-03-19 13:16:38] | [2001:0:5ef5:79fd:2430:2df4:a48a:a064]:52467 [uTP](alpha): Connecting: source: X |
| [2012-03-19 13:16:38] | [2001:0:5ef5:79fd:2430:2df4:a48a:a064]:52467(alpha): Connecting: source: X |
| [2012-03-19 13:16:38] | [2001:0:5ef5:79fd:2430:2df4:a48a:a064]:52467(alpha): Disconnect: Peer error: A socket operation was attempted on a non-socket |
| [2012-03-19 13:16:38] | 143.215.144.178:51413 [uTP](alpha): [Transmission/2.3.3.0 (0.0)]: Encrypted handshake completed |
| [2012-03-19 13:16:39] | 94.66.22.121:26305 [uTP](alpha): [µTorrent/3.1.2.0 (0.0)]: Encrypted handshake completed |
| [2012-03-19 13:16:39] | 180.30.1.52:57223(alpha): [µTorrent/2.2.1.0 (0.0)]: Encrypted handshake completed |
| [2012-03-19 13:16:40] | 94.66.22.121:26305(alpha): Disconnect: Connection closed |
| [2012-03-19 13:16:40] | [2001:a584:2a0:0:5c61:62df:412f:3bb5]:57223 [uTP](alpha): Connecting: source: X |
| [2012-03-19 13:16:40] | [2001:a584:2a0:0:5c61:62df:412f:3bb5]:57223(alpha): Connecting: source: X |
| [2012-03-19 13:16:40] | [2001:a584:2a0:0:5c61:62df:412f:3bb5]:57223(alpha): Disconnect: Peer error: A socket operation was attempted on a non-socket |
| [2012-03-19 13:16:41] | 68.50.8.33:45499 [uTP](alpha): [BitTorrent 7.2.1 (0.0)]: Encrypted handshake completed |

This simple approach can be further developed by building (or buying) specifically modified P2P clients which allow tamper-proof logging, auto feed themselves from torrent RSS⁷⁹ feeds without cooperating in the actual file distribution process (i.e. it receives files from other peers, but does not distribute them). Participation in a P2P network may cause legal issues for an investigation

⁷⁸ These are in effect long collated lists of potential passwords which are then automatically entered in the password box of a target system.

⁷⁹ RSS stands for Really Simple Syndication. It is a system used to deliver content from the web as it is uploaded. Very often it will be related to a news or media service.

depending upon the jurisdiction. More real time investigation might involve sorting the data into a database or real time probing on the IP addresses implicated to gather more data. P2P networks are commonly used for circulating illegal content and are heavily used by law enforcement for proactive child abuse investigations worldwide.



4.3.9 The 'Deep Web' and the 'Darknet'

While the Internet is a place where service and information providers typically want to publish and share data with the general public, there is also a demand for more private areas accessible to a restricted group of people for exclusive purposes. Some of these areas are public places that can only be found by people who have the correct address. Take for example, the couple that want to share photographs of their wedding with their family and friends. They would not want every user of the Internet to see the photos. In this case they could upload the pictures to a cloud service and share the link to the gallery only with personal friends and family. Of course this is not a very secure way to share private data, but it is easy and since the photos would not be regarded as highly confidential this solution might be enough for most people.

There are also other hidden areas of the Internet for which login credentials are needed. A typical bulletin board and a normal webmail account are just two examples of private areas that cannot be found by a search engine or accessed because of their login requirement. Besides the sites that are intentionally hidden from public search engines, there are also websites and databases which cannot be indexed by the search engines because their contents cannot be understood or analysed by them.

The collective name for all those areas of the Internet that are hidden from search engines is called the "**Deep Web**" (other names are "Hidden Web", "Invisible Web" or "Deepnet").⁸⁰

As shown in the examples above, the Deep Web is not a fad, nor is it associated with criminality. It has existed ever since the early days of the Internet. In fact, the first servers on the Internet and the first websites available on the World Wide Web could easily be considered part of the Deep Web. In the days before search engines and public directories became so sophisticated, people could only visit pages if they knew the exact address – for everyone else the server or website was invisible.

It is impossible to measure the size of the Deep Web today because of the very nature of it, but some rough estimates have been given. A study by Bergman⁸¹ from 2001 suggested the following:

| | Surface Web | Deep Web |
|-------------|--------------|----------------|
| Size | 19 terabytes | 7500 terabytes |

⁸⁰ The opposite of the Deep Web is the "Surface Web", so all information that can be found via search engines.

⁸¹ Bergman, M. K. (2001). The Deep Web: Surfacing Hidden Value. Journal of Electronic Publishing 7, 1-17. Available at: <http://www.press.umich.edu/jep/07-01/bergman.html>

| | | |
|------------------|-----------|-------------|
| Documents | 1 billion | 550 billion |
|------------------|-----------|-------------|

Besides the websites, databases and documents that are not indexed by the search engines there is another layer of the Deep Web: the so-called “**Darknet**” (also known as Dark Web). The Darknet, like similar the Deep Web, cannot be searched by the standard search engines. However, while Deep Web websites can be accessed by a normal web browser if the visitor knows the address or the login credentials this is not true for Darknet websites.



Even though the Darknet uses the same physical network (the Internet) as the Deep and the Surface Web, it uses a different internal network and address space. In addition to knowing the Darknet address, an investigator will also need to connect via the Darknet’s internal network to see the content.

Darknet networks are peer-to-peer networks, meaning that every user directly connects to another user. Anyone with the necessary skill-set can create a Darknet and can invite a group of trusted people to participate in this small network. However, there are also some Darknets with thousands of users. The most prominent of these are Freenet and The Onion Routing (Tor) Hidden Services.

The Tor network is an anonymising channel that routes traffic through several nodes. Each node only knows its direct neighbour so it is not possible for any one node (or user) in the chain to tell who exactly sent or received which request. An investigator can access the Tor network simply by downloading the Tor browser⁸². Once connected to the Tor network the investigator can access and configure the hidden services. These services are reachable via “.onion” addresses instead of FQDNs (see section 4.2.4.). An example for such a “.onion” address would be

3g2upl4pq6kufc4m.onion

This is the Darknet service of the legitimate search engine DuckDuckGo, offering anonymous search services.

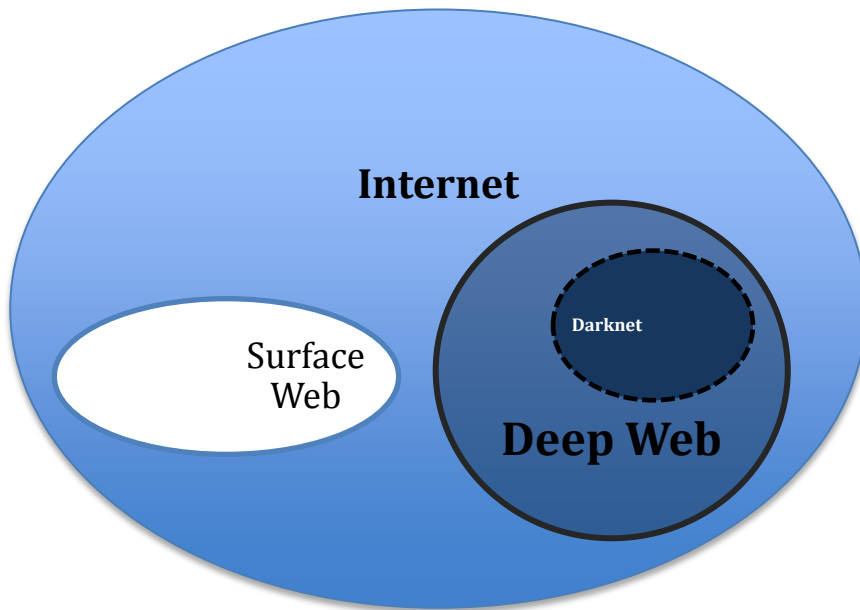
The hidden Tor Services include portals for the following:

- Directories, portals, and information;
- Search engines;
- File storage;
- Peer-to-peer file sharing;
- Social media;
- Email;
- Instant messenger;
- Marketplaces (especially for illegal materials and services);

⁸² <https://www.torproject.org/projects/torbrowser.html.en>

- News, whistleblowing and archives of document archives;
- Pornography.

The following graphic illustrates the relationship between Surface, Deep and Dark Web:



The Deep Web and in particular the Darknet are relevant to law enforcement investigations because the anonymity of the Darknet has attracted merchants and customers trading in illegal material and services such as weapons, drugs, counterfeit money, fake ID cards, stolen identities, botnets, hacking services, child-abuse material, even child-abuse services and contract killers. The most prominent example of such a marketplace is the "Silk Road".



Investigation into the Deep Web and the Darknet is a specialist task that goes beyond the scope of this basic guide. However the following reading list might point readers into the right direction:

- A beginner's guide to exploring the Dark Net:
<http://electronician.hubpages.com/hub/A-Beginners-Guide-to-Exploring-the-Darknet>
- Deep Web Links: <http://deepweblinks.org>
- Deep Web Directories and search engines:
<http://www.thehiddenwiki.net/deep-web-directories-search-engines/>
- Guide to TOR hidden services and elements of the TOR network:
http://en.wikibooks.org/wiki/Guide_to_Tor_hidden_services_and_elements_of_the_Tor_network
- An Adaptive Crawler for Locating Hidden-Web Entry Points, Luciano Barbosa, University of Utah,
<http://www.cs.utah.edu/~juliana/pub/ache-www2007.pdf>

- Investigating the Dark Web – The Challenges of Online Anonymity for Digital Forensics Examiners,
<http://articles.forensicfocus.com/2014/07/28/investigating-the-dark-web-the-challenges-of-online-anonymity-for-digital-forensics-examiners/>
- Crawling the Hidden Web, Raghavan, et al, In: 27th International Conference on Very Large Data Bases (VLDB 2001), September 11-14, 2001, Rome, Italy
<http://ilpubs.stanford.edu:8090/725/>
- Downloading Hidden Web Content, Alexandros Ntoulas et al, UCLA Computer Science
<http://oak.cs.ucla.edu/~cho/papers/ntoulas-hidden.pdf>

4.4 Data v evidence

Having reviewed some of the more prominent sources of evidence for online investigation, a systematic approach will ensure its usability in court.



4.4.1 What do you want that data for?

An investigator must be prepared to answer some or all of the following questions:

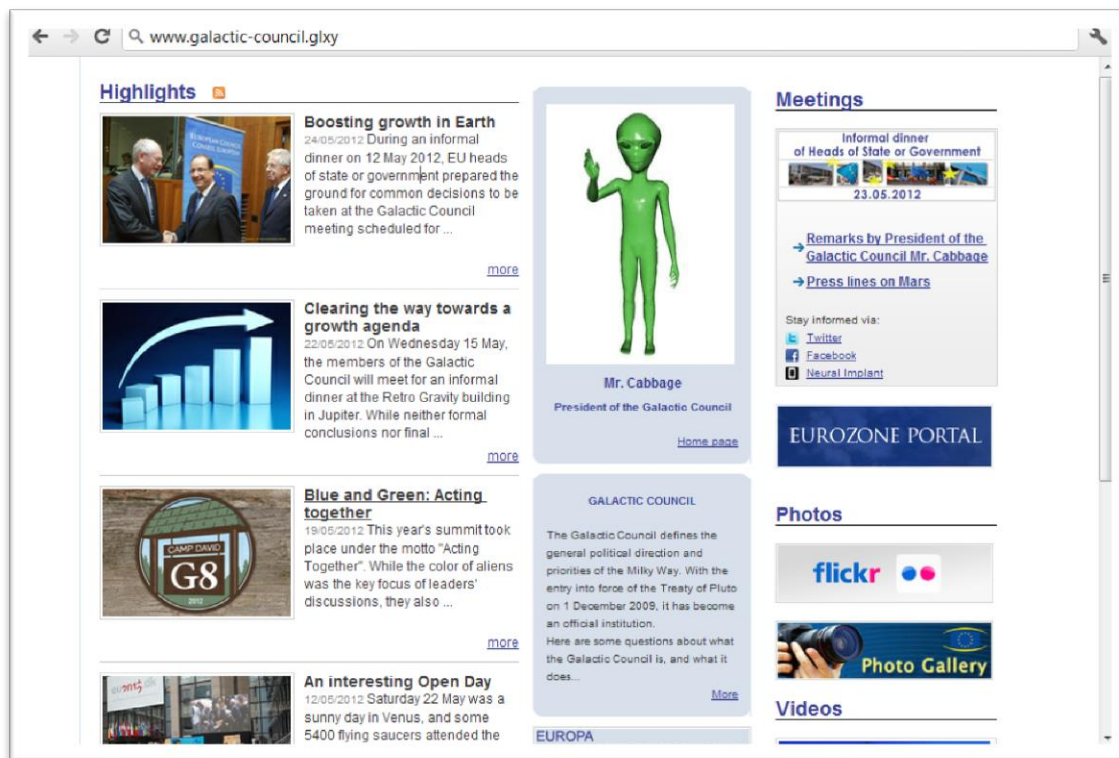
- Where does the data come from?
- Are you sure about the integrity of this data?
- Are you sure this data is complete?
- Are you sure there isn't anything of which you might be unaware that might render your conclusions invalid?

Or simply:

- Can you guarantee the integrity of your evidence?

In deadbox investigations most of these questions will cause no difficulty. There is a pre-established methodology and toolset designed just for this purpose. However, if presenting a snapshot of the browser while visiting a given site, these questions might prove to be a real challenge.

The following is a snapshot of the 'Galactic Council official website':



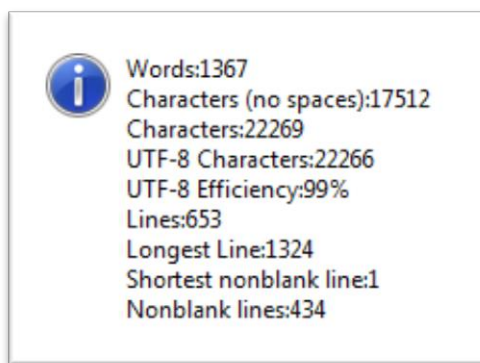
Disclaimer: This is a fake website!

Of course there is no Galactic Council website. This is another website altered to provide the reader with some first-hand fake evidence.

It took roughly 60 seconds to fake that snapshot (40 of which were wasted thinking what to write in it). Given the ease of faking this image, a simple snapshot of online content would never be good enough to prove sufficiently the content of the image for a court. However, the source code for a webpage can help to corroborate content.

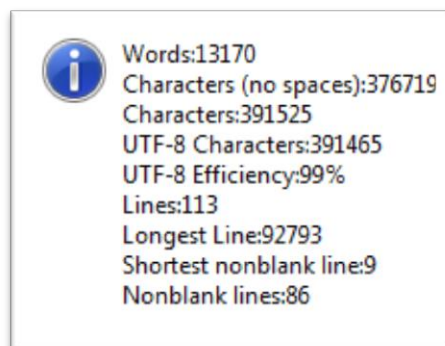
4.4.2 Use the source

The HTML source code can help to establish a snapshot of a web page as evidence for court. Due to space limitations the full source code will not be reproduced, but here are some statistics related to the underlying source code for the fake web page presented earlier.



By comparing these metadata numbers with the image content, it can be shown that quite a bit of data has been added.

That sample webpage was really simple, but here are the statistics for a default Facebook home page:



There is quite a lot of data here and very little of it is actually turned into the screen image by the browser.

As a side note, the HTML and Javascript for that Facebook home page contained 38 references to the user's fbid⁸³ (which looked like this: 100001248123456) plus hundreds of IDs for pictures and other users which are Facebook friends. For someone to hide or disguise all the references in the source code would be a monumental task.

How to find and copy the HTML source code of a web page.

All browsers have the option to save a web page and, in doing so, will actually save the source code. Browser menus will offer options such as "Save Page As" or "File -> Save As". Alternatively, most browsers provide an option called "View source". A right-click on a given web page will reveal the HTML source code that can be copied and pasted into a text file or Word document or saved as an HTML document (which needs to be opened by a browser).

4.4.3 Classic approaches

A common low-cost approach to gathering online evidence is to set up a normal video camera and

⁸³ Facebook ID

simply record opening the web browser and videoing the procedure (displaying the evidence you want to record on your screen). It can also be useful to surf first to the site of a known online newspaper site to provide a sort of crude time stamp. The idea here is that manipulating video footage is not as simple as faking website content on a snapshot.

Those using a video camera should also be aware of something called "Lens Aberration" caused by imperfections in the camera sensor (the imperfections in a printer were discussed in Section 3.4.16). The lens aberration of a camera can be matched to the recorded evidence proving that that particular device was used to make the recording.

4.4.4 High-tech classic approach



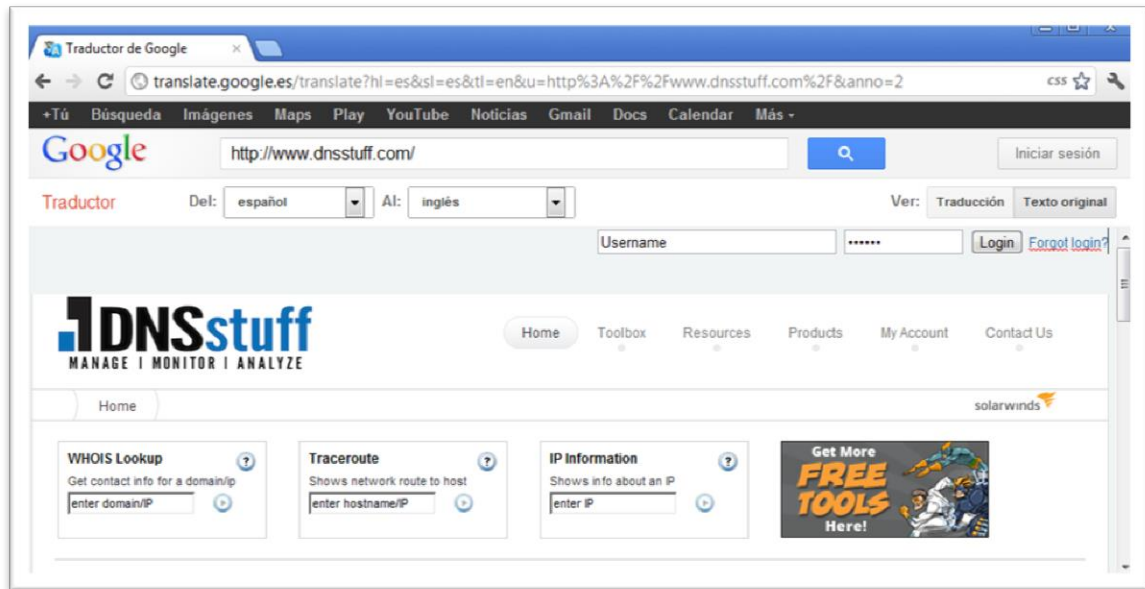
Setting up a standard video camera in front of your computer can be cumbersome. An alternative would be to replace the video camera with digital screen capture software. There are many tools available that can be used in this way. One of the most popular is "Camtasia Studio" by TechSmith. Very similar, but open source, software is "CamStudio Open Source". Both software and video codec have a General Public Licence (GPL) permitting its use. These tools are intuitive and extremely simple to use: Press the red "Record" button and start.

The investigator should always be aware though that the recording is intended as evidence. There should be no added effects. The video should not be edited in any way or even transcoded (i.e. change the format for use on other devices).

Full-screen recording is recommended at all times. It will increase the level of transparency. If the investigator wishes to highlight something by zooming in on an area of the screen the zoom functions of the internet browser (or windows magnifying glass) should be used. The temptation to add a zoom later during editing should be resisted. Last, but not least, the evidence should be videoed in a single file, avoiding cuts and pausing during the recording.

There are also some weaknesses in the recording approach. For instance where a web server has been set up with a copy of a faked web page/site and the DNS records/routing on the computer have been altered to point to the copy instead of the real online website?

This is exactly the kind of challenge that the investigator should try to anticipate. A way around this particular problem could be to record "indirect access" to the online content being recorded to show it is original. A simple way to do this for example is to use something like Google Translate to access the target site (note Google Translate offers a "Show Original Content" button so that the indirect non-translated view can be displayed).



In this image, the DNSstuff website is the (innocent) target and the Google translate is being used to verify that the image on the screen is not a cloned website created by a hacker. So, instead of your computer linking directly to DNSstuff, a Google server contacts the website and requests the home page. This can demonstrate 'live' on video that the examination is indeed being conducted on the genuine webpage. At the same time the time and date of the visit to Google Translate, the IP address and the translated URL will have been recorded in Google Servers logs.

A further way to make the video evidence more robust would be to demonstrate on camera additional, more "technical" data related to the target web pages. One possibility would be to navigate to <http://showmetheheaders.com> which will show "HTTP headers" for a given domain. Headers usually provide a "Date" field supplied directly by the webserver hosting the site showing the time on the web server on which the evidence is hosted.

Here is an example of a header where the last modification, time and the presence of a 'cookie' are shown:

Show Me the Headers for cflabs.com

Server Microsoft-IIS/6.0
X-Powered-By ASP.NET
X-AspNet-Version 2.0.50727

Date Mon, 19 Mar 2012 14:46:33 GMT
Server Apache
Location <http://www.cflabs.es/drupal/index.php>
Cache-Control store, no-cache, must-revalidate, post-check=0, pre-check=0
Content-Length 0
Connection close
Content-Type text/html; charset=utf-8
Expires Sun, 19 Nov 1978 05:00:00 GMT
Last-Modified Mon, 19 Mar 2012 14:46:33 GMT

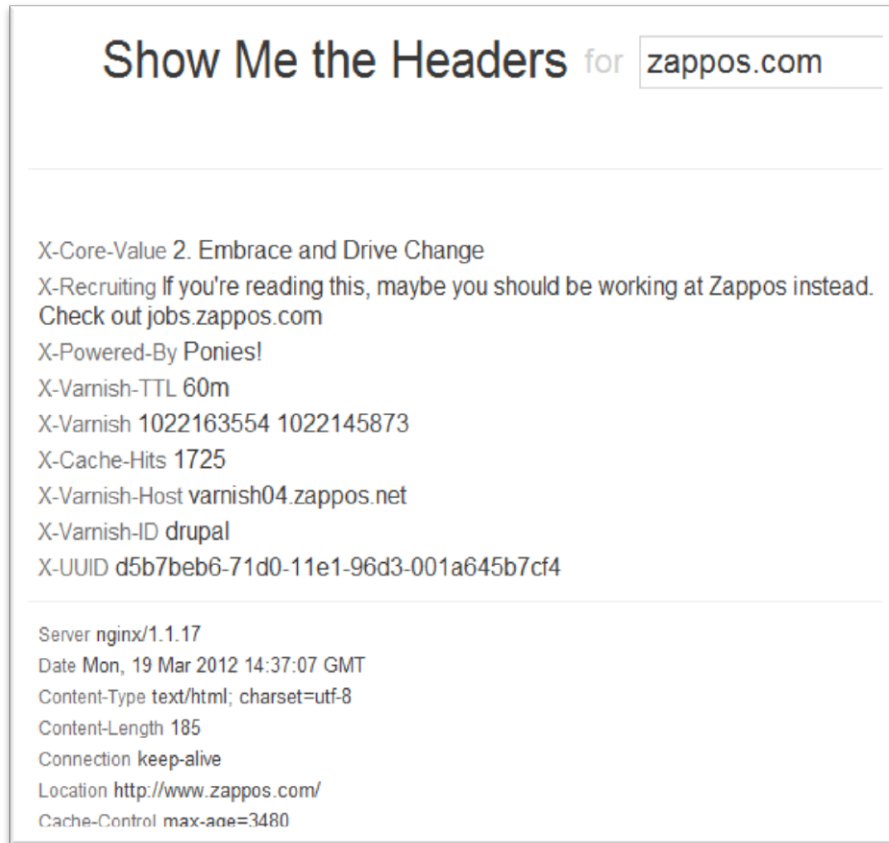
Request took 1.046036 seconds with status codes of 301, 301, 200 and 2 redirects.

```
HTTP/1.1 301 Moved Permanently
Date: Mon, 19 Mar 2012 14:46:32 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Location: http://cflabs.es
Cache-Control: private
Content-Length: 0

HTTP/1.1 301 Moved Permanently
Date: Mon, 19 Mar 2012 14:46:32 GMT
Server: Apache
Location: http://www.cflabs.es/drupal/index.php
Connection: close
Content-Type: text/html; charset=iso-8859-1

HTTP/1.1 200 OK
Date: Mon, 19 Mar 2012 14:46:33 GMT
Server: Apache
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: store, no-cache, must-revalidate, post-check=0, pre-check=0
Set-Cookie: SES31735f053ed6b108ce6fd4d062491549a=huhfk10k24osqs1cpjrbj28tj5; expires=Wed,
Last-Modified: Mon, 19 Mar 2012 14:46:33 GMT
Connection: close
Content-Type: text/html; charset=utf-8
```

Another example to illustrate that some headers might provide additional information too:



4.4.5 Taking it a step further

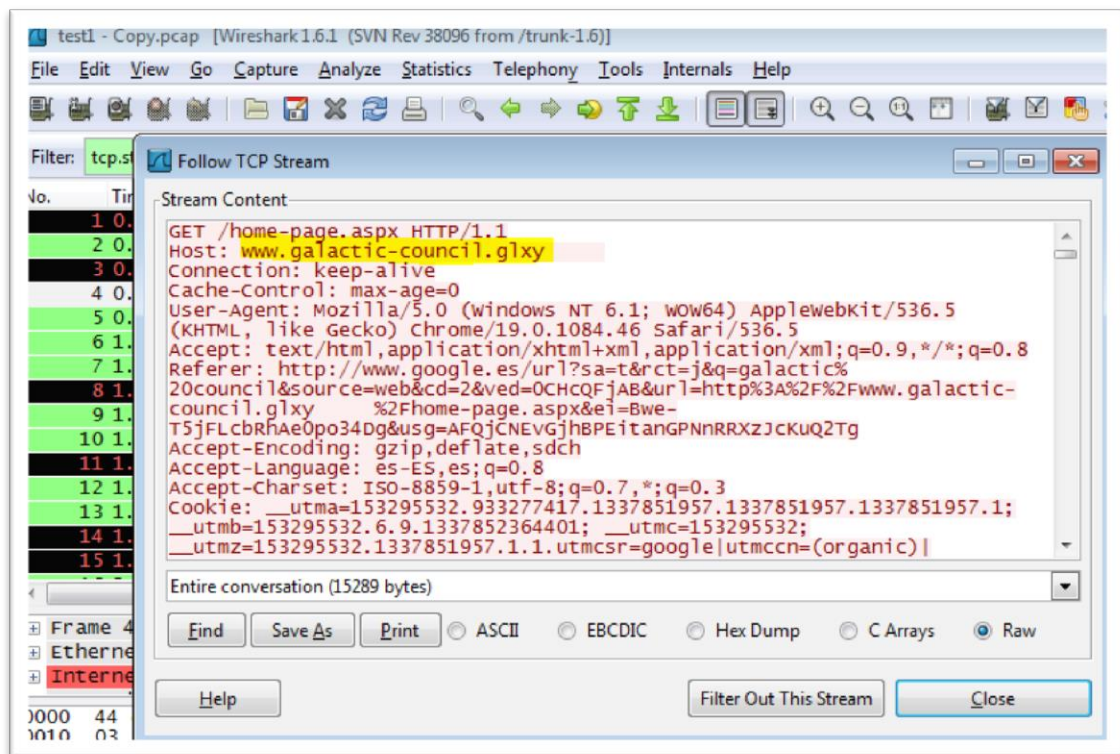


A good way to maintain an overview of what is going on during your on-line investigation and to preserve the technical aspects all in one place is to use a traffic logger/sniffer. This software will record every single packet of data sent and received across the Internet (i.e. the “traffic data”). There are some excellent open source tools available to do this such as WireShark⁸⁴. WireShark software can also capture other online “non-webcentric” technologies including P2P or VoIP.⁸⁵ If encryption is being used (as with some P2P and VoIP services, or HTTPs on webcentric services) then tools like WireShark will capture the encrypted data. Encrypted data will be of limited value to an investigation without the application of considerable specialist expertise.

Here is an example of data captured by Wireshark while loading our reference page “<http://www.galactic-council.glxy>”

⁸⁴ <http://www.wireshark.org/download.html>

⁸⁵ VOIP is internet based telephony and stands for Voice Over Internet Protocol. Skype is a well known example of this



For webcentric data, a compromise between ease of use and detail would be to run the web session through a 'logging proxy'. A proxy server sits between the program run by the user (such as the web browser) and the real server. A 'logging proxy' logs all incoming requests and forwards them to a nominated endpoint. This approach might be easier to setup and has the added benefit that it can be easily extended to integrate with real-time solutions that sign and timestamp the logs generated.

4.4.6 Time stamping



Trusted time stamping is the process of securely recording the times that a document has been created and modified. 'Securely' here means that no one — not even the owner of the document — can change the records once it has been recorded.

There are some good open source time stamping options and many commercial services which might be considered trustworthy enough for local needs.



4.4.7 Creating a viewable duplicate of a website

Another technique for storing the contents of a website for later review is to create a viewable offline copy. The software HTTrack Website Copier is capable of downloading the content of websites as well as media files from the Internet. The tool can change all the paths in the source code to point to media files and linked sites so that the website is effectively reproduced when viewed offline with all associated images. This can be a good approach when it comes to presenting the contents of a website in court, but the investigator must remember that the source

code has been changed by the tool and that such tools are often unable to copy the complete website with all linked media and sites.

4.4.8 Notary

There are situations in which a Notary or other legal officer might be co-opted to help in producing evidence. One of the functions of a Notary in civil law jurisdictions is to review and authenticate certain legal documents and agreements in a way that is acceptable to a court of law. If a notary can be invited to access whatever online material is needed as evidence using their computer and Internet connection, they can then formally attest to the authenticity of the evidence that is uncovered. Where international cooperation is required many countries have agreements recognising notarized documents between them.

4.4.9 Limitations on existing approaches

There are many tools and services that claim to provide automated acquisition of online evidence and appear to guarantee the admissibility of evidence. Though many of these tools and services may increase the probability of evidence being admissible at a court of law, there is no single tool which can guarantee with 100% admissibility under any legal framework.

There are two fundamental limitations:

1. All software tools depend on a 'reliable' computing environment which is something difficult to achieve and almost impossible to prove to a third party. In simple terms, any tool running on an investigator's computer can be compromised and modified. Some great advances have been recently made on this front (with the Trusted Platform Module for example), but such systems are not yet mature enough for evidential purposes.
2. The reliability of a commercial service is only as dependable as the reliability of the companies offering those services. Such services tend to market themselves as offering an impressive range of functions: "time stamping", "encryption", "digital seals", "micro-hashing". The weak point is usually in the initial data acquisition. If there is a risk that the service could be vulnerable to corruption with fake data, then that risk will also be present in any evidence it claims to provide.

4.4.10 Adding it all up

As will by now be apparent, there is no ideal methodology or toolset for securing online digital evidence in a way that guarantees its admissibility in any court of law anywhere. Best practice at the present time involves maximising the quality of the data acquired and to take all necessary steps to ensure, as far as possible, the integrity of evidence and the transparency of the process by which it has been acquired. If local laws permit, the services of a notary or similar civil servant or a governmental trusted Time Stamping Authority might be engaged to add an additional element of objective validation. **Taking all of this into account, the admissibility of a procedure or methodology should be checked with legal advisors before being adopted.**



4.5 Covert online investigations

This Guide can only offer general advice on the covert deployment of a law enforcement officer. Anyone involved in covert investigation (either on the Internet or in the real world) must always be appropriately trained, competent and authorised.

This role may not exist in some jurisdictions or may even be prohibited by national law. Wherever the deployment of covert officers is under consideration, due regard must always be given to legislation, policies, procedures, codes of practice and applicable standards for conducting investigations in that particular jurisdiction.

Before commencing any online investigation the authorising officer and the covert agent must establish the scope and requirements of that investigation as well as the parameters to be applied in the deployment and conduct of the covert online investigator. A risk assessment must be prepared and continually revisited and reviewed throughout the deployment.

All decisions and actions must be documented in accordance with current policy and legislation. This log should show how and when any decisions were made and, where appropriate, contain a note of the reasons for such decisions.

Prior to any deployment, the framework for information and intelligence sharing must be formally established. This may require the use of a support officer to assist the online agent in the case of any unforeseen changes in the direction of the investigation. The support officer will also act as a conduit between the authorising officer and any other service required to continue the online interaction without interruption.

While carrying out covert operations the agent must establish and maintain effective covert online identities appropriate to a range of investigations, taking into account available equipment, resources and support and their own knowledge of Internet based utilities.

Consideration must be given to sourcing the equipment and associated services necessary for undertaking such an investigation in a covert and untraceable way. It should not be possible to track any of the equipment or services back to a law enforcement agency under any circumstances.

On a regular basis the equipment and all potential recording systems must be tested to ensure they are operating properly and to confirm their continued suitability for such operations.

When operating under their covert identity, agents must adhere to appropriate and ethical standards. In gathering information, establishing and maintaining contact with the subject of the investigation they should act in accordance with any conditions set out in their initial deployment instructions.

Because online investigations can develop very quickly, agents must pre-prepare and develop strategies to deal with any potential conflicts or difficulties that may arise during an interaction. In

extreme cases this may, for instance, require simulating equipment failure to allow sufficient time to consider appropriate response.

Agents must:

- Be able to identify the legal limits to their actions (including to be able to recognise what constitutes participation in crime);
- Understand thoroughly the need to corroborate evidence;
- Consider the Human Rights of the subject and all other parties affected by the investigation.

Agents must always ensure that all material relevant to the investigation is retained and recorded in a durable and retrievable form. This may require the development of secure systems not normally available within the agency involved.



4.5.1 Technical risks

From a technical point of view, steps must be taken to protect the true identity of the agent online just as in any covert mission. Most email solutions will provide the IP address of the agent to the suspect; even emailing services that do not provide original IP addresses (like Gmail) might still be used to identify the agent. A classic technique used by a cybercriminal consists of sending “bait” attachments, which will reveal the IP address and other interesting information from the agent’s computer once opened. Other more elaborate techniques also exist. Blogging can be just as revealing and chatting will usually establish a direct connection between both parties (at some point in time) that will again reveal the IP address. For this reason covert equipment should be tested before going online. Experienced investigators have uncovered the identity of criminals who thought they were using a secure “Anonymous remailer” platform, which turned out to be secure only if paid for by subscription. Double check and always try to track back to the computer of the agent.



5 Data held by third parties

It may not always be possible to access a device physically or remotely as described in Chapters 3 and 4. Data stored in large complex devices (such as those of large Internet Service Providers) may be all, but impossible to access without the cooperation and assistance of the Internet Service Provider. A way around this may be to seek the cooperation of a third party (such as the hosting provider), who may be able to supply log files and service registration data. Obtaining data from third parties is further discussed in section 5.1.

Third parties may also collect electronic evidence on a provisional basis indicating that a cybercrime took place and prompting law enforcement to initiate an investigation. This is further discussed in section 5.2. The sheer size of the Internet and the number of transactions conducted every minute, means that it is impossible for the meagre resources available to law enforcement to monitor it effectively. Although some parts of the Internet are fully accessible to all Internet users, other parts are restricted and require registration. When crime takes place through closed communication channels (such as a crime committed using personal email), law enforcement has little chance of noticing that crime or obtaining documentary evidence about it unless it is reported by an individual with access to this private channel.



5.1 Independent data holders

Identifying the perpetrator of crime committed over the Internet can be difficult. Often, the only information known about the source of the crime will be an IP address, a MAC⁸⁶ address, an email address, a domain name or an Internet pseudonym or 'handle'. To be able to identify the physical person behind the Internet address, the specialist needs to obtain data held by Internet Service Providers. Internet access, email or hosting providers are often the only entities who can provide the crucial link between the cyber identity of the perpetrator and a real world identity. Independent data holders can therefore often be the key to bringing a suspect to justice.

The following scenario may help to explain how intermediaries can identify a criminal: A victim's computer is compromised allowing the perpetrator to obtain full access to all the victim's computer files (including bank records and login passwords to various websites). Forensic analysis reveals that the victim received an email containing malware that installed spying software on the victim's machine. The police officer investigating the matter is able to identify both the email account used to send the infected email and the IP address from which it was sent. Information provided by a the Internet Service Provider reveals that the email was sent from a corporate network in a major town in Finland. The email account provider shows that the same email account is being accessed not only from Finland, but also from up to three different countries on the same day. Clearly the perpetrator is sending emails via hacked computers or a proxy network. However, the email account provider also reveals that an attempt has been made to pay for the email account with a

⁸⁶ Media Access Control address is a unique number that identifies a device on a network.

blocked credit card number. The investigator makes a request to the credit card company for information about the credit card holder. Information show the credit card account had belonged to an elderly Japanese gentleman, but that it was disabled recently after the number had been used for some fraudulent purchases on the Internet. One of the fraudulent purchases was for computer equipment by mail order. The computer equipment retailer is able to indicate the delivery address in Holland to which the goods were shipped. When this Dutch address is searched, a laptop is found and in its memory there is a copy of the email with the malware that was sent to the first victim.

This example demonstrates how identifying a perpetrator of internet crime may involve an extended string of linked inquiries as well as the need for strong international cooperation. Such inquiries can take time (in particular when requesting evidence from abroad⁸⁷) and there is a real risk that the data stored by a third party may no longer be available by the time a request is made. This can be a particular difficulty when seeking traffic data IP addresses.

It is highly likely that independent third parties will require a court order or other legal process of authorisation before releasing any personal data about customers or about the customers' Internet activities. Such information is commonly protected by national privacy and personal data legislation and by the terms of the service contracts. However, evidential data released in accordance with accepted legal practice will be admissible in court.

As users increasingly store their data with ISPs in the cloud it has become increasingly common to need to approach third parties for access to that data. In 2008 the Council of Europe published an overview of good practice and recommendations for working with ISPs to secure evidence under the title "***Guidelines for the cooperation between law enforcement and internet service providers against cybercrime***".⁸⁸



5.1.1 Fostering cooperation between independent data holders and law enforcement

Using databases to identify criminals is an established process within the criminal justice system. Fingerprint and DNA databases have become mainstays for criminal investigation in many jurisdictions. However, the data bases involved in electronic evidence are unlikely to be owned by law enforcement or government entities. The databases for electronic evidence are spread across the multitude, the thousands, of private companies that make up the Internet. This means that the relationship and cooperation with private companies is extremely important. However, a lack of central information about customer identifying information held by ISPs makes it difficult to establish standards for the exchange of information. Each of these companies has its own methods for dealing with criminal activity on their network, for preserving requested data, and for prioritising the preservation requests they receive.

⁸⁷ See Section 8 on jurisdiction.

⁸⁸ http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf

Establishing regular dialogue directly with an independent data holder can help avoid misunderstandings and provide guidance on which requests are urgent and which are of a lower priority and will also help foster a culture of cooperation. A cooperative dialogue can also encourage service providers who witness a crime to report it to their law enforcement contacts.

The Council of Europe's ***Guidelines for the cooperation between law enforcement and Internet service providers against cybercrime*** provide a number of suggestions on how to encourage cooperation. Suggestions include the use of standard formats for making requests and replies and the nomination of single points of contact to facilitate information exchange. The Guidelines also suggest that both parties prepare written procedures governing how requests will be processed and managed. Such procedures can provide confidence in the way the data is preserved and obtained and can ensure human rights and privacy expectations of data subjects are protected.

The Guidelines also suggest regular meetings between law enforcement and ISPs and other third party data holders. This can become a forum for discussing difficulties with regard to the cooperation, but also for discussing emerging trends and threats in a strategic and forward looking manner. Cooperation may also include joint training between law enforcement and the private sector. Such training can help to dismantle preconceptions and foster an environment of trust between the participants.

5.1.2 Data preservation

Any procedural law (such as production orders, requisitions or subpoenas seeking information from Internet Service Providers) enacted in one jurisdiction will not be enforceable in another. To obtain evidence from a foreign ISP, a request needs to go through an authorised mutual legal assistance process as described in Section 8. This can be time consuming and there is a risk that by the time the data holder, the service provider, receives the request such requested data may no longer be available. Communication service providers do not store traffic data indefinitely and will not normally store such data any longer than is necessary for billing purposes.

One example of data retention legislation to try to prevent this was the European Union's Directive 2006/24/EC. This Directive aimed at harmonizing the period of time that electronic communication providers would retain communication traffic data.⁸⁹ The Directive required Member States to legislate for service providers to retain data for not less than 6 months and no more than 24 months. However, in April 2014 the European Court of Justice, in a case brought by interest groups from Ireland and Austria, found that the Directive was disproportionate in its application and therefore incompatible with fundamental rights. The Directive was, therefore, struck down. Since then the doctrine of data retention has been under review in the EU. The UK immediately enacted emergency replacement legislation to ensure such data is retained. Other EU Member States have been more reticent.

⁸⁹ i.e. data about the data communication, not the content of that communication.

For any investigation involving the Internet, traffic data may be the only evidence linking an electronic communication to a physical person. If those data are deleted before the investigator can request them, that link is lost forever. Unfortunately it can take a long time for an investigation to be launched and even longer before the investigation identifies the Internet resources used by a criminal (who is quite likely to have hidden his or her tracks). The traditional diplomatic channels for international assistance requests can also take a substantial length of time and prevent timely submission of a request to the relevant service provider.

For this reason Article 16 of the Budapest Convention allows parties to the Convention to request the preservation of computer data even before a court order has been obtained. Article 17 on traffic data as well as establishing a procedure for requesting the rapid preservation of data also allows a competent authority to disclose 'expeditiously' sufficient traffic data 'to enable the Party to identify the service providers and the path through which the communication was transmitted'. A Party to the Convention can make a request to another Party to preserve traffic data and content data using the 24/7 contact network created in accordance with Article 35 of the Budapest Convention.

It is suggested that, when making a request for the preservation of data, an investigator should also request both confirmation that the data has been preserved and a reference number for the stored data.

It is not compulsory for Parties to the Budapest Convention to use the 24/7 contact point network. Indeed direct cooperation between ISPs and Law Enforcement Authorities can be potentially more flexible and result in a better understanding of their respective needs and limitations.

5.2 Receiving reports about cybercrime



In many cases a victim of an Internet crime will not know that his or her data has been illegally copied until the stolen data start to be used by the criminal in the real world. Indeed victims may never know their data have been stolen. If they do not know they have been a victim, they will never report it; law enforcement will never record the offence and it will never appear in official statistics. Cybercrime is believed to be greatly underreported.

A further challenge for law enforcement is that there is comparatively little public space on the Internet that can be monitored. Most Internet communications (as in the real world) happen in private between private individuals in privately owned space. Without special permission from the court, law enforcement can only monitor that small amount of Internet content posted on public web pages.

Since crimes committed over the Internet are largely invisible, law enforcement is more dependent on reports by third parties of suspicious activities. The sections below on victim and witness reports explain how electronic evidence may be collected to help law enforcement identify crimes.



Obtaining credible reports, substantiated by electronic evidence, can assist law enforcement at the strategic level to understand cybercrime as a phenomenon, identify emerging trends and developing threats as well as focus on those modus operandi that cause most harm to the public. Reports from third parties can also be of value to commercial companies that may not be aware that their network and data have been compromised. In the case of botnets⁹⁰, for example, many innocent users will not realise that their machines have been infected and enslaved by the criminal network until a third party, such as an internet security company, contacts the ISP with a list of infected IP addresses.

Normally, victims of computer crime will report an offence if they have sustained losses or some kind of damage that affects them personally. However, a number of victims of computer crime may also choose not to report a crime because their loss is minor, they don't want to get involved, they think reporting the offence will embroil them in lengthy bureaucracy and/or they have no confidence that law enforcement will be able to bring the criminal to justice.

An example of minor inconvenience that may seem insignificant for a victim, but have a larger criminal footprint would be the case of spam messages. Spam emails are not illegal everywhere, but even in a country where spam messages are unlawful, a user seeing a single spam message will normally add it to the junk folder and forget about it. The user does not think of the millions of similar messages being sent and being used to support organised criminal activity. Similarly, a user may be infected with a computer virus that provides a hacker with access to his computer, but once the anti-virus software disinfects the computer, the victim may not feel compelled to report the offence to the police. Even so, the victims of such crimes could still provide important information to law enforcement if there were a simplified way of submitting it.

Since 2002 the United States Federal Trade Commission (FTC) has invited users to forward any spam they receive to the email address spam@uce.gov so that the FTC can analyse the trends and focus its anti-spam efforts more effectively.

Several national police forces have also launched user friendly methods for reporting internet-based offences including:

- Belgian Federal Police's <http://e-cops.be>
- French national police's <https://www.internet-signalement.gouv.fr/>
- French NGO <http://www.signal-spam.fr/>
- United Kingdom's <http://www.actionfraud.police.uk/>
- United States FBI's Internet Crime Complaint Center <http://www.ic3.gov/>

It should be noted that such reporting centres are not meant to be used for reporting emergency situations.

⁹⁰ Botnet comes from joining the words roBOT and NETwork. It describes a network of computers that have all been infected by a particular virus so that they can all be used remotely to further some illegal internet activity. The computers are used without the owners' knowledge.

5.2.1 Collating several victim reports to build a case

As discussed above, a cybercrime offence may only involve a limited monetary loss to an individual, but these individual small amounts will not reflect the overall gains made by the cybercriminals involved nor the damage the criminals are causing society as a whole. An analysis of multiple minor cases taken together may justify the allocation of resources and investigation time not warranted by one minor offence seen in isolation. Indeed even to process an international request for assistance, some countries require the case to meet minimum threshold criteria more easily met when considering a series of minor crimes taken together.

Receiving and collating reports at the international level can also be beneficial since the targets of cybercrime are likely to be spread across the globe. Europol has created a trans-European investigation database where EU law enforcement can input data. Similarly the Inhope Foundation (www.inhope.org), has a global database of addresses reported to be hosting child pornography. The Foundation cooperates with affiliated reporting hotlines to identify common reports law enforcement can use as evidence to request the content to be taken down and to conduct further investigation. Law enforcement from across the world can work with Interpol (www.interpol.int). Interpol HQ in Lyon maintains a database of known child abuse images that may be used as evidence. Contact with Interpol should be made via the National Central Bureaux in each country.

Reporting centres can also be set up as a public-private partnership. A good example of this is the French association www.signal-spam.fr which collects and collates reports of spam from the general public. Signal-spam reports its findings not only to law enforcement, but also to email routers. This allows the email providers the option of unsubscribing those users responsible for abusing their services.

5.2.2 Witnesses to cybercrime

Network operators while monitoring activity on their computer network may sometimes discover that an attack is taking place. Email hosting providers may see an unusually large number of emails going to or from a particular address. An antivirus software publisher analysing a new form of malware may identify a computer server with a hosting providers that is being used as a botnet command and control centre. These are all witnesses to cybercrime, but may not know how or to whom the criminal behaviour should be notified.

Having a central reporting centre for witnesses to report crime can be very beneficial (and can be incorporated in the kind of centre for victims mentioned in section 0). Such a reporting centre needs to be centralised, accessible and properly marketed with the general public.

The US Internet Fraud Alert Center (<http://www.ifraudalert.org>) was set up to receive reports of stolen credit card information. This center is a cooperative venture between law enforcement and the private sector represented by ISPs and credit card companies. The center compares publicly disclosed credit card numbers with those credit card numbers that have already been blocked by



the financial institutions in order to ascertain whether the reports concern new thefts and whether the credit card needs to be blocked.

Another example of a repository of witness information and electronic evidence is the website malwareurl.com where witnesses can report web pages with malicious activity.

A reporting centre can be public, but can also be restricted to members only (such as the website ops-trust.net). Both public and private reporting centres collect a wealth of information that can help inform law enforcement at the strategic if not the operational level.

Finally, it needs to be pointed out that for some types of crimes, reporting centres should encourage users to make reports, but discourage them from conducting their own investigations or to seek out unlawful material actively. Indeed, in some instances, such as with child abuse images, the very act of searching for such material can be unlawful.



6 Analysing evidence

Once evidence has been obtained from a computer system as described in the three previous chapters, the next phase of the investigation is to extract the important elements from the seized data. That is, those elements relevant to establishing facts in the investigation.

This chapter will describe the concept of Digital Forensics, the process model that builds the foundation for forensic examinations, the principles that need to be followed during an examination and the common methods used perform certain tasks. It also takes a closer look at digital traces and the kinds of evidential analysis that are commonly used by forensics specialists (such as hard disk analysis, digital photo analysis, and traffic log analysis).

The common principles for obtaining the data listed in Section 1.7 also apply in the analysis phase. Indeed, they are all the more important during analysis as it is here that data will be established as legal evidence.

An International Data Corporation (IDC) study⁹¹ forecast that in the year 2020 a total of 44 zeta bytes (44 trillion gigabytes) of data will be generated and consumed worldwide. The IDC study was based on the premise that the amount of data worldwide doubles in size every two years and that this data consists mostly of records of the activities of the computer user. In an investigation such data can provide valuable insights into the activity of the user.

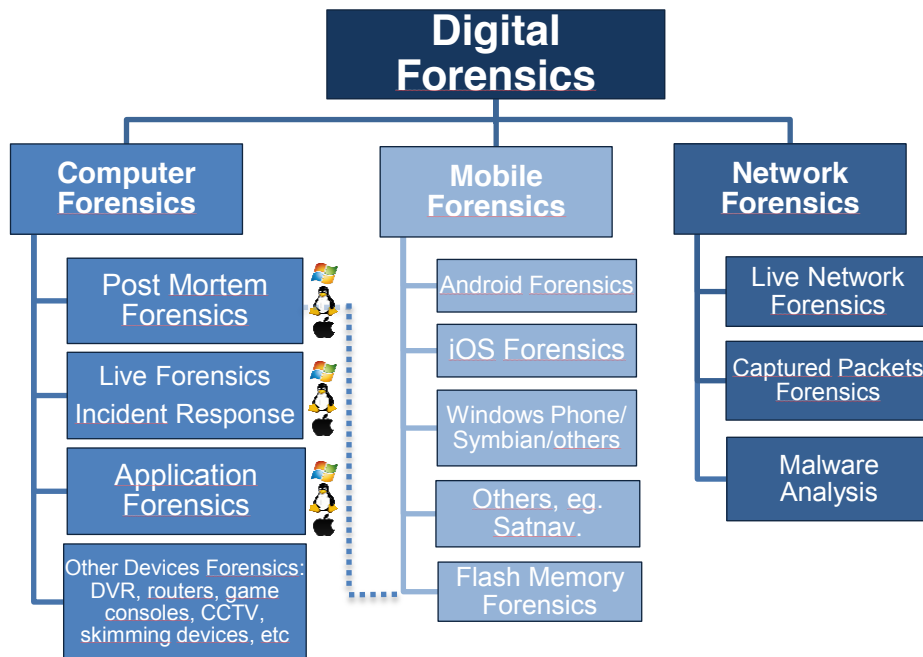


6.1 Digital Forensics

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:

⁹¹ IDC study entitled "Digital Universe Study 2014", April 2014, made available by EMC at <http://www.emc.com/leadership/digital-universe/index.htm>.



The three main categories are:

1.) Computer Forensics is the oldest of the categories. It affects personal computers, servers and storage media. There are four areas of Computer Forensics. They are:

- **Post Mortem Forensics**, which is all about how to acquire, process, analyse and present data stored on computer systems that were not turned on at the time of seizure. This is the most traditional area of computer forensics. Post mortem forensics also includes the broad area of physical disk recovery, file system forensics and other advanced techniques.
- **Live Forensics** is all about how to acquire, process, analyse and present data from a computer system that is turned on. Incident Response is the branch of Live Forensics that relates to incidents occurring on computer systems (e.g. security breaches) and how to prevent and react to them. Compared to Post Mortem Forensics this is rather a young area that is becoming more and more important as so much data is now being stored temporarily, remotely or encrypted - or in the case of incident response needs urgent action on running systems.
- **Application forensics** is the area that focuses on analysing traces left by thousands of different applications (programs).

- The last area of computer forensics is that pertaining to **other hardware devices**, such as digital video recorders, routers, game consoles, skimming devices and many more. A lot of these devices have their own proprietary file and operation systems.

The first three areas may be further subdivided to align with the different operation systems, like Windows, Linux, Mac OS.

2.) Mobile Forensics is also younger category, but is becoming quite popular with the adoption of mobile devices like smartphones and tablet computers. The areas within this category reflect the many different operation systems. The most popular at the moment are Google Android and iOS from Apple. In mobile forensics the experts distinguish between logical⁹² and physical acquisition and analysis. A new, specialised area that crosses the boundary between mobile forensics and computer forensics is flash memory forensics.

3.) Network forensics handles electronic evidence that is transmitted over a network, be it wireless or wired, Internet or a local area network (LAN). In live network forensics the investigators are normally intercepting a network connection and need to analyse the data streams 'on-the-fly'. While in 'captured packets forensics' they analyse files that already contain recorded network traffic.



6.2 Digital Forensics process model

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



Acquisition: Digital evidence needs to be acquired. This can happen by collecting volatile data during a house search, by acquiring a suspect's disk from a seized computer or in any other process during an investigation. The application of correct and robust procedures at the acquisition step is crucial as there is enormous scope for irreversible errors to be made. It is important to keep the chain of custody intact, to document all steps carefully and to verify all images and copies that were acquired.

⁹² i.e. what can be found in the logic circuits of a computer system.

Processing: During processing the forensic examiners may prioritise certain devices or data and will produce an exact copy or image⁹³ 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.).

Analysis: During the analysis phase the examiner actually searches for digital 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.

Presentation: After evidence has been found in the analysis step, 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. He may also be expected to interpret those facts and to express an opinion on their meaning.

6.3 Common principles when analysing electronic evidence

Common principles help to ensure that electronic evidence is obtained in a manner that safeguards its integrity and in a way that can be verified.

Because computers have become so integral to modern life, they are no longer used merely for business activities, but contain all sorts of personal information that can reveal intimate details about the user. Consequently, it is likely that sooner or later private, confidential or legally privileged information will be revealed that may give rise to legal challenges and issues of fundamental rights.⁹⁴ Such issues, if raised, will not be easy to settle on the spot, but nor is it necessarily prudent to discard the data because of such a challenge. The challenge might be wrong. One solution is to seize the data, but to place it under seal with a process server or bailiff until the legal status can be worked out. Indeed placing the data under seal, may also allow time to obtain authorization to access the data even if it is indeed confidential. This is discussed further in section 6.3.5.

6.3.1 Data integrity

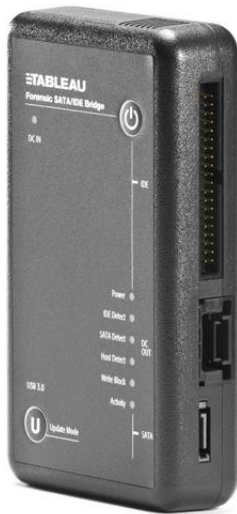
Analysing a computer device is similar to an investigator examining a physical crime scene in that evidence must be kept preserved intact, as close to the original condition as possible and free from contamination.

Similarly computer forensics analysts have to be careful not to disturb or modify any of the electronic data they examine in the forensics laboratory. Even the slightest operation applied to a

⁹³ An image is sometimes called a mirror, a bitstream copy or bit-by-bit copy. This duplicate reproduces everything exactly, including 'empty' space

⁹⁴ Especially the right to respect private and family life, Article 8 of the European Convention on Human Rights

device can change the content of its memory. Merely listing the content of a file directory or opening a file will modify the file's "last accessed" entry.



As mentioned above the primary precaution forensics examiners take in safeguarding data integrity is to conduct their examination on an identical copy or image of the data rather than on the original. In order to prove the original and the copy are exactly the same, a mathematical algorithm is applied to both data sets. This algorithm produces a very complex number called a hash value. If the hash value for both files is the same, then the files 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.

Another method commonly applied is to access the device in "read-only" mode. This is typically done by using a hardware write-blocking device such as shown in the picture on the left.

Finally, as part of the data integrity principle, an experienced examiner should always be alert to the possibility of anti-forensic techniques. S/he should 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 its seizure by law enforcement. Knowledge of anti-forensics techniques should always be part of forensics examiner's curriculum.

6.3.2 Audit trail



Imagine the scenario where a private company's server is hacked and all data, including employee details, have been copied. Investigations on the server show that the hacking originated from a residential Internet connection in a neighbouring town. The suspect, the occupier of the house from which the attack was launched claims he is innocent and that the perpetrator must have hacked into his home computer and used it to hack into the company server remotely. Further complicating the puzzle is that the suspect is a computer science graduate who may have the requisite knowledge to hack into a server.

In any complex investigation, proper record keeping and indexing of those records is essential. It not only helps with understanding the situation and generating new lines of inquiry, record keeping also provides an audit trail that can be scrutinised later and used to validate the investigating process. All investigations made on the server and the suspect's computer should be carefully logged throughout the investigation procedure. These records will help the examiner approach the evidence methodically and will identify more easily any gaps. The audit trail should also be sufficient to show that all reasonable lines of inquiry were followed and that a suspect's alternative account has been investigated and discounted. In the scenario this would include showing that his home computer had not been hacked by an unknown party.

Many analysts use standardised forms or checklists to document their analysis and to ensure that they perform all the necessary actions and examinations. Contemporaneous notes as to findings, conclusions and justifications for certain actions (or for actions not taken) should be kept throughout the investigation. Timestamps, where available, can help to validate such notes.

Of course, the documentation may also include screenshots, photographs and video records provided they are properly labelled and authenticated.

6.3.3 Specialist support

As already discussed, the technical nature of electronic evidence makes it necessary to use specialists who know where to look and how to extract evidential data. The circumstances of the case will dictate the kind of expertise required which may include particular skills in live forensics, reverse engineering of malware, or recovering data from damaged computer systems. However, no matter the level of skills and experience of the specialist, s/he will not be able to apply those skills without adequate resources and equipment.


This may include access to a fully equipped forensics laboratory furnished with appropriate software tools to automate certain examinations, facilities for imaging devices, secure storage in a climate controlled room protected by a Faraday cage and the sort of ancillary equipment such as that listed in 3.1.

6.3.4 Appropriate training

As with any professional, the digital forensics specialist needs to stay on top of all the new developments in his or her field. This means continuous professional education and regular reassessment of competency frameworks. The computer forensics world advances at the same pace as computer technology and forensic procedures used a year ago may already be outmoded.

In some cases, appropriate skills levels can be measured and assessed through formal training and certificates. A training framework delivered nationally on an interagency basis may have advantages and should be harmonised with international good practice.

Forensic examiners should be encouraged to meet and exchange information and knowledge with other forensics specialists and to develop cooperation with academia and industry in order to learn about latest techniques and developing trends. Regular meetings and workshops at the country level and international level can promote this.

 Apart from forensics specialists, there is also a need for capacity building at the level of investigators, first responders, judges and prosecutors. A range of comprehensive training concepts and materials are freely available and can be used as templates for developing national training initiatives. These include:

- The proposal for law enforcement training strategies prepared by the Council of Europe under CyberCrime@IPA;

Restricted

- The judicial training concept prepared by the Council of Europe under CyberCrime@IPA;
- The study on the co-operation between LE, Industry and Academia to deliver long term sustainable training to key cybercrime personnel (Octopus Interface 2009);
- Basic judicial training manual prepared by the Council of Europe under CyberCrime@IPA;
- Advanced judicial training manual prepared by the Council of Europe under CyberCrime@IPA;
- First responder training pack prepared by the Council of Europe prepared by the Council of Europe under CyberCrime@IPA.

These documents are available at www.coe.int/cybercrime.

Another excellent source for training materials on computer forensics topics is the European Cybercrime Training and Education Group (E.C.T.E.G). The course packs include student manuals, trainer manuals, lesson plans, slides and other teaching materials (e.g. images). E.C.T.E.G provides these courses free of charge exclusively to law enforcement only. The following courses were available at the time of writing:

- E.C.T.E.G Linux as an Investigative Tool (part 1)
- E.C.T.E.G Linux as an Investigative Tool (part 2)
- E.C.T.E.G Applied NTFS Forensics
- E.C.T.E.G Core Skills in Mobile Phone Forensics
- E.C.T.E.G Internet Investigations
- E.C.T.E.G Network Investigations
- E.C.T.E.G Wireless LAN and VOIP Investigations
- E.C.T.E.G Malware Analysis and Investigations
- E.C.T.E.G Forensic Scripting using BASH
- E.C.T.E.G Introductory Open Source IT Forensics and Network Investigation Course
- E.C.T.E.G Live Data Forensics
- E.C.T.E.G Macintosh Forensic Course
- E.C.T.E.G Network Forensic Intermediate Course
- E.C.T.E.G Solid State and other Storage media Forensic Course
- E.C.T.E.G Vista and Windows 7 forensics
- E.C.T.E.G Data mining and databases
- E.C.T.E.G Intermediate Mobile Phone Forensics

These tools are available via www.ecteg.eu.

Some computer hardware and software companies may also be able to provide additional information about their digital forensics products. Industry has played its part in assisting law enforcement in the provision of support forums based on their products that explain their forensics capabilities of their products.



6.3.5 Legality

As already discussed under 6.3 above, people are increasingly storing personal and confidential data on their computers and smart phones. Invariably any examination of an individual's computer system will occasionally expose private data that is irrelevant, confidential and possibly subject to legal privilege. Although there may be no intention on the part of investigators to intrude into or access such data, it is not always marked as personal and it can be impossible to judge where the confidential information starts and where it ends. Within the same email folder, there may be emails that are of interest to the investigation, some that are legally protected and many others that play no part at all in the investigation.

In some jurisdictions, if an investigator stumbles upon personal data outside the scope of the investigation, s/he is required immediately to cease viewing this data and to mark it as personal for future orientation. However, there are caveats, criminals are known to hide data in a folder labelled personal in order to mislead the forensic examiner.

We have already discussed the possibility of placing the disputed data under a court seal and preserving it subject to court decision as to its status.

6.4 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 |
|--|---|
| Thumbcaches Most Recently Used Lists Logfiles Browser Histories Browser Caches Most Used Programs Form Data Pagefile.sys Hiberfil.sys Volume Shadow Copies ... | Slacks Unallocated Space MFT Entries RAM Some application traces |

6.5 Types of forensic analysis



This section will provide examples of types of forensics analysis. It will give some insight into the challenges involved, but also show the evidential value forensic analysis can have.



6.5.1 File system analysis

Data storage devices store their information in a binary⁹⁵ format: meaning that the tiny building blocks that make up computer memory are stored as zeros or ones, or as on or off. These smallest particles are called 'bits'. To structure these bits methodically so that a computer system knows which bits go with which, computer science engineers have invented the file system. The file system can be thought of as the drawers of old fashioned hard copy index cards found in an analogue (book) library. The cards are 'indexed' or sorted (perhaps by author or title or subject) and cross referenced with locations in the building. Each card shows in which aisle, bookcase and shelf the book to which it refers is placed. In the same way a file system allows the storage and retrieval of computer files in a device.

⁹⁵ The basis of our usual numerical system is ten. In binary systems the basis is two.

Data storage devices may be subdivided into sections called 'partitions' and each partition must have a file system applied. Partitioning a hard disk is analogous to partitioning the library building with a new interior wall to create two separate, smaller libraries. Each mini-library will have its own index card systems. When a hard disk is divided up into two partitions it will be displayed as two different drives. In Windows the different drives would take different alphabetical labels such as drive c:\ and drive d:\.

It is also possible for one data partition to span more than one physical hard disk (typically in the RAID⁹⁶ system described in Section 2.2). When that is the case, the computer user will see only one data drive in the software interface (for example drive c:\), but in reality the C-drive is spanning two or more physical hard drives. What ties it all together is the RAID controller (be it a hardware or software RAID) and the file system that make either a part of a hard disk or multiple hard disks will appear as a single unit to the operating system.

The most common file systems are NTFS (New Technology File System) and FAT (File Allocation Table). The FAT system was created in 1980 and was used for the very first personal computers. It is still being used today because it is robust and widely compatible. Apple computers, Windows PCs, Linux, and most other software can read FAT partitions.

Microsoft Windows uses the NTFS file system, but Apple computers use HFS+, while Linux uses several different file systems such as EXT, BTRFS, XFS, or ReiserFS. In order to copy and analyse a device, the forensic examiner needs to identify how many partitions are on that device and what file system is being used. There may also be hidden partitions which the operating system does not immediately recognize, but which the computer user can mount or attach at will to access the content. The existence of other hidden areas like HPA (Host Protected Areas) and DCO (Device Configuration Overlay) that can only be opened through special ATA⁹⁷ commands also needs to be taken into consideration.

6.5.2 File recovery



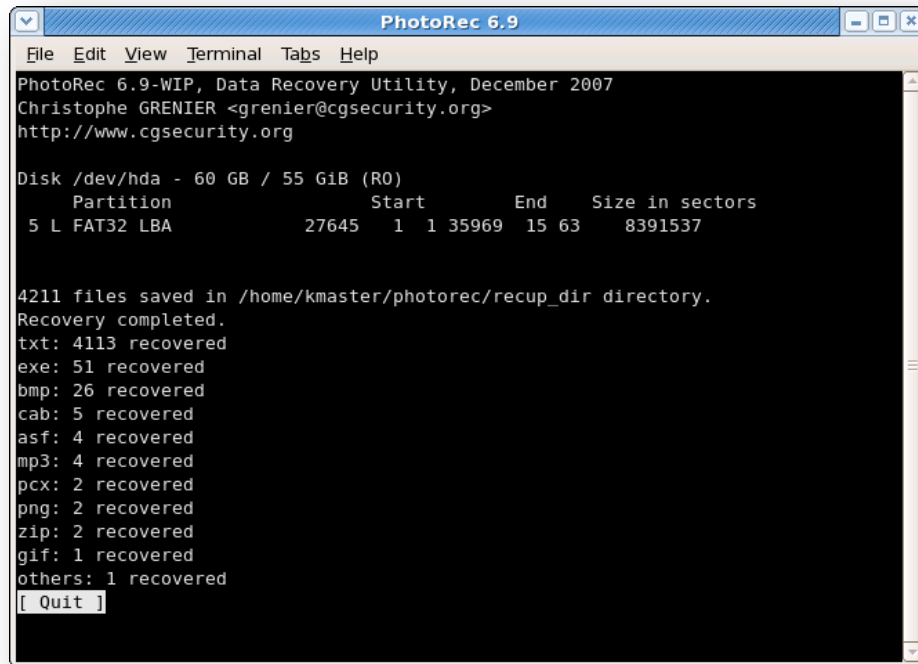
It is always worth checking the deleted files folder to see whether the user has concealed files there. Unlawful content in that folder will indicate the directory from which it was deleted which can then itself be searched of other evidence.

Even when the deleted files folder has been emptied, it may still be possible to recover deleted files. When a computer user presses the delete button, the file is not physically deleted from the data storage device, but marked as no longer wanted and references to the file's location are erased from the file system's index. The data will remain on the hard disk until the part of the disk where it is located is needed for another file or some other deliberate action is applied. This means it is possible to recover deleted files even when the file system no longer holds any reference to it.

⁹⁶ Redundant Array of Independent Disks – a mechanism for storing data across multiple disks.

⁹⁷ Advanced Technology Attachment is a mechanism for connecting computer drives.

A number of tools for undeleting files exist, including the free tools TestDisk and PhotoRec by CGsecurity.⁹⁸



```

PhotoRec 6.9
File Edit View Terminal Tabs Help
PhotoRec 6.9-WIP, Data Recovery Utility, December 2007
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk /dev/hda - 60 GB / 55 GiB (R0)
Partition      Start      End      Size in sectors
5 L FAT32 LBA   27645     1 1 35969 15 63   8391537

4211 files saved in /home/kmaster/photorec/recup_dir directory.
Recovery completed.
txt: 4113 recovered
exe: 51 recovered
bmp: 26 recovered
cab: 5 recovered
asf: 4 recovered
mp3: 4 recovered
pcx: 2 recovered
png: 2 recovered
zip: 2 recovered
gif: 1 recovered
others: 1 recovered
[ Quit ]

```

Software tools have been created by which files can be permanently deleted from hard disks. They do this by continuously overwriting the area on the disk where the file was located with various fake files until no trace of the deleted file is left. This is a simple anti-forensics technique, but is used relatively seldom. Indeed when anti-forensics are used, their use should raise the level of suspicion.

6.5.3 If the hard disk has been physically damaged it may still be possible to recover some of the files by disassembling the disks and carefully reading the magnetic information that remains. In the case of flash memory storage devices (such as SSD drives), which are substantially more robust than magnetic disks, the individual flash cells that make up the disk can also be examined for still functioning cells from which data can be retrieved. This is a highly specialised task requiring expert tools and knowledge. Searching the file system

The large size of data storage devices makes it all, but impossible to look at each stored file individually. To expedite analysis, most forensics analysts will first look in common data storage

⁹⁸ <http://www.cgsecurity.org/wiki/PhotoRec>

directories for suspiciously named files and directories. This technique of course is not sufficient when analysing hundreds of computer systems with several terabytes of data.

A second method of analysis is to use a search engine to search the file system for keywords of interest to the investigation. Some search engines also offer the possibility to search images (by performing image recognition and detection of things like skin tone). One image recognition tool available free to law enforcement investigators is NetClean Analyze.⁹⁹ This tool recognises common child abuse images and even modified copies of common child abuse images that have previously been reported to child abuse hotlines.

6.5.4 Dealing with file encryption



To protect their files criminals can make use of encryption technology to convert their files or even their entire hard drive into an unreadable code. Encryption technology is built into many modern operating systems: Bitlocker in Windows 7, FileVault in MacOS X, and eCryptFS in many Linux distributions. File encryption technology can also be independently installed such as PGP,¹⁰⁰ Folderlock or SafeHouse.¹⁰¹

Encryption modifies digital content by changing the bits, the zeros and ones, through the application of a mathematical operation that renders the content unintelligible. The only way to change the content back to the original content is by applying a reverse mathematical operation.

A forensics examiner who does not know or have access to the correct password or 'key' will find it practically impossible to access the encrypted data. It is possible to try various different decryption key combinations, one by one, but in practice decrypting the data would take several years, even with the help of the most powerful computers in the world.

Unless the suspect volunteers the decryption key there are limited options for the forensics examiner. S/he can try any passwords the suspect is known to use; look for word or number combinations that look like passwords near the machine or in the possession of the suspect, or try lists of passwords in common use (often words from the dictionary).

Some studies have shown that many users use easy-to-remember passwords such as 123456, password, qwerty, superman, or football. Lists of the most commonly used passwords can be easily obtained by searching the internet.

Where encryption keys have been supplied by the computer network, the network administrator will have a copy of the decryption key and may be able to decrypt the drive. This is the case for BitLocker encryption of computers in a Windows Active Directory.

⁹⁹ <https://www.netclean.com/en/analyze/investigations/analyze-di/>

¹⁰⁰ Stands for 'Pretty Good Privacy'

¹⁰¹ TrueCrypt was a leading file encryption software, but ceased to be available in 2014. It may still be found.

Because this is such a problem some countries have legislation that allows law enforcement under certain circumstances to obtain a court order to compel the computer owner to disclose a password for his encrypted storage device.¹⁰²

6.5.5 Document forensic analysis



Electronic document forensics (as opposed to hard copy document forensics) is different from data file forensics in that it focuses on obtaining as much information as possible about a file found on the computer.

Document forensics may be able to indicate who created a specific computer file, if the file was modified and whether any information has been hidden inside the file.

6.5.5.1 Metadata

Metadata, or data about data, consists of information about a file other than the content of the file. The file 'properties' can include the date and time that the document was created, when it was last modified and last accessed and by whom. This data can be extremely useful in linking files to individuals. For example, the creator of the Melissa computer virus, which affected millions of computers worldwide, was identified because of the metadata found in the source code of this macro virus.

As mentioned in Section 4.3.3 above, a digital photograph file often contains metadata in a part of the file called the EXIF¹⁰³ section. Any image viewing program and even the operating system can display EXIF information as part of the file properties. EXIF data will include the date and time the photo was taken, exposure time, focal length, serial number of the camera, and geographical coordinates of the place where the picture was captured.



When trying to establish the identity of someone who took a photograph, it is strong evidence if a camera found in a suspect's possession carries the same serial number as the one recorded in the image. EXIF data can be altered, but any alteration can usually be detected as much of the technical data of image in the EXIF section is interlocking.

Many mobile phones today also have a camera functionality and most smart phones can store the GPS coordinates in either fine mode (with a level of detail down to 10 meters) or in coarse mode by triangulating the distances to the nearby cell phone towers with an accuracy of a couple of kilometres.

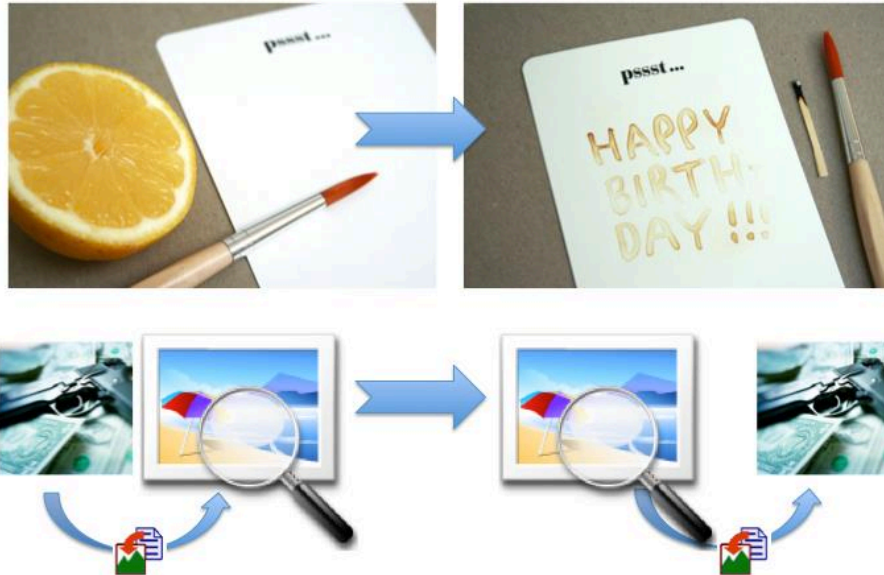
Most editable documents, including word processing documents, store metadata in the file. The document properties may contain the revision history of the document including the names of the users who modified it as well as the name of any printer used to print the document.

¹⁰² Examples are the United Kingdom (Part III of the Regulation of Investigative Powers Act 2000) and France (Article L 434-15-2 of the French Criminal Code)

¹⁰³ Exchangeable Image Format

6.5.6 Steganography

Steganography is a technique for hiding a message or other information inside a document file. It can be compared to writing a message on a blank piece of paper with magic ink or lemon juice that disappears when dry. Just like the magical ink on the paper, the hidden file is overlooked because it is concealed within something innocuous like a photograph or pdf.



A forensics analyst can identify a file hidden in this way by detecting an unusual distribution of light in the picture (histogram) or through a statistical analysis of picture files to see if they exhibit unusual properties. Once identified, steganography software can be used to attempt to extract the hidden file. A forensic examiner may be alerted to the possibility of hidden files if the suspect's computer system is found to have known steganography software installed.

6.5.7 Log file forensic analysis

Log file forensics aims to identify how a computer system and operating system have been used.

File system forensics may identify an unlawful file (such as a computer virus). Document forensics may identify that the file was created on the suspect's machine. The next step is to show that the suspect was the person who created the virus.

Log forensics can provide evidence on what software, processes and services were running on a machine and which users have logged onto the system and when. These forensics can be particularly valuable when seeking evidence of a third party having accessed the system illegally.

Log file forensic analyses what was happening on the system in a historical context while the live forensics analysis (as described in chapter 3.5.) questions what is happening here and now on a running computer system.

Log files are part of an operating system and are included in Windows, Mac OS, and Linux. They are used to record information about what the computer is/was doing and create a chronological record of the computer's events. The original purpose of a log file was to identify the causes of crashes in software to help software developers correct them, but log files also include records of interest for security professionals such as when a user logged in and when attempts to access the system were made.

Being able to analyse the chronological record and see who logged in, when they logged in, as well as which software or service was started and at what time, can help to show if a third party has accessed the system and could be very strong evidence of unauthorized access to a computer system.

Log files can also exist on an application level as, for example, in accounting software. Here the software log may record which user inputted a transaction in the ledger and analysis of an accounting software log can help unravel fraudulent records.

Microsoft Windows has provided, in parallel to the log file, something called a registry database. Its purpose is slightly different in that it records configurations of the computer system, but the registry can also be used for forensics purposes. It contains information about which external devices such as USB sticks are already configured to connect to the machine, for which network a computer is configured etc. It also stores the various networks, including WiFi networks, to which that computer system has been connected. The Windows Registry can potentially be useful for proving if a system was used in a specific place or if a USB key had been connected to it.



6.5.8 Network forensic analysis

The purpose of analysing network traffic is to identify the source of a communication or the source of an attack over the Internet. Often the forensics analyst already has a starting point either through the log file containing the IP address of the malicious communication sent to the computer, or the domain name and IP address of a website with illegal content, or possibly the header containing the route taken by an email with criminal content.

From this starting point, the examiner will look at links and relationships to other Internet resources both to help identify the perpetrator, but also as the associated links start to develop and reveal further criminal behaviour. If other malicious Internet resources are found, law enforcement may request that these be shut down.



6.5.9 IP addresses and the DNS

Section 4.2 provides a technical overview of the nature of IP addresses and the domain name service. The forensics analyst needs to look more closely at both IP addresses and domain names used by the perpetrator in order to identify linked Internet resources (such as other domain names hosted on the same Internet server) and identifying the Classless Inter-Domain Routing (CIDR) notation and the Autonomous System to which the IP address belongs. Identifying other domain

names and IP addresses used by the perpetrator gives a better overview of all the potential unlawful activities of the suspect and may also help in providing additional information by which to identify him or her.

The following sub-sections will look at the forensic analysis of email and Internet searches.

6.5.9.1 Email forensics analysis

Email forensics examines the email source text to identify from where the email message was sent. Email software normally hides the technical information that is in the email message from the reader. Such information is called the email header (or sometimes the extended header). The email header will be in a common standardised Internet format (RFC 2822), however the method of revealing the header information varies depending on which email client is used.

Each time an email server, also known as a Mail Transfer Agent (MTA), receives an email message and passes it along to the next MTA on its journey to the recipient, it stamp adds a line in the email header showing the IP address from which it was received as well as the time.

By reading the email header it is possible to follow the path that the email travelled on its way to the recipient's inbox.

Below is an example of an email header from an email message with the subject "Email header" and the body text "This is the body text":

```
Delivered-To: forensics@forensics.com
Received: by 10.229.233.207 with SMTP id jz15csp53304qcb;
      Wed, 30 May 2012 00:37:09 -0700 (PDT)
Received: by 10.68.130.9 with SMTP id oa9mr46792071pbb.95.1338363429020;
      Wed, 30 May 2012 00:37:09 -0700 (PDT)
Return-Path: <forensics@hotmail.com>
Received: from bay0-omc2-sl6.bay0.hotmail.com [65.54.190.91]
      by mx.google.com with ESMTP id
      rg2sil7612042pbc.261.2012.05.30.00.37.08;
      Wed, 30 May 2012 00:37:08 -0700 (PDT)
Received: from BAY157-W32 ([65.54.190.123]) by with Microsoft
      SMTPSVC(6.0.3790.4675);
      Wed, 30 May 2012 00:36:32 -0700
Message-ID: <BAY157-W32F746CCEC9B74654CC7C0A40A0@phx.gbl>
Return-Path: forensics@hotmail.com
X-Originating-IP: [84.169.25.82]
From: Forensics <forensics@hotmail.com>
Sender: <forensics@hotmail.com>
To: <forensics@forensics.com>
Subject: Email header
Date: Wed, 30 May 2012 07:36:51 +0000
Importance: Normal
MIME-Version: 1.0

This is the body text.
```

Identifying the sender of the email message can still be challenging if the sender hacked into someone's computer to send the email, for example, by using a botnet. A sender can also hide his tracks by going to a public location such as an Internet café. The sender IP address will belong to the café and not point back to him or her.

Where analysis reveals that the sender machine was possibly hacked, live forensics and log file forensics will need to be performed to identify the origin of the hack. If the email was sent from a public location such as a hotel lobby or an Internet café, old fashioned detective work can be used to help identify the customer using the public computer at the time the email was sent. It is also important to note that most of the information in an e-mail header can be manipulated since they are added by different e-mail servers which might not be trustworthy. Basically this applies to all information at the bottom of an e-mail header because it comes directly from the sender's mail server (which could be under the control of the suspect). The information that is located at the very top of the header is more reliable since it was added by the mail server of the receiver.

6.5.9.2 Internet searches

A user's Internet searches can reveal much about him or her. For example, in a case where a husband reported his wife as missing, the police searched the home computer to see if the missing spouse had left clues indicating where she might have gone. When preparing a trip, computer users will often search the Internet for information about the place they are visiting or for a hotel room. In



this case, police looked at the search history on the home computer and discovered that the computer had been used to search the Internet for "How to murder someone and not get caught" and "killing someone quietly". This revelation shifted the police mind set.

All searches and webpage views are available in the history section of the browser, whether Internet Explorer, Mozilla Firefox, Opera, or Google Chrome, and can be invoked by pressing Ctrl+H in Windows and Linux, or Command+H in Mac OS. The search engines Google and Bing keep the search history on their servers for several years. Google keeps the user's search history at the address <http://www.google.com/history>, and Windows Live (Bing) displays the search history at the address <http://www.bing.com/profile/history>. Once logged in, the search history of a particular user account will show the searches made using these engines from a user's mobile phone, office computer, and home computer all stored in one central place.



6.6 Connected services on seized devices

A seized device may be connected to a number of online services that contain further information of interest to the investigation. For example a device may be configured to automatically log onto a social network account, a VoIP account or an email account etc., and have passwords preregistered in the browser for a number of websites. Access to this information can be very valuable for the investigator.

The device may have a connection open to a cloud data storage account, providing access to files stored by the user on the Internet that are not stored locally on the device. Access to the browser of the device may also reveal a number of common passwords to try against other online services used by the device owner. In the Firefox Options dialogue box, under the security section, it is possible to click a button to view any of the users passwords stored by the browser.

To which extent a specialist examining the device is allowed to access remotely stored data, in particular data stored outside of the specialist's jurisdiction, will depend on the national law that applies and cannot be answered in this Guide.

Similarly any email account using either IMAP, Microsoft Exchange Server, or Gmail services can store the content of a user's email account locally on the device for offline use. However, understanding if the specialist is accessing the emails locally on the device or remotely on a server can be challenging to answer with certainty. Forensic examiners need to be alert to the possibility that they may inadvertently be contravening international legal rules on jurisdiction.

7 Preparation and presentation of the evidence

7.1 Use of electronic evidence in court proceedings

This section complements section 1.6 which discusses the principles of electronic evidence.

The use of electronic evidence has increased in the past few years as courts have had to admit and consider electronic evidence in the form of e-mails, digital photographs, ATM transaction logs, word processing documents, instant messages, spreadsheets, Internet browser histories, databases, the contents of computer memory, computer backups, computer printouts and digital video and audio files – all of which constitute digital data.

A digital device involved in crime should be secured just as you would with other forms of physical evidence found at a crime scene, because all such devices remain physical evidence. As with fingerprint and DNA evidence, digital evidence is fragile and easily lost or altered if appropriate precautions are not followed. In the early days of dealing with digital evidence, untrained members of law enforcement switched on computers to look for evidence before submitting them for a forensic examination or switched devices off and lost the data and potential evidence lost in the RAM.

It is important to record where the digital device was found and seized, because it can reveal a great deal about the intent of the suspected offender. It is good practice to record the search and seizure by video. This will show the position of digital devices, so that there is no longer an argument, for instance, as to whether the wireless device was found hidden in the loft rather than in an open access area in the sitting room.

7.2 Evidence in criminal proceedings

7.2.1 Admissibility

Computer Evidence is admissible if it conforms to a series of laws and rules that ensure it is acceptable to the court. The proper procedures must be followed when obtaining evidence. These are articulated in the preceding chapters.

7.2.2 Authenticity

Electronic evidence is no different to physical evidence, such as a document recorded on a piece of paper. It is necessary to ensure that the evidence is authentic. The difference between electronic evidence and physical evidence is usually the ease with which electronic evidence can be changed and altered, either deliberately or inadvertently.



7.2.3 Convincing

In the event that there is a doubt about electronic data adduced in evidence, it is for the defence to raise a challenge to its admissibility. Once the issue is raised, the prosecution has to deal with it, usually by providing sufficient evidence that the integrity of the data is trustworthy, and is therefore considered to be reliable.

Another important aspect of evidence is how it was obtained and whether the methodology by which that evidence was established is amenable to objective, scientific validation and review. For instance, if the prosecution can produce a telephone bill showing that the defendant connected to his ISP at a certain time of day, then this will be usually accepted. By contrast, if the prosecution claim that 'The defendant deleted all the files on his hard drive, reformatted it, then threw it out of a 10-storey window, but we've been able to reconstruct the files by going to a data recovery firm', then the defence may question the validity of this method of recovering the evidence. It is for the prosecution to demonstrate that the methods used to recover the evidence were valid and convince the court that the evidence should be admitted.

It is necessary to strike the right balance. On the one hand, it is not reasonable to expect the deciders of fact (whether members of a jury or a single judge) to understand technical minutiae. On the other hand, it is inappropriate to expect them to accept data recovery techniques as 'magic'. In some countries, the response is peer review – if other specialists in the field have studied the technique, tested it, and validated the results then the court will accept the evidence.

It is worth repeating, electronic evidence is dealt with in court in the same way as any other form of evidence. The prosecution will have to prove that the document is authentic and its contents are admissible. All dealings with electronic evidence must conform to the principles of electronic evidence set out in this Guide.



7.3 Explanation of the principles

When considering evidence in criminal proceedings it should be remembered that electronic evidence is subject to the same rules and laws that apply to documentary evidence. The doctrine of documentary evidence may be explained thus: the onus is on the prosecution to show to the court that the evidence produced is no more and no less now than when it was first taken into the possession of law enforcement. Operating systems and other programs frequently alter and add to the contents of electronic storage. This may happen automatically without the user necessarily being aware that the data has been changed.

As already discussed in Section 6.2, wherever practicable, an image (duplicate) should be made of the entire target device. Partial or selective file copying may be considered as an alternative in certain circumstances, for instance when the amount of data to be imaged makes this impracticable. However, investigators should be careful to be able to show that all relevant evidence is captured if this approach is adopted.

In a minority of cases, it may not be possible to obtain an image using a recognised imaging device. In these circumstances, it may become necessary to obtain access to the original machine to recover the evidence. With this in mind, it is essential that a suitably qualified digital evidence specialist, who is competent to give evidence in court, obtains the evidence.

At trial it is essential to display objectivity, as well as the continuity and integrity of evidence. It is also necessary to demonstrate how evidence has been recovered, showing each process through which the evidence was obtained. Evidence should be preserved to such an extent that a third party is able to repeat the same process and arrive at the same result as that presented to a court.

7.4 Disclosure

Each jurisdiction has different rules and procedures for disclosing evidence to the defence. Usually, the investigator has an obligation to pursue all reasonable lines of enquiry whether these point towards or away from the suspect. The deletion of any law enforcement generated material or third-party material in possession of law enforcement, prior to their respective retention periods, may amount to a breach of procedure if they are not available for disclosure with fatal consequences for the prosecution case. In practice this means that law enforcement generated evidence should always be accompanied by a full audit trail, from the point of its capture until it is passed to the prosecution and throughout the whole management process.

7.5 Unused material

In some jurisdictions, unused material is material that may be relevant to the investigation and has been retained, but does not form part of the case for the prosecution against the accused. The principles of disclosure apply to electronic evidence in the same way as any other material obtained in the course of an investigation. It is a matter for the investigator to decide which material it is reasonable to enquire into, and in what manner.

Any material that has not been examined should be described by general category with the extent and manner of any inspection or examination of the material being recorded with a justification for not having examined it as part of the investigation.

It is preferred that, whenever possible, information or data is provided to the prosecutor in its original format, because transferring it on to a different format or media will not create exact copies and some loss of the original quality will occur. Any conversion to a different format from the original format should include consideration and assessment of the copy's quality. Effort should be made to capture and store evidence in standard formats that are readily available to the prosecutor and court system. In circumstances in which the local prosecutor is not able to readily view material in its original or native format, arrangements should be made to facilitate examination or convert it into another format. Local protocols, including service level agreements, should be developed to ensure that prosecutors are able to view evidence quickly in order to make timely decisions.



7.6 Care of victims and witnesses

The European Convention on Human Rights requires public authorities to act in ways that are compatible with the human rights of victims and witnesses. These rights must, however, be respected and balanced against those of the defendant.

If the evidence in the case is sufficient to justify a prosecution, the interests of the victim are an important consideration. Consideration has to be given to the effect of the offence on the victim. This is particularly important in cases involving abuse of children and the potential for prosecutions related to digital images of such abuse.

Many witnesses to crimes may feel stress and fear during the investigation of a crime, and subsequently when attending court and giving evidence. Stress can affect the quantity and quality of testimony of witnesses of all ages. Some witnesses may have particular difficulties attending court and giving evidence because of their age, personal circumstances, fear of intimidation or because of their particular needs. Extra provision should be made available for vulnerable and intimidated witnesses to help them give their best evidence in court and to relieve some of the stress associated with giving evidence.



7.7 Court presentation

Presentation is important if lawyers, judges and, where the system provides for one, the jury¹⁰⁴ is to give expert evidence the weight it deserves. Presentation of electronic evidence to the court is more effective if it is visual, using computer demonstrations, video demonstration, computer graphics, schedules and charts. However, prosecutors should be aware of the bias that using such technology can cause, and be prepared to discuss these issues with authority if the defence challenges the use of such technology.

Research has found that many people give more attention to what they see rather than hear. Since a prosecutor's duty is to put forward the prosecution case in the best possible light, visual presentation of evidence especially in complicated cases is advisable.

One example of how to develop a prosecutor's skills in visual presentation of electronic evidence can be found in a training programme for interns and prosecutors in Georgia.

All interns of the Prosecution Service who have successfully passed entry exams and an interview are obliged to undergo an intensive one month course for practical preparation for prosecutorial work. The course includes an obligatory three day course on trial skills structured around the process of presentation of evidence in the court. It requires prosecutors to master logic, attention, posture, control, tone and other elements necessary for presenting the case and its arguments to the a tribunal of fact. The use of flipcharts, projector devices, PowerPoint presentations, diagrams

¹⁰⁴ Juries are a feature especially of the Common Law system that holds the principle that an accused should be judged by a panel of his or her peers. Where they exist, juries are deciders of fact while the judge is the decider of law.

and other visual material is highlighted throughout the course and is a requirement for successful prosecution in complex cases (cybercrime cases being one such example). Another aspect highlighted throughout the course is the direct cross examination of expert witnesses who are often the key to successful trials in cybercrime cases.

It is notable that the trial skills course is obligatory not only for starting prosecutors, but also for those who are already working in the Prosecution Service. In 2006 and 2010, all of the prosecutors received training and re-training in trial skills (including advanced training from US and UK prosecutors).

The two day legal writing course for prosecutors and Prosecution Service interns is also obligatory and taught to interns as a part of their preparation program as well as to serving prosecutors as a part of re-training programmes. The use of pictures, diagrams, descriptive figures, charts, etc. is strongly encouraged and adds a visual element to the presentation.

It must be noted that the above-noted experience of Georgia in giving trial skills and legal writing training to prosecutors is not centred on cybercrime cases, but is rather a universal skill-set that can be used in complex trials involving issues that may be difficult to comprehend by the judge and the jury, cybercrime cases being a classic example of such complex material.

8 Jurisdiction

8.1 The international dimension of cybercrime

In the networked world, national frontiers could be said to facilitate cybercriminals, but to constrain criminal justice. Criminals on the internet travel across continents 'virtually' at will. Although the involvement of multiple legal jurisdictions is the rule for any cybercrime investigator, s/he does not enjoy the same freedom of movement in pursuing evidence of a crime. The circumstances in which a law enforcement agent can lawfully investigate outside his or her own country (including in terms of evidence stored in the 'cloud') can be very different depending on national law and whatever Mutual Legal Assistance frameworks have been joined by the investigator's government.

There are two sets of circumstances that are important to distinguish when dealing with electronic evidence that is not physically located within the jurisdiction:

1. Where an investigator has taken control of a computer that is connected to the Internet. In such circumstances, the investigator may have the power to click on websites or enter computers in other jurisdictions. The authority to do so may be given to the investigator by virtue of domestic law or a combination of domestic law and the provisions of Article 32 of the Budapest Convention on Cybercrime. (However, the country where the actual servers or computers are physically located may take another view).
2. Where electronic evidence is located in the 'cloud' – that is, where the e-mails of a suspect, for instance, are not stored in their home computer, but are stored elsewhere on a separate hard drive in a foreign jurisdiction.

It is important to understand the difference between these two sets of circumstances because investigating authorities will have to take different actions in each situation depending on the laws that apply.

8.2 International justice cooperation networks

There are various measures that have been taken internationally to respond to cybercrime. The most relevant ones include Interpol, the Council of Europe and developments by the European Union (the Contact Point Network, Europol, Eurojust and the European Judicial Network in Criminal Matters). The resources of these groups may be available to different players in the criminal justice system to assist them in investigations or prosecutions.

8.3 Mutual Legal Assistance

There has long been a formal framework by which one sovereign state has been able to request another sovereign state for assistance in legal matters. The most common legal basis for this

cooperation is the Mutual Legal Assistance (MLA) Treaties and multi-lateral Conventions that provide for mutual assistance (such as the UN Convention on Transnational Organised Crime). Cross border requests for assistance are particularly important in cases involving electronic evidence because of the international nature of Internet services. The real challenge in these cases is to be able to act quickly enough to prevent evidence from being altered or deleted, but traditional forms of international cooperation are slow and cumbersome and the success of such a request often depends on the goodwill and level of expertise of both the requesting and the requested authorities.

8.4 Cross-border cases

When a case crosses a number of jurisdictions, the substantive law for each jurisdiction must be considered. This can be a complex area and sometimes a decision is taken to allow a single team of investigators in one jurisdiction to take the lead. The relevant agencies in the other jurisdictions will agree to cooperate with the lead investigative agency and to secure relevant evidence in their own jurisdiction.

Article 35 of the Budapest Convention offers some practical assistance to investigators in that it requires each Party to 'designate a point of contact available on a twenty-four hour, seven-day-a-week basis.' The purpose of this is to promote 'immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.'

Parties to the Convention are expected to carry out a number of other measures, providing their domestic law and practice permit. These are as follows:

1. The provision of technical advice;
2. The preservation of data pursuant to Articles 29 and 30;
3. The collection of evidence, the provision of legal information, and locating of suspects.

These measures can play an important role in facilitating the effective and efficient work of investigations dealing with crimes that include an element of electronic evidence across jurisdictions.

9 Role specific considerations

There are a number of considerations that are specific to the various roles in cases involving electronic evidence:

- Investigation management
- Chain of Custody
- Examination of evidence (laboratory actions)
- Impact on subjects of searches (e.g. corporate networks)

- Safeguards privacy considerations, proportionality, collateral intrusion

9.1 LEAs, possibly all investigative authorities



There is no need to provide role specific information for law enforcement as all the considerations addressed in this section are already dealt with in the preceding chapters.

9.2 Prosecutors

9.2.1 Management of investigations



Investigators, prosecutors, defence representatives and judges all need to understand information and technology. Cases can fail if the prosecutor is not able to identify all the issues that need to be decided in a case and to present them simply and concisely to the court, especially if technical aspects are involved. Prosecutors and investigators need to be trained and equipped with specialist skills and knowledge to investigate and prosecute, especially when new technologies are involved.

Prosecutors need to be able to determine the most appropriate jurisdiction for a prosecution in cross-border crime matters and be able to use the latest technology to present that evidence at court. This may mean that court hearings must be equipped with additional technology to facilitate the presentation of the evidence.

Depending on the country, prosecutors must work side by side with law enforcement or otherwise be available to advise on measures to avoid legal pitfalls, maximise evidential opportunities and develop strong, robust and well-presented cases at court. Prosecutors must uphold the core values of independence, impartiality and fairness in everything that they do.

9.2.2 Management of prosecutions



The right to a fair trial is sacrosanct, and the responsibility of the prosecution team in terms of gathering, preserving and presenting electronic evidence to a court fairly and objectively remain uppermost. Each member of the prosecution team will have a clearly identified role to play. There should be regular case conferences between the prosecutor and the investigators and other relevant personnel throughout the life of the case. After prosecution, there should be formal debriefing sessions involving all participants to help both identify and disseminate any lessons to be learnt.

Because cybercrime knows no geographical boundaries prosecutors have an increasing role in facilitating cross-border liaison and in obtaining electronic evidence through mutual legal assistance.

Prosecutors need to be proactive in identifying, and where possible, rectifying deficiencies in electronic evidence and to bring an early conclusion to those cases that cannot be strengthened by further investigation.

It is important to keep in mind that each case is unique and must be considered on its own facts and merits (and in the context of the national law that applies) to be able to determine accurately what measures are needed to ensure the result of the investigation.

9.2.3 Disclosure to the defence

As discussed in Section 7.5, any investigation will produce material that will not be relied upon in court. The right for a defendant to receive a fair trial is enshrined in Article 6 of the European Convention on Human Rights (ECHR) and it is important for an investigator to identify any material that might either undermine the prosecution case or assist the defence case. Where court practice requires the prosecution to prepare schedules of prosecution evidence for the defence, the investigator should ensure such unused material is properly highlighted.

Prosecutors must do all that they can to facilitate proper disclosure under the relevant legislation, as part of their general and professional responsibility to act fairly and impartially, in the interests of justice and in accordance with the law. Prosecutors must also be alert to the need to provide advice to, and where necessary, probe actions taken by investigators to ensure that disclosure obligations are met.

9.2.4 Admissibility of evidence

Digital evidence in criminal trials, as discussed in Section 7 above, must be admissible, authentic, accurate and complete. It must conform to applicable laws and rules and be acceptable to the court.

In reviewing the case, the prosecutor will consider if it is possible to explicitly link files (data to specific individuals and events) and to explain how an exhibit came into being by showing an unbroken continuity of evidence.

During criminal trials, the prosecutor must use evidence to prove the case to the criminal standard (in many countries this means 'beyond a reasonable doubt'). As part of the rules of evidence, the court is always entitled to be presented with the best evidence. Traditionally, best evidence is the original document, but under certain circumstances, secondary evidence can be accepted. Typically secondary evidence comprises copies or extracts of the best evidence.

An early review by the prosecutor of the electronic evidence in a case, which help to determine whether the evidence is sufficient, where there are weaknesses and where further electronic evidence is required. If this is done at an early stage there may still be the opportunity to obtain additional evidence from other jurisdictions before the case goes to trial.

At the heart of the role of the forensic witness lies the production of reports relating to the electronic evidence obtained, statements and the rebuttal of opposition reports where appropriate. The prosecutor should encourage short statements, clearly divided into fact and opinion, so as to allow for clarity on the witness' thought processes and findings. The prosecutor should request

supporting documentation to be supplied as appendices if necessary, rather than in an unnecessarily bulky document.

A short report can be a good report; a long report is not necessary if no one is able to read it all the way through.

Having reviewed the report(s) (and where it is appropriate under national criminal procedure) the witness should be asked for specific information and explanations on points that the defence is likely to raise – particularly in respect of any contradictions contained in the statements of opposition witnesses. It can also be very useful if the witness prepares an agreed a glossary of terms to be used in the case.

During the pre-trial period (and if necessary during the main trial) the prosecution may find it helpful to meet the defence to discuss the scope of electronic evidence and its availability/content in order to clarify the evidential situation.

The evidence given by the forensic witness should be:

- Credible
- Impartial
- Clear

9.3 Judges

9.3.1 The investigative role of the judge

As judges play a crucial role in court, they must also understand the technical aspects of electronic evidence as well as where and how evidence may be located. They also need to have an understanding of the technology and applications from which digital evidence is derived in order to make robust and appropriate decisions on its admissibility.

As with other forms of evidence, digital evidence must be properly authenticated. Judges should deal with electronic evidence in civil or criminal proceedings in the same way as any other evidence and ensure it conforms to three broad principles:

- Admissible;
- Authentic (including accuracy and completeness);
- Persuasive.

Judges determine what evidence is to be admitted in a case and make rulings on specialist and expert testimony. In many jurisdictions judges decide on the facts as well as the law. Such decisions must be made from an informed perspective. Any hi-tech case may involve prodigious amounts of material, much of it of a complex and technical nature. Judges need to be able to manage such cases and to be able to distinguish between those applications that have merit and those that do not.

9.3.2 The role of the expert



Legal proceedings recognise that there may be things beyond the knowledge of the court that need explaining by someone who has greater understanding and experience of a particular subject. This person is the 'expert' witness and is distinguished in his or her role because s/he is able to discuss opinion and not just the facts known personally to him or her. A judge must be able to assess the qualifications and level of knowledgeable insight an expert brings to the case.

The rules on who can and who can't be an expert witness vary from country to country. In some there are well developed requirements;¹⁰⁵ in others the situation is less prescriptive.

An expert witness must be independent and impartial. S/he owes a duty to the court and should bring to the attention of the court any weakness or limitation on the evidence that is provided.

Some criteria are discussed in Section 2.6 for an 'independent consulting witness'. In many cases these would also apply to the expert witness.

9.3.3 Dealing with unused material

In any investigation, there will be material that will not be relied upon in evidence. In order to ensure that a defendant has a fair trial, the judge should ensure that the prosecution has properly discharged its disclosure responsibilities.



9.3.4 Jurisdiction

Judges will also be required to decide upon the merits of applications related to mutual legal assistance involving electronic evidence – in particular when it comes to the need to issue court orders for investigators to access records and data held by service providers - and in questions of extradition of criminals to face trial in countries where criminal justice can have a very different approach. There may even be the need to rule on disputes over the most appropriate country in which to hold a trial.

As has been repeated throughout this Guide, an understanding and appreciation of the technical aspects of electronic evidence will make such decisions easier for those involved and this includes the judge.

9.4 Non-criminal proceedings



The increased use of electronic evidence to adjudicate civil matters (i.e. legal disputes between private entities) is a natural consequence of human communication moving from paper-based to electronic systems. Important business deals are concluded without ever seeing a piece of paper through email exchanges or bidding platforms. One spouse may deceive the other and leave behind evidence in the form of SMS messages. A company may improperly obtain inside

¹⁰⁵ See for instance Federal Rule of Evidence 702 in the USA.

information on the business dealings of a competitor. These are all potential investigations the outcome of which will depend on digital examination and analysis of electronic evidence.

A forensic investigation in the civil sphere needs even more careful preparation. Investigators in the private sector do not have the same legal powers as those working in competent authorities and it is essential to acquire appropriate legal authorisation for any activity involving third party computer systems or electronic devices. Parties involved in civil litigation will normally strongly resist any disclosure of business confidential information or personal information to the other side. The civil courts will usually impose strict requirements and limitations before authorizing the seizure of data from computers or devices of third parties.



9.4.1 Preparing the seizure of data

Computer forensics work, in private sector cases, normally begins with a consultation with the client. This meeting or series of meetings will establish the nature of the legal claims, the client's requirements and expectations and will determine the most appropriate procedures and strategies to be applied. It is extremely important that the forensics specialist ensures that the agreed terms of reference are in writing, formally approved by the client and that they clearly state the scope, responsibilities and limitations of his or her involvement.

During the consultation, where possible, the type and range of electronic devices should be identified and the nature of the electronic evidence sought should be determined. Depending on the issues to be reviewed, data capture may only be needed for internal administrative purposes or it might be apparent from the outset that potential criminal liability will follow. If the data needs to be captured in a way to ensure that it is admissible at court, it is recommended that the parties make use of qualified computer-forensics specialists familiar with such requirements.

Once these formalities have been completed and the target devices have been identified the process for capturing the data will need to be planned. Obtaining data from devices or a network without consent of the owner inevitably means an application to the court for a court order.



9.4.2 The data capturing process

As already explained numerous times in this Guide the content of any electronic device must be handled and preserved in such a way as to be able to guarantee that it has not been modified or manipulated. To do otherwise would be to undermine the value of any evidence obtained from it.

A strategy will need to be designed on how to get access to the data (particularly if it is held by a non-compliant party to the litigation). Can it be achieved through written consent? Or will it be necessary to obtain a court order?

Once the necessary authorisation has been obtained, the actual process of capturing the data is the same as in Sections 3.4 and 3.5 above, but without seizing the devices. The investigator will

make an exact 'bitstream' copy of the electronic contents of the device (see Section 6.2) that will serve as the master copy from which working copies will be made. The master copy will then be sealed and remain untouched, but can be used as a point of reference in any subsequent dispute.

The data collection strategy should also consider if it is necessary and/or desirable to inform the owner or user of the identified electronic device that the capture process that will take place, or if whether the procedure can be ex parte. In the business environment (as already mentioned) staff at a third party facility may in any case be contractually obliged to notify the subject or owner of the data that it has been accessed and copied. Having that individual present may help protect his or her rights, but may present other problems in terms of interference and obstruction.

In some cases, company policy and procedure may permit senior management to authorise access to company devices used by an employee without the need for a court order or that employee's consent. In other situations the employees' rights to privacy will take precedence.

Civil procedure varies greatly from jurisdiction to jurisdiction, but most civil procedure laws carry a presumption of evidence where a court appointed legal officer (such as a public notary or a bailiff) produces the evidence to the court. If this is the case, it might well be useful to involve such a legal officer in the evidence gathering process. The legal officer can assist both during the seizure but also in the post-seizure phases such as the cloning of the data when additional copies are needed. In many instances the legal officer will also be able to attest that the evidence remained in his or her custody and was not altered.

Whether a legal office is co-opted or not into the data capture and copying, it is highly recommended that the actions taken during the capturing process be logged in contemporaneous notes and/or (as mentioned in this Guide) on video.

If the log or minutes are kept by a legal officer (public notary, bailiff, or other) in a document that s/he can authenticate, the capturing process will be afforded a greater guarantee as to the reliability, integrity of the seizure.

It need not be repeated that any one actually conducting technical operations on the device should be properly skilled and experienced in the procedures s/he is expected to perform.

9.4.3 Chain of custody of the seized data



As described in the first principle of electronic evidence (section 1.7.1) and in various subsequent sections throughout this Guide, the Chain of Custody is an essential step in preserving and proving the integrity of the data.

In some limited cases, it might also be feasible to seize the device itself provided there will be no economic hardship or commercial prejudice to its owner. In doing so the same rules on labelling, packaging and storing will apply as described in Section 3.4.1. If physically feasible, consideration

might be given to lodging any such device with a legal officer for safekeeping (if the appropriate storage conditions can be reproduced).

Before returning any seized data storage device to its owner, care should be taken to ascertain that there is no illegal data such as child abuse images, illegally obtained third parties personal information, login names and passwords, payment card details etc. Consider placing a warning to this effect in the examination report.

9.4.4 Forensics analysis

Once the data is seized the technical analysis methods will be identical for both criminal and civil legal proceedings.



10 Cases



10.1 Criminal cases

10.1.1 Admissibility of computer printout as evidence

R v Wood (Stanley William) (1983) 76 Cr. App. R. 23

In this English case a quantity of metal was stolen in transit. Metal of the same type was found in Mr Wood's possession and he was charged with handling stolen goods. In order to establish that the metal handled by Mr Wood had formed part of the stolen consignment, the owner's records on the chemical composition of the consignment (consisting in part of printouts from a computer used to conduct complex calculations) were compared with the results of a chemical analysis conducted on the metal seized from Mr Wood. The composition of the metal was found to be an exact match

At his trial Mr Wood objected to the admission of the computer printouts in evidence. The trial judge overruled that objection and oral evidence, not otherwise disputed by the appellant, was given by the chemists and the programmer of the computer software (the record keepers) about the actions they had taken. Mr Wood was convicted and he appealed.

In dismissing the appeal the Court of Appeal held that the computer had been used merely as a calculator for performing calculations that could not have been done manually - it was a tool (analogous to a piece of litmus paper used to test acidity or a weighing machine). The printouts were real evidence proved by the oral testimony of the programmer of the device.

Comment: In cases where a computer is used as a calculator and its programming and use are both proved by oral evidence, the printout produced is not hearsay evidence.

10.1.2 Unauthorised modification of a computer

Director of Public Prosecutions v Lennon, Queen's Bench Division (Divisional Court) Hearing Date 11 May 2006 Citation: BLD 1205061482.

This was the first case in the UK relating to denial of service attack. David Lennon was charged that, between 30th January and 5th February 2004 he caused an unauthorised modification to a computer belonging to Domestic and General Group Plc ("D&G") with intent to impair the contents of the computer. The facts were that Mr Lennon was employed by D&G for three months until he was dismissed in December 2003. He was then 16. On 30th January 2004 Mr Lennon started to send emails to D&G using a "mail-bombing" program called Avalanche V3.6 which he had downloaded from the Internet. The program was set to "mail until stopped". That meant it would continue to send emails until it was manually stopped from doing so. It was estimated that Mr Lennon's use of the program caused approximately 5 million emails to be received by the D&G email servers.

The company's email server crashed and Mr Lennon was summonsed for unauthorised modification of the contents of a computer contrary to section 3(1) of the Computer Misuse Act 1990 (CMA).

The prosecution case was that by his actions in relation to the Avalanche program Mr Lennon caused an unauthorised modification to the contents of D&G's computers by adding data to their contents, that is to say, the half million emails which he caused to be sent, and that when he did so he had the requisite intent and the requisite knowledge. It was alleged that he had the requisite intent because he intended to hinder the operation of the computers by overwhelming them with the emails, and that he intended thereby to prevent or hinder access to their programs and data, and to impair the operation of their programs and the reliability of their data. It was alleged that he had the requisite knowledge as provided because he knew that the modifications he intended to cause by adding the emails to the data in the computers were unauthorised.

In the Youth Court Mr Lennon successfully argued that that there was no case for him to answer as the function of the company's email server was to receive emails, D&G had consented to receive emails and so D&G authorised potential senders of emails to modify the contents of the server by sending them.

The prosecution appealed and the Divisional Court found that there was a case to answer and ordered a retrial. The Divisional Court stated that although the owner of a computer able to receive emails ordinarily consents to receipt of email, such implied consent is not without limits, and the consent did not cover emails sent not for the purpose of communicating with the owner, but for the purpose of interrupting the operation of the system.

10.1.3 Employee obtained unauthorised access to a computer

R v Bow Street Magistrates Court and Allison (AP) Ex parte Government of the United States of America (Allison) [2002]2 AC 216

On 18 March 1997, Mr Allison was arrested upon a provisional warrant issued under the Extradition Act 1989 at the request of the Government of the United States. It alleged that he had between 1 January 1996 and 18 June 1996 within the jurisdiction of the United States of America conspired with Joan Ojomo and others -

- a) To secure unauthorised access to the American Express computer system with intent to commit theft,
- b) To secure unauthorised access to the American Express computer system with intent to commit forgery, and
- c) To cause unauthorised modification to the contents of the American Express computer system.

Joan Ojomo was an employee of American Express. She was assigned to the credit section of the company's office in Plantation, Florida, as a credit analyst. In her daily work it was possible for her to access all customer accounts, but she was only authorised to access those accounts that were assigned to her. However she accessed various other accounts and files which had not been assigned to her and which she had not been given authority to work on. Having accessed those accounts and files without authority, she gave confidential information obtained from those accounts and files to, among others, Mr Allison. The information she gave to him and to others was then used to encode other credit cards and supply PIN numbers which could then be fraudulently used to obtain large sums of money from automatic teller machines.

The evidence concerning Joan Ojomo's authority to access the material data showed that she did not have authority to access the data she used for this purpose. At no time did she have any blanket authorisation to access any account or file not specifically assigned to her to work on. Any access by her to an account which she was not authorised to be working on would be considered a breach of company policy and ethics and would be considered an unauthorised access by the Company. The computer records showed that she accessed 189 accounts that did not fall within the scope of her duties. Her accessing of these accounts was unauthorised.

Using these methods, she and her fellow conspirators defrauded American Express of approximately US\$1,000,000. Mr Allison was arrested with forged American Express cards in his possession and was photographed using one such card to obtain money from an automatic teller machine in London.

The House of Lords considered whether an employee could commit an offence of securing "unauthorised access" to a computer contrary to section 1 of the Computer Misuse Act 1990. It was held that the employee clearly came within the provisions of section 1 CMA as the employee intentionally caused a computer to give her access to data which she knew she was not authorised to access.

Their Lordships made it clear that an employee would only be guilty of an offence if the employer clearly defined the limits of the employee's authority to access a program or data.

10.1.4 Hacking computer systems

Yarimaka v Governor of HM Prison Brixton; Zezev v Government of the United States of America (2002).

This was an extradition case arising from an attempt to extort \$200,000 from Michael Bloomberg by hacking into his company's computer system and then showing how it was done. One of the arguments advanced on behalf of the defendants was that causing a computer to record the arrival of information that did not come from the source it purported to come from (in effect by providing misleading data) was not conduct affecting the reliability of the data for the purposes of s 3 Computer Misuse Act (CMA).

The Court of Appeal rejected this interpretation and Wright J said: 'But if an individual, by misusing or bypassing any relevant password, places in the files of the computer a bogus e-mail by pretending that the password holder is the author when he is not, then such an addition to such data is plainly unauthorised, as defined in section 17(8) CMA; intent to modify the contents of the computer as defined in section 3(2) CMA is self-evident and, by so doing, the reliability of the data in the computer is impaired within the meaning of section 3(2)(c) CMA.'

10.1.5 Possessing indecent photographs of children

R v Ross Warwick Porter [Neutral Citation Number: [2006] EWCA Crim 560

On 5 November 2002, the police raided the appellant's house and seized some hard drives and two computers which were linked to the Internet almost permanently. The appellant worked in the field of information technology and had built two computers. 3575 still images and 40 movie files of child pornography were recovered from the hard disk drives of the two computers.

Of the 3575 still images, 873 of the remaining 3573 found had been deleted in the sense that they had been placed in the "recycle bin" of the computer which had then been emptied. The remaining 2700 still images were saved in a database of a programme called ACDSee. This programme is designed for viewing graphical images and is used by photographers. When opened in the "gallery view", the programme creates "thumbnail" images of the pictures viewed. These would originally have been larger images associated with each thumbnail. If one had clicked on the thumbnail, the larger image could have been viewed. All of the larger images had, however, been deleted. The effect of deleting the larger images was that the thumbnail could no longer be viewed in the gallery view, but a trace of each thumbnail ("the metadata") remained in the database of the programme.

It was conceded by the Crown that:

1. All the deleted items had been deleted before 5 November 2002;
2. The appellant did not have the software to retrieve or view the deleted still or movie files;

3. The thumbnail images were only retrievable with the use of specialist forensic techniques and equipment, which would not have been available to the public. It is common ground that the appellant could have acquired software to enable him to retrieve the items which had been emptied from the recycle bin. There was no evidence that the appellant had attempted to do this.

The appellant was found guilty at Snaresbrook Crown Court of fifteen counts of making an indecent photograph of a child contrary to section 1(1)(a) of the Protection of Children Act 1978 and two counts of possessing indecent photographs of children contrary to section 160(1) of the Criminal Justice Act 1988 ("the 1988 Act"). The appellant appealed against conviction on two counts of possessing indecent photographs of children.

The Court ruled that in the special case of deleted computer images, where a person could not retrieve or gain access to an image, he would no longer have custody or control of it. It followed that it was not appropriate to say that a person who could not retrieve an image from the hard disk drive would be in possession of the image by reason of his possession of the hard disk drive itself.

10.1.6 Extraterritorial data seizure

*The arrest of Vasily Gorshkov, and Alexey Ivanov of Russia in November 2000*¹⁰⁶

Vasily Gorshkov and Alexey Ivanov were arrested (and subsequently convicted) in the United States in November 2000. The men were alleged to be kingpins of Russian computer crime who hacked into the networks of at least 40 U.S. companies and then attempted to extort money.

"Ivanov attracted FBI attention in the Fall of 1999, when the internet service provider (ISP) Speakeasy discovered its network had been compromised and informed the Seattle branch of the FBI. In early 2000, OIB also detected an attack and notified the FBI in Connecticut. Between late 1999 and early 2000, other large Internet corporations including CD Universe, Yahoo, and Ebay also experienced similar attacks to Speakeasy and OIB. Computer forensics determined the Internet traffic for all attacks originated from the same machine in Russia. After linking his online alias "subbsta" and his resume, the FBI determined Ivanov's identity and initiated a sting operation to lure him to the United States for arrest.

"The FBI constructed a false computer security company, Invita, in Seattle, Washington and invited Ivanov to interview for a position on November 10, 2000. Ivanov's interview involved hacking an FBI controlled honeypot. While Ivanov was hacking the FBI honeypot, all keystrokes and network traffic were recorded as potential evidence. In addition, the FBI made video and audio recordings of the entire interview process. After Ivanov successfully gained access to the FBI honeypot, he was arrested. The FBI used the recorded keystrokes and network traffic log to access the intermediary computers Ivanov used in Russia."

¹⁰⁶ Source: http://en.wikipedia.org/wiki/United_States_v._Ivanov#cite_note-resume-3

"After arresting the men, the agents used account numbers and passwords obtained by the program to gain access to data stored on the pair's computers in Russia. When the FBI accessed Ivanov's machines, they found folders with data corresponding to the companies he had remotely attacked. Over 2.3 GB of data was recovered from Ivanov's machines, including the tools used to gain illegal access and scripts that referenced companies that had been attacked."

The FBI agents downloaded evidence before obtaining a search warrant. The Russian Federal Security Service started criminal proceedings against FBI Agent Michael Schuler for unauthorized access to computer information.

Please note: The actions of the FBI agent of obtaining evidence from Ivanov's computer in Russia would not be acceptable in some jurisdictions.

10.1.7 Identity theft, password hijacking, social networks

Old Tbilisi Police Department received a complaint from the citizen S. S. on the hacking and illegal manipulation of her Facebook account by someone who changed the password to her Facebook account and then posted intimate and indecent photos of her. A fake account of S. S. without her approval has been also created in Odnoklassniki.ru social network, where S. S. and her family member's telephones were posted as contact numbers for sex escort services. A number of such calls from various person seeking sexual services have been received by S.S. and her family members. An investigation was launched under Article 284, par 1 of the Georgian Criminal Code (access to a computer system without right).

The main suspect in the case, as indicated by interviewed victim and her family, is ex-boyfriend of S. S., G. A. who, since breakup with S. S., has been extremely jealous and insistent with phone calls to the victim, having been out of contact with the S.S. only for a few last months (when actually the actions described took place). Also, in past, S. S. and G. A. have created and managed a shared Facebook page. A further argument by the victims was that indecent images posted on Facebook and Odnoklassniki.ru has portrayed both S. S. and G. A. in various situations and circumstances, including intimate moments.

IMEI codes identifying all incoming calls to S. S. asking for sexual favors have been ordered to be produced from Geocell and Magticom (major telecommunications operators) central offices, and relevant tables showing incoming calls, phone numbers, IMEI and caller's IDs have been received without delay. None of them contained any data related to G. A. who nevertheless remained a prime suspect.

A search and seizure in exigent circumstances was made at G. A.-s premises and his personal computer has been seized. Investigation argued that, since G. A. has with high probability learned about ongoing investigation against him, he would be inclined to destroy related evidence and thus exigent search and seizure was justified. The judge approved of the reasons presented and declared search and seizure lawful.

The seized PC has been sent to forensic examination laboratory with questions put to an expert as to whether the evidence was found of G.A. accessing the pages of social networks in question, what passwords were used for such access and whether pictures posted thereto were uploaded from the said computer. The expert provided negative answers to all of the questions above except for photos which were found on a hard drive as well as CD that was seized together with the PC. However, no upload or internet browsing history of the said actions was found on the computer.

IP activity history has been requested from the Internet Service Provider, as well as mobile service providers, in order to identify G.A. internet activity history in the relevant period. None of the ISPs were able to provide information since, under Georgian law, the ISPs are not required to keep and maintain traffic data.

With so little evidence available, the prosecutor has nevertheless decided to charge G.A. with a single count of illegal access to a computer system, and during initial interview of the accused G.A. has fully admitted guilt and provided investigation with detailed information on his actions, including password used to access S.S. Facebook and Odnoklassniki pages, as well as reasons and motives for such actions (jealousy, post-breakup stress, etc.). As a result of his admission and negotiations involving his attorney and the prosecution, a plea agreement has been concluded between the parties, where prosecution pleaded to the same offence but with the suspended sentence and a fine of 3000 GEL (approx 1500 EUR).

The judge has held a hearing on the next day of concluding a plea agreement. The judge has reviewed the materials of the case, has questioned the defendant as to possible coercion or any other circumstance that may taint his free admission of guilt, and has found the defendant guilty sentencing him to 2 years of imprisonment (suspended) and a fine of 3000 GEL. None of the parties, including victim, have appealed the decision.

10.1.8 Hacking computer systems (Qurban Ali)

Qurban Ali and another v The State (2007) P Cr. L J 675 [Karachi]

This case involved the abduction of a man for ransom. The ransom was duly paid and the abductee was released and was subsequently able to identify a number of the kidnappers.

The Court found that e-mail evidence was available because of modern devices. The Court looked at the evidentiary value of e mail. The Court recognised that anyone could send e-mail to any other person, if he or she knew the e-mail account name of the other person. Password of the receiving person was not required for that purpose and the address of the telephone holder/owner, could be attained from P.T.C.L/N.T.C.

In that way the computer that sent the e-mail could be identified and the e-mail data could be retrieved from it by using computer forensics tools. It is also possible to prove this in a Court of law provided a proper chain of custody exists. It was, however, in this case difficult to identify the particular person who sent the e-mail.

The Court recognised that this was an area where investigation by some police agency was required, no law existed by which Cyber Cafes were required to keep record of persons using their computers, nor did they keep historical data for long. The Prosecution, in this case had not provided a proper chain of custody for the e-mail evidence in accordance with the law and therefore could not be relied upon and thus, was discarded.

10.2 Civil cases

10.2.1 Legal risk mitigation on a massive layoffs at pharmaceutical sector

A pharmaceutical company is about to lay off a hundred employees and is searching for a way to mitigate legal risks. They request a computer forensic expert to produce a forensic copy of computers assigned to each employee as soon as he/she leaves the company. They need to "freeze" the available evidence in time in order to be able to analyse it should the need arise.

The forensic experts designed an acquisition strategy specifically to cope with the speed at which devices had to be imaged, hashed and tagged. Logistics and technology where the key points which allowed the team to produce forensic images faster than computers could be brought to the in-house temporary laboratory that had been set-up for the operation.

Nine months later seven of those forensic images enabled the pharmaceutical company to provide crucial evidence to dismiss false testimony at court by a group of employees.

In this case it was essential to ensure the electronic devices involved to preserve their original contents and be able to prove or refute the controversy facts at Court or to be used in internal negotiations. In this case it was crucial to be able to identify accurately which electronic devices were involved to proceed immediately to preserve their original content and be able of using it afterwards to obtain the electronic evidence related to the case.

10.2.2 Data forensics pursuant to a data breach

Several employees present voluntary resignations at the same time. Management suspects that confidential information and in-house developed tools might end up on a direct competitor.

The team of experts began the investigation on computers assigned to the twenty six ex employees. The results obtained by the Computer Forensics done to the electronic devices involved in the investigation prove that strategic corporate information had been stolen. On the resulting forensic report specifics on data theft were provided: patent related intellectual property, source code and a partial dump of the corporate CRM had been retrieved from corporate systems.

The experts were able to go a step further on the investigation by proving that stolen source code had been slightly altered and was being used and sold by a competitor months after.

The forensic report became an essential piece of evidence at court allowing quick and successful prosecution. In this case it was imperative to analyse the employee's computers to obtain the electronic evidence necessary to prove that the fraud had taken place. In this way, it was necessary to clone the original electronic device to practice an informatics forensics analysis by the required experts with the correct knowledge and experience. These professionals, with the right forensic tools, were able to obtain the relevant electronic evidence that was essential to prove the fraud committed by the companies employees. It's also crucial to take all technical and legal

measures, during the Computer Forensics procedure, to ensure the admissibility of the electronic evidence obtained at Court.

10.2.3 Investigations of a boycott of an online sales system

An airline company suffers a boycott involving its online sales website. Clients have trouble buying tickets online at the corporate website and this quickly starts to affect the economy and public image of the company.

The computer forensic expert, through its online investigation services is able to provide the necessary insight into the case. There was an unusually high activity on the websites logs, which leads the experts to reveal that clients are randomly being redirected to other pages through the purchase process.

The expert, through its investigation and report allows the company to take technical and legal measures to solve the problem and recover its corporate image. In this case it was very important to be able to demonstrate and explain the technical aspects that proved that the corporate webpage had been manipulated. To do so, the expert had to analyse the technical contents of the affected webpage and then carry out the necessary online investigation to gather the bases needed to support the accusation.

10.2.4 Electronic discovery for the legal risk analysis in a company buy out

As part of the conditions of a Merger & acquisition agreement, the client was imposed a clause that specifically regulated the transfer of intellectual property associated with certain patents during the last five years. This clause specifically included any kind of intellectual property transfer, being it formal or not. Due to the penalties this clause included in the agreement our client needed to be 100% sure that no formal or informal IP transfer of any kind had taken place by any of the 2,500 employees on the Group.

The computer forensics team, through its e-Discovery service located all documents and e-mails whose content was related to patented IP. Millions of documents and emails were identified, copied, categorized, indexed and made available to the staff of the company and the law firm that advised the M&A operation to review all the material in a comfortable and efficient way.

The completeness of the job performed allowed both client and law firm to adequately measure the risks involved in the operation. Without the e-discovery computer forensics service, the identification and selection of the relevant documents in the case would have last for ages. Using this computer forensics service, the experts, by a selection of the correct key words where able of obtaining all the relevant documents between millions of documents that where potential involved in the investigation.

10.2.5 Proving the authenticity of an email

Against non-payment of a debt indebted by email raises a lawsuit in which the email plays a key role. The defendant denies the debt has been recognized and argues that the email was never sent.

Through the implementation of a specific expert service adverse email that allows the recognition of debt shield made through email, the experts are able to access to the technical part of the email and recognize whether it's original or whether it's been manipulated . In this specific case, the email was the evidence needed to prove the conflict situation between the parties, what made the client understand it was necessary to be able to guarantee before Court its authenticity.

By the implementation of this service, the client could prove to the competent judicial authorities their version of events. Get a ruling in their favour, ordering the defendant to the payment of outstanding debt plus interest with the express statutory imposition of the costs incurred by the defendant.

11 Glossary¹⁰⁷

24/7 RealMedia: is a technology company headquartered in New York City specializing in Digital Marketing. It provides digital marketing solutions for publishers, advertisers and agencies globally. It was formerly listed as "TFSM" on the NASDAQ stock exchange.

3G networks: 3G or 3rd generation mobile telecommunications is a generation of standards for mobile phones and mobile telecommunication services fulfilling the **International Mobile Telecommunications-2000 (IMT-2000)** specifications by the International Telecommunication Union. Application services include wide-area wireless voice telephone, mobile Internet access, video calls and mobile TV, all in a mobile environment.

Access Control Lists (ACLs): is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation.

Access token: is an object encapsulating the security descriptor of a process. Attached to a process, a security descriptor identifies the owner of the object (in this case, the process) and ACLs that specify access rights allowed or denied to the owner of the object. While a token is used to represent only the security information, it is technically free-form and can enclose any data. The access token is used by Windows when the process or thread tries to interact with objects whose security descriptors enforce access control (*securable objects*).

Acquisition: a process referred to as Imaging. The duplicate is created using a hard-drive duplicator or software imaging tools such as DCFLdd, IXimager, Guymager, TrueBack, EnCase, FTK Imager or FDAS. The original drive is then returned to secure storage to prevent tampering. The acquired image is verified by using the SHA-1 or MD5 hash functions. At critical points throughout the analysis, the media is verified again, known as "hashing", to ensure that the evidence is still in its original state. In corporate environments seeking civil or internal charges, such steps are generally overlooked due to the time required to perform them.

Active data: Files and folders that reside in the IT system storage units that are accessible and visible to the users in an immediate and direct manner by the means of the operating system's tools.

AdBrite: is an online advertising network, based in San Francisco, California, which was founded by Philip J. Kaplan and Gidon Wise in 2002. Originally founded as Marketbanker.com, the site was relaunched as AdBrite in 2004 and now serves advertisements on hundreds of thousands of sites, according to their published statistics.

AdCenter: Microsoft adCenter (formerly **MSN adCenter**), is the division of the Microsoft Network (MSN) responsible for MSN's advertising services. Microsoft adCenter provides pay per

¹⁰⁷ Source: Wikipedia.org

click advertisements. This is a service aimed at people who want to advertise a product. Microsoft also has a (still in beta) service for webmasters who want to monetize on their site: Microsoft pubCenter.

AfriNIC (African Network Information Center): is the regional Internet registry (RIR) for Africa.

Amazon S3 (Simple Storage Service): is an online storage web service offered by Amazon Web Services. Amazon S3 provides storage through web services interfaces (REST, SOAP, and BitTorrent). Amazon launched S3, its first publicly-available web service, in the United States in March 2006 and in Europe in November 2007.

API: An **application programming interface** is a specification intended to be used as an interface by software components to communicate with each other. An API may include specifications for routines, data structures, object classes, and variables. An API specification can take many forms, including an International Standard such as POSIX or vendor documentation such as the Microsoft Windows API, or the libraries of a programming language, e.g. Standard Template Library in C++ or Java API.

APNIC (Asia Pacific Network Information Centre): is the regional Internet registry for the Asia Pacific region. APNIC provides number resource allocation and registration services that support the global operation of the Internet. It is a not-for-profit, membership-based organization whose members include Internet Service Providers, National Internet Registries, and similar organizations.

ARIN (American Registry for Internet Numbers): is the Regional Internet Registry (RIR) for Canada, many Caribbean and North Atlantic islands, and the United States. ARIN manages the distribution of Internet number resources, including IPv4 and IPv6 address space and AS numbers.

Assistant (PDA): They come in many forms and sizes and usually have storage capability built in the form of hard disks or flash memory. They have become very popular in recent years and may be useful sources of electronic evidence as they run their own operation systems and are often connected to the internet via **WLAN**, **3G** or **LTE** networks.

ATM: An automatic teller machine (ATM), is a computerized telecommunications device that provides the clients of a financial institution with access to financial transactions in a public space without the need for a cashier, human clerk or bank teller (from Wikipedia)

Autonomous System: is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet.

Azure: Microsoft Windows Azure Platform is a Microsoft cloud computing platform used to build, host and scale web applications through Microsoft data centers. Azure is classified as platform as a

service and forms part of Microsoft's cloud computing strategy, along with its software as a service offering, Microsoft Online Services. The platform consists of various on-demand services hosted in Microsoft data centers and commoditized through three product brands. These are Windows Azure (an operating system providing scalable compute and storage facilities), SQL Azure (a cloud-based, scale-out version of SQL Server) and Windows Azure AppFabric (a collection of services supporting applications both in the cloud and on premise). Microsoft has announced free Ingress for all the customers of Azure from 1 July 2011.

Backup: A copy taken of all information held on a computer in case something goes wrong with the original copy.

Biometric scanners: a device connected to a computer system that recognizes physical characteristics of an individual (e.g., fingerprint, voice, retina).

BIOS: Basic Input Output System. The set of routines stored in read-only memory that enable a computer to start the operating system and to communicate with the various devices in the system such as disk drives, keyboard, monitor, printer, and communication ports.

Bit: A **bit** (a contraction of **binary digit**) is the basic capacity of information in computing and telecommunications; a bit represents either 1 or 0 (one or zero) only. The representation may be implemented, in a variety of systems, by means of a two state device. In computing, a bit can also be defined as a variable or computed quantity that can have only two possible values. These two values are often interpreted as binary digits and are usually denoted by the numerical digits 0 and 1. The two values can also be interpreted as logical values (*true/false, yes/no*), algebraic signs (+/-), activation states (*on/off*), or any other two-valued attribute. The correspondence between these values and the physical states of the underlying storage or device is a matter of convention, and different assignments may be used even within the same device or program. The length of a binary number may be referred to as its "bit-length."

Bluetooth: A telecommunications industry specification that describes how mobile phones, computers, and PDAs can easily interconnect with each other and with home and business phones and computers using a short-range wireless connection. Bluetooth requires that a low-cost transceiver chip be included in each device.

Blu-ray Disc (BD): is an optical disc storage medium designed to supersede the DVD format. The plastic disc is 120 mm in diameter and 1.2 mm thick, the same size as DVDs and CDs. Blu-ray Discs contain 25 GB per layer, with dual layer discs (50 GB) being the norm for feature-length video discs. Triple layer discs (100 GB) and quadruple layers (128 GB) are available for BD-XL re-writer drives.

Capturing data: Capturing data means to copy data from a computer system or electronic media and store them on an external storage media before verifying the integrity of the data where possible (e.g. not possible for capturing RAM). Capturing data can also be possible for network

data. In this context on machine in the network is used to capture the network packets and store their information to a file (e.g. in PCAP format).

CentralOps: CentralOps is a website offering investigative lookup opportunities like a domain dossier, email dossier, whois lookups, etc. These services can provide information about IP-addresses, domains and email addresses. The website is run by Hexillion is a privately-held company based in the USA. Its' address is: <http://centralops.net>

Chat logs: is an archive of transcripts from online chat and instant messaging conversations. Many chat or IM applications allow for the client-side archiving of online chat conversations, while a subset of chat or IM clients (i.e., Google Talk and Yahoo! Messenger 11 Beta) allow for the saving of chat archives on a server for future retrieval. The latter trend has been adopted by the applications' vendors because of the decreasing cost of web server hard drive space.

CIDR notation: is a compact specification of an Internet Protocol address and its associated routing prefix. Classless Inter-Domain Routing (CIDR) is an Internet Protocol (IP) address allocation and route aggregation methodology^[1] used within the Internet addressing architecture that replaced the IPv4 classful network organization of the IP address space. It is used also for IPv6 networking, the next generation of the IP addressing architecture.

Circuit boards: A thin plate with chips, devices and other electronic components installed on the plate (also referred to as the printed circuit board).

Closed Circuit Television (CCTV): They are used by companies, governments and individuals for security and may provide evidence that certain activities have or have not taken place.

Cloud: Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[...]

CMOS: Complementary metal-oxide semiconductor. Semiconductor technology used in the transistors that are manufactured into most of today's computer microchips. It commonly holds the BIOS preferences of the computer through power off with the aid of a battery (adapted from).

Compact Disk (CD): Optical disc 12cm in diameter used for storing binary information. Its formatted capacity is between 640-700 Mb and was primarily used to store audio. When used for storing generic data it is called CD-ROM.

Computer Memory: Memory is the electronic holding place for instructions and data that a computer's microprocessor can reach quickly. RAM is located on one or more microchips installed in a computer.

Computer Networks: consists of connections between two or more computers that are linked by data cables or by wireless connectivity. These computers are able to share data and other

resources between them. They often have other hardware components to enable the scope of activities required of the network.

Cookie: Cookies are small files that the internet server downloads onto the hard drive of the user's computer. These files contain specific information that identifies the user (for example, through passwords and lists of websites visited).

CPU: Central processing unit. The computational and control unit of a computer. Located inside a computer, it is the "brain" that performs all arithmetic, logic, and control functions in a computer.

Cracker: A Cracker is a person that enters into a system without authorisation with the intention of causing some form of damage or to make beneficial gain.

Cybercrime: refers to any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target.

Cybersquatter: A Cybersquatter is a person that reserves or buys domain names with the intention of selling them to interested companies in the future.

DAT (Digital Audio Tape): Digital audio tape used for storing media on *back-up* systems.

Data storage devices: A **data storage device** is a device for recording (storing) information (data). Recording can be done using virtually any form of energy, spanning from manual muscle power in handwriting, to acoustic vibrations in phonographic recording, to electromagnetic energy modulating magnetic tape and optical discs.

DATABASE: Structured collection of data that can be accessed in many ways. Common database programs are: Dbase, Paradox, Access. Uses: various including – address links, invoicing information, etc.

Dead box forensics: Dead box forensics is one part of computer forensics which is a branch of digital forensic science pertaining to legal evidence found in computers. Computer forensics deals with the examination of computer systems in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts that might become evidence in a trial. Dead box forensics follow this aim but is only focused on storage media in computer systems that are in a turned off state.

Deleted data: Files and folders that existed previously on the computer as active data but since have been deleted by the operating system or the end-user. Deleted data will remain in the storage unit until they are overwritten by another file.

Desktops: The term has been adopted as an adjective to distinguish office appliances (such as photocopiers and printers) which can be fitted on top of a desk, from larger equipment covering its own area on the floor. Desktop may also refer to Desktop computer, a personal computer designed to fit on a desk

Digital Forensics: Digital Forensics is a branch of forensic science related to the acquisition, processing, analysis and reporting of evidence that is stored on computer systems, digital devices and other storage media with the aim of admissibility in court.

Digital media: is a form of electronic media where data are stored in digital (as opposed to analogue) form. It can refer to the technical aspect of storage and transmission (e.g. hard disk drives or computer networking) of information or to the "end product", such as digital video, augmented reality or digital art.

Digital photography: Digital photography is a form of photography that uses an array of light sensitive sensors to capture the image focused by the lens, (from Wikipedia)

Digital Video Disk (DVD): Digital Versatile (video) Disc. Presently the natural successor of the CD for the reproduction of quality sound and image.

DIGITAL VIDEO: Video captured, manipulated and stored in a digital format.

Digitalisation: To store electronic information as a chain of "ones" and "zeros". Due to the fact that as many "zeros" as "ones" can be easily represented by 2 voltaic levels in electronic media, the binary numbering system is widely used in the digital IT world.

Diskette Proprietary tools: IT applications that have been developed expressly in keeping with the functionalities and the operation of the company that utilises it and that, in general, are not available for purchase on the open market.

Diskette: Form of media storage, becoming less frequently used, that consists of a circular piece of magnetic material within a plastic case / covering.

DNS: Domain Name System (DNS). Transforms the name of a domain, for example www.cybex.es, into the IP address where the server that you are looking for is situated.

Docking stations: A device to which a portable computer (e.g., laptop, notebook) can be attached for use as a desktop computer, usually having a connector for externally connected devices such as hard drives, scanners, keyboards, monitors, and printers.

Domain name: The **Domain Name System (DNS)** is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. A **Domain Name Service** resolves queries for domain names (which are easier to understand and utilize when accessing the internet) into IP addresses for the purpose of locating computer services and devices worldwide. An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name www.example.com translates to the addresses 192.0.43.10 (IPv4) and 2620:0:2d0:200::10 (IPv6).

DomainTools: DomainTools, LLC provides a directory of domain name Whois ownership records that serves as a comprehensive snapshot of past and present domain name registration and ownership records that span more than a decade of Internet history. In addition to Whois data, DomainTools offers a set of research tools that helps individuals and organizations discover and monitor everything about a domain name. DomainTools is also known for offering advanced semantic name suggestion technology, patented Reverse IP technology, and incorporating millions of screenshots into a combined screenshot history view of how a website looks now and how it used to look like in the past.

Dongle: is a small piece of hardware that plugs into an electrical connector on a computer and serves as an electronic "key" for a piece of software; the program will run only when the dongle is plugged in. The term "dongle" was originally used to refer only to software-protection dongles; however, currently "dongle" is often used to refer to any small piece of hardware that plugs into a computer. This article is limited in scope to dongles used for the purpose of copy protection or authentication of software to be used on that system.

Drive duplicators: A device for fast copying (duplicating) of different storage media, e.g., hard disks or CDs.

DropBox: is a file hosting service operated by Dropbox, Inc. that offers cloud storage, file synchronization, and client software.

Dynamic Host Configuration Protocol (DHCP): is a protocol used to automatically assign a pool of IP addresses to a group of devices.

Electronic evidence: Electronic evidence is information generated, stored or transmitted using electronic devices that may be relied upon in court. To guarantee that the evidence is accepted in court, it is necessary to obtain the information following very well defined processes using specialised personnel and operating within an adequate legal framework.

E-mail virus: Viruses cannot travel in e-mail messages because they only use a 7 bit format to transfer text. The only way that they can travel is by binary files that are sent as attachments with the text message. It is recommended to check these files with an anti-virus before opening.

Email: The exchange of computer-stored messages by telecommunication

Encryption: Method of scrambling and encoding data. Used to convert plain text into ciphertext (by using a mathematical parameter called cryptographic key) in order to prevent anyone but the intended recipient from reading that data.

Environmental data: Refers, as a whole, to the data that is not active on the IT system. Environmental data includes: Data found in unused or unassigned areas, Data found in the "Slack" file space and File data that has been deleted that is not visible using the operating system tools.

Event logs: Event Logs are the logfiles saved by the Windows operating systems. Usually there are several Event Logs auditing a variety of events from different services of Windows. The creation of certain Event Logs is turned on by default but can be disabled by the user. The default storage location for Windows XP machines is: C:\Windows\system32\config*.evt, for Windows Vista/7 machines it is: C:\Windows\system32\Winevt*.evtx

EXIF metadata: Exchangeable image file format (Exif) is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras. Typically there is a lot of information to find in the EXIF metadata, e.g. time, date and place of when and where a photograph has been taken and which camera model with which configuration was used.

EXT4: or **fourth extended filesystem** is a journaling file system for Linux, developed as the successor to EXT3.

External hard drives: External hard drives are a kind of external storage media. Modern external hard drives consist of a chassis, that offers connectivity via USB, Firewire, eSATA and/or Thunderbolt, and a regular 2,5" or 3,5" hard disk or SSD that is residing inside the chassis. Typically external hard drives can store a larger amount of data compared to USB thumbdrives or SD cards.

Faraday isolation bags: A dimensionless unit of electric charge quantity, equal to approximately 6.02×10^{23} electric charge carriers. This is equivalent to one mole, also known as Avogadro's constant. Faraday isolation bags are used to prevent mobile phones and devices from connecting to communication signals

FAT (File Allocation Table): is the name of a computer file system architecture and a family of industry standard file systems utilizing it. The FAT file system is technically relatively simple yet robust. It offers reasonably good performance even in light-weight implementations and is therefore widely adopted and supported by virtually all existing operating systems for personal computers. This makes it a well-suited format for data exchange between computers and devices of almost any type and age from the early 1980s up to the present.

File extension: File label usually 3 characters in length, preceded by a decimal point, that identifies the format of the data file or the application used to modify it.

FireBug: integrates with Firefox to put a wealth of development tools while browsing. It allows the user to edit, debug, and monitor CSS, HTML and JavaScript live in any web page.

FireWire: A high-speed serial bus that allows for the connection of up to 63 devices. Widely used for downloading video from digital camcorders to the computer.

Flash cards: are devices for storing digital information. They are often used in many electronic devices such as digital cameras, mobile phones, laptop computers, music players and games

consoles. They are able to retain data without power and come in a variety of capacities, meaning they can store huge amounts of data while being easy to hide from view.

Forensic Boot-DVDs: Forensic Boot-DVDs are DVDs that are bootable and contain an operating system containing software to perform digital forensics tasks. Besides just offering the forensic tools these Boot-DVDs take measures to prevent unintended write operations to any of the attached storage media.

FQDN (Fully Qualified Domain Name): sometimes also referred as an *absolute domain name*, is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain and the root zone. A fully qualified domain name is distinguished by its unambiguity; it can only be interpreted one way.

Fragmented data: Fragmented data is active data that has been divided and stored in different physical locations on the hard disk.

FTK Imager: FTK Imager is a multi-purpose software by Access Data Inc. It is free of charge and is capable of imaging, verifying, converting and mounting hard-discs and image files. FTK Imager can be downloaded at the following website: <http://accessdata.com/support/adownloads>

FTP (File Transfer Protocol): Protocol of the internet that allows transfer of files / data between computers connected via the internet.

Google AdSense: is a program run by Google Inc. that allows publishers in the Google Network of content sites to serve automatic text, image, video, and rich media adverts that are targeted to site content and audience. These adverts are administered, sorted, and maintained by Google, and they can generate revenue on either a per-click or per-impression basis.

GPS: The GPS (Global Positioning System) is a "constellation" of 24 well-spaced satellites that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location. The location accuracy is anywhere from 100m to 10m for most equipment. GPS devices can provide information on previous travel via destination information, way points, and routes.

Hacker: Person that has a thorough knowledge of the functionality of computers and networks that enables them to take advantage of the errors and failures in security of said systems.

Hard disk: Metal disk covered with a ferromagnetic burning layer. Making an analogy with a vinyl disc, the flat sides of the disc are the burning layer, the arm of the turntable is the laser arm and the needle on the turntable arm is the laser beam that reads / writes the information. A user can write, delete or re-write on magnetic disks as with audio tape.

Hard drives: Hard drives are the major storage device within computer systems. They consist of a circuit board, data and power connections, along with internal magnetically charged, ceramic,

metal or glass platters that store the data. It is not unusual to discover hard drives that are not connected to or installed in a computer system.

Hardware: The physical components that make up a computer system such as the keyboard, monitor and mouse.

Hoax: Term used to define false rumours, especially about non-existent viruses spread over the network. Sometimes they are very successful and cause as much damage as a real virus.

Hosting providers: An **Internet hosting service** is a service that runs Internet servers, allowing organizations and individuals to serve content to the Internet. There are various levels of service and various kinds of services offered. A common kind of hosting is web hosting. Most hosting providers offer a combined variety of services. Web hosting services also offer e-mail hosting service, for example. DNS hosting service is usually bundled with domain name registration.

HTML code (Hypertext Markup Language): Language used for writing documents for web servers. HTML is an application from ISO Standard 8879:1986.

HTTP (Hypertext Transfer Protocol): HTTP is a protocol with the necessary agility and velocity to distribute and handle multimedia information systems over the internet. A characteristic of HTTP is the independence in the visualisation and representation of the data, allowing systems to be constructed independently of the development of new advances in the representation of data.

HTTPS: Secure HTTP protocol. The 2 principal characteristics are the coding and authentication. By means of the coding, the content of the communication of the server to the third party is concealed. The authentication allows users know that the server is bonafide with the use of certificated signatures by Certification of Authority.

Forensic copy: An exact copy (bit by bit) of the unit of storage of an IT system used in a forensic investigation.

Hubs: A place of convergence in a network where data arrives from one or more directions and is forwarded out in one or more other directions. It usually works as a multiport repeater by generating a number of identical outputs from a single input (output=input). A hub may include a switch of some kind (adapted from).

I ROM memory: ROM stands for *Read-Only Memory*. The memory of the semiconductor that cannot be overwritten and maintains stored information intact, including in the case of loss of power supply. ROM is used to storing the system configuration or the programme from the boot-up of the computer.

ICQ: is an instant messaging computer program, which was first developed and popularized by the Israeli company Mirabilis, then bought by America Online, and since April 2010 owned by

Mail.ru Group. The name *ICQ* is a homophone for the phrase "I seek you". This is an adaptation of the Morse code callout "CQ", which means "calling any station".

IMAP: Internet Message Access Protocol. An Internet service based on a standardized protocol for retrieving and/or accessing e-mail messages from the mail server (i.e., IMAP server).

Infrared: Infrared wireless technology is used for short- and medium-range communications and control in a variety of applications (e.g., wireless local area networks, links between notebooks and desktop computers, cordless modems, intrusion detectors). Infrared refers to energy in the region of the electromagnetic radiation spectrum at wavelengths longer than those of visible light, but shorter than those of radio waves.

Instrument of Pre-Accession: The Instrument for Pre-Accession Assistance (IPA) is the financial instrument for the European Union (EU) pre-accession process for the period 2007-2013. Assistance is provided on the basis of the European Partnerships of the potential candidates and the Accession Partnerships of the candidate countries, which means the Western Balkan countries, Turkey and Iceland. The IPA is intended as a flexible instrument and therefore provides assistance which depends on the progress made by the beneficiary countries and their needs as shown in the Commission's evaluations and strategy papers.

Interface "Gnome": Is the core user interface of the GNOME desktop environment used by a variety of different Linux distributions. It provides basic functionality like switching between windows and launching applications. It replaces GNOME Panel and other software components from GNOME 2 to offer a user experience that breaks from the previous model of desktop metaphor, used in earlier versions of GNOME.

Internet access: is the means by which individual terminals, computers, mobile devices, and local area networks are connected to the global Internet. Internet access is usually sold by Internet Service Providers (ISPs) that use many different technologies offering a wide range of data rates to the end user.

Internet Assigned Numbers Authority (IANA): is the entity that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and numbers. IANA is a department operated by the Internet Corporation for Assigned Names and Numbers, also known as ICANN.

Internet browsing history: Software that is designed to browse websites like Apple Safari, Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, etc often save histories of websites that were visited by the users of a computer system. The main purpose of these history logfiles or databases is to allow the user to easily choose websites that were visited recently or very often. For forensic examiners the internet browsing history saved by the browsers can be a valuable source for finding evidence.

Internet Service Provider (ISP): is an organization that provides access to the Internet. Internet service providers can be either community-owned and non-profit, or privately owned and for-profit.

Internet: Global network of data based on TCP/IP protocol that are utilised to interconnect computers and, as such, the transport of diverse services, the most popular being e-mail, web and FTP services.

IP address: Chain of 4 numbers separated by decimal points that are used to represent and identify a computer on the internet. ISP's assign IPs automatically when we connect to the internet.

ISP (Internet Service Provider): Organisation that provides connection to the internet for computers that are dedicated lines or switches. A profit making entity that as well as providing access to the internet for individuals and / or legal entities, can offer services such as web hosting, web-design consultancy, integration of websites and intranets, etc.

IT system: An information system (IS) - or application landscape - is any combination of information technology and people's activities that support operations, management and decision making. In a very broad sense, the term information system is frequently used to refer to the interaction between people, processes, data and technology. In this sense, the term is used to refer not only to the information and communication technology (ICT) that an organization uses, but also to the way in which people interact with this technology in support of business processes.

JAVA: Java is a language oriented to objects and developed by Sun Microsystems. It shares similarities with C, C++ and Objective C. Basing itself on other object oriented languages, Java utilises the best parts of the others and eliminates the least effective points. The principal objective of Java was to make a language that had the capacity to be executed in a secure way across the internet (although the code was maliciously written). This characteristic requires the elimination of many C and C++ uses and constructions. The most important is that no pointers exist. In Java, the program cannot arbitrarily access memory addresses.

LACNIC (Latin America and Caribbean Network Information Centre): is the Regional Internet Registry for the Latin American and Caribbean regions. LACNIC provides number resource allocation and registration services that support the global operation of the Internet. It is a not-for-profit, membership-based organisation whose members include Internet Service Providers, and similar organisations.

LAN: Local Area Network. A common name for the networking technologies standardized by the IEEE (Institute of Electrical and Electronics Engineers).

LAN CONFIGURATION: LAN topology such as Ethernet or token ring, or MAC addresses such as Ethernet address (MAC: Medium Access Control, a part of the data link layer in the OSI seven layer model).

Linux: is a Unix-like computer operating system assembled under the model of free and open source software development and distribution. The defining component of Linux is the Linux kernel, an operating system kernel first released 5 October 1991 by Linus Torvalds.

Live computer system: A Live computer system is a computer system that is powered on.

Live data forensics: Live data forensics is one part of computer forensics which is a branch of digital forensic science pertaining to legal evidence found in computers. Computer forensics deals with the examination of computer systems in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts that might become evidence in a trial. Live data forensics follow this aim but is only focused on computer systems that are powered on. The main purpose is to acquire volatile data that would otherwise get lost if the computer system is turned off or would be overwritten if the computer system will stay turned on for a longer period.

Log: Register of determined events generated by the operating system, or application, about a given period of time. Logs can be used by external auditors for registering / reconstructing the use of the computer or application.

LTE networks: LTE Advanced is a mobile communication standard, formally submitted as a candidate 4G system to ITU-T in late 2009, was approved into ITU, International Telecommunications Union, IMT-Advanced and was finalized by 3GPP in March 2011.^[1] It is standardized by the 3rd Generation Partnership Project (3GPP) as a major enhancement of the Long Term Evolution (LTE).standard.

MAC address (Media Access Control): Also known as the hardware address or Ethernet address. A unique identifier specific to the network card inside a computer. Allows the DHCP server to confirm that the computer is allowed to access the network. MAC addresses are written as XX-XX-XX-XX-XX, where the Xs represent digits or letters from A to F.

Mac OS: is a series of graphical user interface-based operating systems developed by Apple Inc. (formerly Apple Computer, Inc.) for their Macintosh line of computer systems. The Macintosh user experience is credited with popularizing the graphical user interface. The original form of what Apple would later name the "Mac OS" was the integral and unnamed system software first introduced in 1984 with the original Macintosh, usually referred to simply as the **System** software.

Macro virus: Ultimate presentation of the virus. They are transported in application files (Word, Excel, etc.) and not in binary files (how traditional viruses are). They are executed on the opening of the data file in which they are contained.

Mainframe computers: An industry term for a large computer, typically manufactured by a large company such as IBM for the commercial applications and other large-scale computing purposes.

Malware: Malicious software. Any programme whose objective is to cause damage to computers, systems or networks and, as a result, to its users.

Memory cache: A type of memory that temporarily stores information that is used frequently to enable rapid access to this data.

Memory cards: are devices for storing digital information. They are often used in many electronic devices such as digital cameras, mobile phones, laptop computers, music players and games consoles. They are able to retain data without power and come in a variety of capacities, meaning they can store huge amounts of data while being easy to hide from view.

Memory devices: A memory device is any device that is capable of storing data either permanently or non-permanently.

Metadata: Metadata is information about a combination of files and / or folders that can describe, for example, how and when it was created, received, accessed and modified and by whom. This data is utilised in Computer Forensics to reconstruct the chain of events associated to the analysed file. Depending on the context in which the term is employed, it can refer to one piece of data or another.

Microprocessors: incorporates the functions of a computer's central processing unit (CPU) on a single integrated circuit, (IC) or at most a few integrated circuits. It is a multipurpose, programmable device that accepts digital data as input, processes it according to instructions stored in its memory, and provides results as output. It is an example of sequential digital logic, as it has internal memory. Microprocessors operate on numbers and symbols represented in the binary numeral system.

COFEE: Computer Online Forensic Evidence Extractor is a tool kit, developed by Microsoft, to help computer forensic investigators extract evidence from a Windows computer. Installed on a USB flash drive or other external disk drive, it acts as an automated forensic tool during a live analysis. Microsoft provides COFEE devices and online technical support free to law enforcement agencies.

Microsoft PubCenter is a publisher's ad serving application developed by Microsoft in addition to Microsoft adCenter, which allows advertisers to place ads on search engines as well as select MSN websites or applications. Currently, in its beta version.

Microsoft Windows is a series of graphical interface operating systems developed, marketed, and sold by Microsoft.

Minicomputers: is a term for a class of smaller computers that evolved in the mid-1960s and sold for much less than mainframe and mid-size computers from IBM and its direct competitors.

Modem: MOdulator/DEModulator. A device used by computers to communicate over telephone lines. It is usually recognized by connection to a phone line, but there are also cable modems

based on the DSL technology (e.g., cable modems). Can be combined with a facsimile (fax) functionality within a PC card (adapted from).

Modular rack-mounted systems: Modular rack-mounted systems are computer systems that are hosted in a rack and often times are built in a modular way allowing each hardware module to be replaced instantly without having negative impacts on the whole system. These racks most usually can host multiple computer systems with 19" form factor.

Mozilla Firefox is a free and open source web browser developed for Microsoft Windows, Mac OS X, and Linux coordinated by Mozilla Corporation and Mozilla Foundation. Firefox uses the Gecko layout engine to render web pages, which implements current and anticipated web standards.

Network interface cards: Provides network connection (either with cable or wireless). Can be in the form of an expansion board or a PC card.

NTFS (New Technology File System) is a proprietary file system developed by Microsoft Corporation for its Windows line of operating systems, beginning with Windows NT 3.1 and Windows 2000, including Windows XP, Windows Server 2003, and all their successors to date.

Online service provider: can for example be an internet service provider, email provider, news provider (press), entertainment provider (music, movies), search, e-shopping site (online stores), e-finance or e-banking site, e-health site, e-government site, Wikipedia, Usenet. In its original more limited definition it referred only to a commercial computer communication service in which paid members could dial via a computer modem the service's private computer network and access various services and information resources such as bulletin boards, downloadable files and programs, news articles, chat rooms, and electronic mail services.

P2P-Peer to Peer: Protocol that uses the internet for the interchange and download of files. The term P2P comes from *peer-to-peer* and refers to a network of equals, meaning that the status of each client is the same. The existence of servers in the practical application of the P2P networks is due to the fact that its clients do not possess fixed IP addresses. As a consequence these servers only offer a listing of clients and file searches.

Pagers: A pager is a device that may be used for sending and receiving electronic messages, numeric (e.g., phone numbers) and alphanumeric (text, often including e-mail)

Parallel port dongle: A small device with a parallel port connector that may provide programmable memory, remote update, lease control algorithms or counters.

Partitions: is the act of dividing a hard disk drive into multiple logical storage units referred to as *partitions*, to treat one physical disk drive as if it were multiple disks. Partitions are also termed "slices" for operating systems based on BSD, Solaris or GNU Hurd. A partition editor software program can be used to create, resize, delete, and manipulate these partitions on the hard disk.

Peripheral Devices: are not an integral part of the computer but connect to it to improve its capabilities. Examples of peripheral devices are: scanners, printers, tape drives, webcams, loudspeakers, microphones, fax , answering machines and card readers.

Personal Digital Assistant (PDA): A small (i.e., pocket-sized) device that can include computing, telephone/fax, paging, networking, and other features.

PGP: Pretty Good Privacy. Freeware cryptography software (see, e.g., www.pgpI.org) originally developed by Philip R. Zimmermann in 1991. Can be used to encrypt/sign e-mails or encrypt computer files. There is also a low-cost commercial version.

Pharming: A technique with the same objective as *Phishing*, but is not based on misleading the user but the Domain Named System (DNS) instead. In this way, if the user's ISP utilizes vulnerable DNSs, the "pharmer" redirects all the traffic of the URLs that are of interest, to the servers under his/her control. These have an identical appearance to the originals. The only way to detect this type of attack is through the certified servers that, in the case of the "pharmer", will not have a Certification of Authority.

Phishing: Technique of deception that combines social engineering with certain technical tricks with the objective of stealing personal banking information from an individual user. *Phishing* attacks cleverly take the appearance of e-mails from a trusted entity requesting bank details or passwords of the user.

Phreaker or Phreak: IT pirate specialised in using telephone networks to access other people's systems or often just to avoid paying telephone bills. The techniques used by *Phreakers* are commonly known as *phreaks*.

Programme pirating: Activity of copying, distributing or using existing IT programmes, infringing legally upon the intellectual property rights that protect its authors.

POP3: Post Office Protocol. An Internet service based on a standardized protocol for retrieving e-mail messages from the mail server (i.e., POP server).

Port replicators: A device containing common PC ports such as serial, parallel, and network ports that plugs into a portable computer. A port replicator is similar to a docking station, but docking stations normally provide capability for additional expansion boards.

Portable media players: store and play digital media such as music and other audio, images, video as well as other files including documents and other types of fields that are capable of being stored digitally.

Proxy: In computer networks, a **proxy server** is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server. The proxy server evaluates the request as a

way to simplify and control their complexity. Today, most proxies are **web proxies**, facilitating access to content on the World Wide Web.

Qwerty: is the most common modern-day keyboard layout.

RAM memory: RAM stands for *Random Access Memory*. RAM memory temporarily stores data that the computer is working with. This memory loses its content as a result of a power loss.

Recovered data: The term that identifies recovered or reconstructed files or folders that had been deleted from the active data area. These files can be recovered with the original size and format or in small fragments that will require a forensic reconstruction task.

Refusal of service: Incident where a user or an organisation are refused access to a resource they can normally use. Usually, the loss of access is due to the unavailability of a particular network service, such as e-mail, or the temporary loss of all network connections and services. In the worst case, for example, a website where millions of people access can be forced temporarily to cease operating. Although, normally intentional and malicious these type of attacks sometimes occur accidentally. If these attacks do not always result in the theft of information, they almost invariably cost a lot of time and money to the person or organisation affected.

Reverse engineering: Consists of the analysis of the binary code of a programme or application to determine its behaviour.

RIPE Réseaux IP Européens (RIPE, French for "European IP Networks"): is a forum open to all parties with an interest in the technical development of the Internet. The RIPE community's objective is to ensure that the administrative and technical coordination necessary to maintain and develop the Internet continues. It is not a standardisation organisation like the IETF and does not deal with domain names like ICANN.

Routers: is a device that determines the next network point that a packet should be forwarded towards its destination. It must be connected to at least 2 networks. It is intelligent and works on routing tables. Although it is located at the gateway to a network it does not necessarily have to be the networks gateway to the Internet.

Scheduler: is the method by which threads, processes or data flows are given access to system resources (e.g. processor time, communications bandwidth). This is usually done to load balance a system effectively or achieve a target quality of service. The need for a scheduling algorithm arises from the requirement for most modern systems to perform multitasking (execute more than one process at a time) and multiplexing (transmit multiple flows simultaneously).

SHA-256 hash: is a set of cryptographic hash functions (**SHA-224, SHA-256, SHA-384, SHA-512**) designed by the National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. SHA-2 includes a

significant number of changes from its predecessor, SHA-1. SHA-2 consists of a set of four hash functions with digests that are 224, 256, 384 or 512 bits.

Slack area data: Due to the necessity of the computer to assign fixed sized blocks of disk space, there exists an area at the end of every file that, despite being assigned to the file, contains information not relating to the other information contained therein. This area is called "slack" and contains information of the contents that were on this block space before it was assigned a new file.

Slack space: Slack space is an area of space on a storage devices that is allocated to a certain unit, e.g. a file, a partition, a disk, an MFT record but is not used by this unit. Oftentimes a forensic specialist can find data belonging to formerly stored files in these slack spaces. If for example a cluster gets allocated to a newly created file but the data of this file do not use the whole cluster than there is a good chance to find traces of a previously stored file in the slack space of the cluster.

Social Engineering: Techniques or skills that allow manipulation of a person that, voluntarily carries out actions that they normally would not do, such as the revealing of information.

Software: Computer programs designed to perform specific tasks, such as word processing, accounting, network management, Website development, file management, or inventory management.

Solid state disks: they store information in a different way than hard disks, while intending to provide access in the same way as traditional hard disks. Whereas hard disks store data on platters, solid state disks store data using microchips that have no moving parts. As such they are less likely to be damaged by shock and they offer faster access to the data. These devices may hold valuable evidence.

Speaker magnets: Common speakers consist of a magnet, a coil and a cone. The speaker magnet is there to provide a permanent magnetic field for the the speaker coil, which is embedded in the paper of the speaker cone. When the audio signal flows throw the speaker coil it generates a small magnetic field the strength of which varies with the strength of the audio signal. This small magnetic field is repelled by or attracted to the permanent magnetic field produced by the speaker magnet.

Storage devices: is a device for recording (storing) information (data). Recording can be done using virtually any form of energy, spanning from manual muscle power in handwriting, to acoustic vibrations in phonographic recording, to electromagnetic energy modulating magnetic tape and optical discs.

Tablet Devices: A tablet computer is a device that is operated by touching the screen rather than using a keyboard or mouse. It is normally larger than a mobile phone or **Personal Digital Assistant**

Traceable: Traceability refers to the completeness of the information about every step in a process chain. The formal definition of traceability is the ability to chronologically interrelate uniquely identifiable entities in a way that is verifiable. Traceability is the ability to verify the history, location, or application of an item by means of documented recorded identification.

TrueCrypt: is a free software application used for on-the-fly encryption (OTFE). It can create a virtual encrypted disk within a file or encrypt a partition or (under Microsoft Windows except Windows 2000) the entire storage device (pre-boot authentication).

Trusted Platform Module (TPM): Most commonly the concept of TPM is applied in a TPM cryptoprocessor, known as TPM chip. This chip which is responsible for carrying out the TPM tasks is soldered to the mainboard of a computer system. The primary scope of a TPM is to assure the integrity of a platform. In this context "integrity" means "behave as intended" and a "platform" is generically any computer platform: Start the power-on boot process from a trusted condition and extend this trust until the OS has fully booted and applications running. TPM is also oftentimes used in combination with disk encryption, e.g. Truecrypt or Bitlocker Full Disk Encryption where it is used to protect the keys used to encrypt the computer's hard disks and provide integrity authentication for a trusted boot pathway.

Ubuntu Linux: is a computer operating system based on the Debian Linux distribution and distributed as free and open source software, using its own desktop environment. It is named after the Southern African philosophy of ubuntu ("humanity towards others"). Ubuntu is designed primarily for use on personal computers, although a server edition also exists.

Universal Serial Bus (USB): is a standard that defines the protocols for communication, connection and power supply for devices that are to be connected to computers. Since its advent in the 1990s the number of devices that are now capable of being connected using this protocol has grown and new devices in all sorts of shapes and sizes are now used to store data.

Unix: is a multitasking, multi-user computer operating system originally developed in 1969.

Untrusted binaries: The term "untrusted binary" is most often used in conjunction with executable binary files that are stored or copied from an untrusted source. Any source that cannot be verified or has not undergone defined close validation procedures may potentially contain altered or even harmful source code and therefore should be considered untrusted. A typical example for untrusted binaries are executable files that are stored on a system other than the validated machine of the forensic specialist.

Unused or unassigned area data: Data that presently resides in the disk area that does not belong to a file; the remainder of the deleted digital documents.

URL(Uniform Resource Locator): A chain of characters which is assigned a unique address to each of the documents of the World Wide Web (*news, gopher, etc.*)

UTorrent: is a freeware, closed source BitTorrent client now owned by BitTorrent, Inc. It is the most widely used BitTorrent client outside China (where Xunlei is more popular). It gets the "μ" in its name from the SI prefix "micro-", referring to the program's small memory footprint: the program was designed to use minimal computer resources while offering functionality comparable to larger BitTorrent clients such as Vuze or BitComet. The program has received consistently good reviews for its feature set, performance, stability, and support for older hardware and versions of Windows.

Virtual environment: The computational simulation of a work environment formed by the interconnection of multiple computers that permits the access to digital information independent of their physical location.

Virus: Programme that can infect other programmes, modifying them to include a copy of itself. Viruses basically have the function of propagation and replication but, furthermore, there are some that have harmful contents (*payload*) with different objectives, from a simple joke to causing serious damage to systems. These types of programmes can operate in various ways: Only notifying the user of its presence without causing apparent damage, Attempt to go unnoticed to cause the most damage possible or Take possession of the principal functions (to infect the filing system).

VoIP: Voice over Internet Protocol. The technology used to transmit voice conversations over a data network using the Internet protocol. Data network may be the Internet or a corporate Internet.

Volatile Data: Volatile Data are data that are digitally stored in a way that the probability is very high for their contents to get deleted, overwritten or altered in a short amount of time by human or automated interaction.

Warez: Pirate copies of programmes. Protected software versions that have had the protection removed.

Web Browser: A web browser can also be defined as an application software or program designed to enable users to access, retrieve and view documents and other resources on the Internet.

Windows Explorer: is a file manager application that is included with releases of the Microsoft Windows operating system from Windows 95 onwards. It provides a graphical user interface for accessing the file systems. It is also the component of the operating system that presents many user interface items on the monitor such as the taskbar and desktop. Controlling the computer is possible without Windows Explorer running (for example, the File | Run command in Task Manager on NT-derived versions of Windows will function without it, as will commands typed in a command prompt window).

Wireless Modems: A wireless modem is a type of modulator-demodulator which connects to a wireless network instead of using telephone or cable television lines. A mobile Internet user can connect using a wireless modem to a wireless Internet Service Provider (ISP) to get Internet access.

WireShark: is a free and open-source packet analyser. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named **Ethereal**, in May 2006 the project was renamed Wireshark due to trademark issues.

WLAN networks: wireless local area network (WLAN) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network. Most modern WLANs are based on IEEE 802.11 standards, marketed under the Wi-Fi brand name.

Word Processor: A software program used to turn the computer into a typewriter for wiring letters, reports and documents. Common Word Processing programs: Wordstar, Wordperfect, MS-Word.

Worm: IT programme that auto-duplicates and auto-propagates. In contrast with viruses, worms are usually written especially for networks. Network worms were first defined by Shoch & Hupp, of Xerox, in the magazine *ACM Communications* (March 1982). The first famous internet worm appeared in November 1988 propagated itself to more than 6,000 systems at large on the internet.

WWW (World Wide Web): The universe of network-accessible information, i.e., all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP)

ZIP drives: A removable hard disk system. A ZIP drive is a small, portable disk drive used primarily for backing up and archiving personal computer files. The trademarked ZIP drive was developed and is sold by Iomega Corporation. Zip drives and disks come in two sizes.

12 Further information

12.1 Books

12.1.1 Electronic evidence

- Stephen Mason, *Electronic Evidence* (2nd edn, LexisNexis Butterworths, 2010) covering: Australia, Canada, England & Wales, Hong Kong, India, Ireland, New Zealand, Scotland, Singapore, South Africa and the United States of America
- Stephen Mason (Editor), *International Electronic Evidence* (British Institute of International and Comparative Law, 2008) covering: Argentina, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, Norway, Poland, Romania, Russia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Thailand and Turkey

12.1.2 United States of America

- US Department of Justice - Electronic Crime Scene Investigation – A guide for first responders. <https://www.ncjrs.gov/pdffiles1/nij/187736.pdf>
- US Department of Justice - Forensic Examination of Digital Evidence: A Guide for Law Enforcement. <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>
- Michael R Arkfeld, *Arkfeld on Electronic Discovery and Evidence* (3rd edn, Lexis, 2011) Looseleaf
- Adam I. Cohen and David J. Lender, *Electronic Discovery: Law and Practice* (2nd edn, Aspen Publishers, 2011) Looseleaf
- Jay E. Grenig, William C. Gleisner, Troy Larson and John L. Carroll, *eDiscovery & Digital Evidence* (2nd edn, Westlaw, 2011) Looseleaf
- Michele C.S. Lange and Kristen M. Nimsgers, *Electronic Evidence and Discovery: What Every Lawyer Should Know* (2nd edn, American Bar Association, 2009)
- George L. Paul, *Foundations of Digital Evidence* (American Bar Association, 2008)
- Paul R. Rice, *Electronic Evidence – Law and Practice* (American Bar Association, 2005)

12.1.3 United Kingdom

- Crown Prosecution Service Legal Guidance. <http://www.cps.gov.uk/legal/index.html>
- The Association of Chief Police Officers (ACPO) Guide for Electronic Evidence. http://7safe.com/electronic_evidence/index.html#
- The Association of Chief Police Officers (ACPO) Good Practice and Advice Guide for Managers of E-crime Investigation. <http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf>

12.2 Journals

- Digital Evidence and Electronic Signature Law Review. <http://www.deaeslr.org>
- The International Journal of Digital Forensics & Incident Response.
<http://www.compseconline.com/digitalinvestigation/>
- International Journal of Digital Crime and Forensics. <http://www.igi-global.com/>
- International Journal of Forensic Computer Science.
<http://www.ijofcs.org/webjournal/index.php/ijofcs>
- Journal of Digital Forensic Practice. <http://www.tandf.co.uk/>
- Journal of Digital Forensics, Security and Law. <http://www.jdfsl.org>
- IEEE Transactions on Information Forensics and Security. <http://www.ieee.org/>
- Forensic Science Communications (considers all aspects of forensics).
<http://www.fbi.gov/hq/lab/fsc/current/index.htm>
- Small Scale Digital Device Forensics Journal. <http://www.ssddfj.org/>
- International Journal on Digital evidence -
<http://www.utica.edu/academic/institutes/ecii/publications/ijde.cfm>

12.3 About the authors

The Council of Europe selected individuals with complementary backgrounds to author this guide. They are:

Esther George (UK) LLB(Hons), LLM, MA; Until 2014 Esther was a policy advisor and senior crown prosecutor with the Crown Prosecution Service (CPS) of England and Wales. She is now working as an international consultant. Esther specialises in Internet and computer enabled crime, digital evidence, intellectual property theft and data protection. She developed and designed the Crown Prosecution Service national high-tech crime training course for prosecutors. In 2010 Esther received a Certificate of Merit from the International Association of Prosecutors for initiating and developing the Global Prosecutors E-Crime Network (GPEN), which is an on-line information sharing network to help solve hi-tech crime around the world. Esther regularly speaks on high-tech crime issues at conferences and training sessions nationally and internationally.

Fredesvinda Insa Mérida; Fredesvinda is a law graduate and a Doctor of Information and Communication Technology. She worked as a lawyer for Price Waterhouse Coopers, the Council of Europe and subsequently in Cybex from 2004 to 2010, the year in which Cybex ceased to operate. She was the Strategic Development Director in Cybex and managed institutional relationships on a national, European and international level. She oversaw the legal, training, project and communication departments in Cybex. She is specialised in the forensic analysis of electronic media and electronic evidence from a legal standpoint, studying and analysing the legal situation of electronic evidence in Spain and Europe, promoting the sector and spreading knowledge of the subject. She managed the European projects called " The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime", "European Certificate on Cybercrime and Electronic

Evidence" and "Electronic Newsletter on the fight against Cybercrime" financed by the European Commission. She is a named expert on these issues by the European Commission and the Council of Europe, and a member of the High Level Expert Group of the International Telecommunication Union agency of the United Nations. She is the creator and organiser of the Electronic Evidence Seminars that have taken place every year since 2004 in Spain at the General Council of the Judicial Power of Spain. She collaborates with specialist magazines and takes part in conferences and events. Fredesvinda Insa is currently Strategic Development Director for CFLabs.

Uwe Rasmussen; Uwe is a senior attorney in the IP/IT department of the Paris-based law firm August & Debouzy where he manages cases in the areas of copyright, database rights, personal data protection, and compliance. Since 2006 he has worked on secondment with Microsoft's Digital Crimes Unit to work on cybercrime enforcement and cooperation initiatives. Mr Rasmussen holds law degrees from Sorbonne in Paris and Copenhagen University and has studied IP law at Santa Clara University and is moreover a Microsoft Certified Systems Engineer. He speaks Danish, Dutch, English, French, German and Spanish.

Victor Völzow; Victor is a trainer in digital forensics and cybercrime investigation at the Hesse State Police Academy. In this position he is responsible for development and implementation of the curriculum for digital forensics examiners. Besides teaching his job at the academy also involves providing practical support and technical consultation for High-Tech Crime units and other law enforcement agencies. Victor is also giving expert trainings for organisations such as the Council of Europe (CoE), the European Anti-Fraud Office (OLAF) and Europol. He acts as guest speaker for different Universities and is involved in the German digital forensics expert training programme at the Bundeskriminalamt (BKA). Being a police officer for more than ten years he has spent over six years in the field of digital forensics and cybercrime investigations and acted as expert witness on several occasions. Besides holding professional certifications Certified Cyber Forensics Professional (CCFP – EU), EnCase Certified Examiner (EnCE), Access Data Certified Examiner (ACE) and Certified Ethical Hacker (CEH) Victor completed the academic degree MSc in Forensic Computing and Cybercrime Investigations at University College Dublin in 2011 getting awarded the Garda Commissioner's Medal for the best result.

Nigel Jones MBE FBCS; Nigel is currently a director of Technology Risk Limited, a company specialising in technology risk solutions and training and is a visiting professor at Canterbury Christ Church University in England. He is also the law enforcement coordinator for a project developing a cybercrime centre's of excellence network in training, research and education (2CENTRE). Prior to this he was responsible for the creation and running of the National Hi Tech Crime Training Centre at the National Centre for Policing Excellence at Wyboston in the UK. He is co-author of the ACPO "Computer Based Evidence - Good Practice Guide" and member of the Technical Working Group on the Investigation of Electronic Evidence (TWGIEE) in the USA. Nigel has given presentations at numerous national and international events including the preparation and moderation of a hi-tech crime scenario at the United Nations 10th Crime Congress. In January 2005 Nigel was elected by the Member Countries as Chair of the Interpol European Working Party

Restricted

on IT Crime. Nigel has delivered cybercrime training on behalf of Interpol to its own staff as well as international courses in India, Cyprus and Syria. He has recently delivered training to the Georgian criminal justice authorities on behalf of the Council of Europe. He has also delivered training in Europe, the Middle East and North America.

13 Appendices

Appendix A – Search and seizure law enforcement flowchart

Appendix B – Live forensics flowchart

Appendix C – Private sector preparation flowchart

Appendix D - Private sector search and seizure flowchart

Appendix E – Acquisition of digital evidence flowchart

Appendix F – Chain of custody record

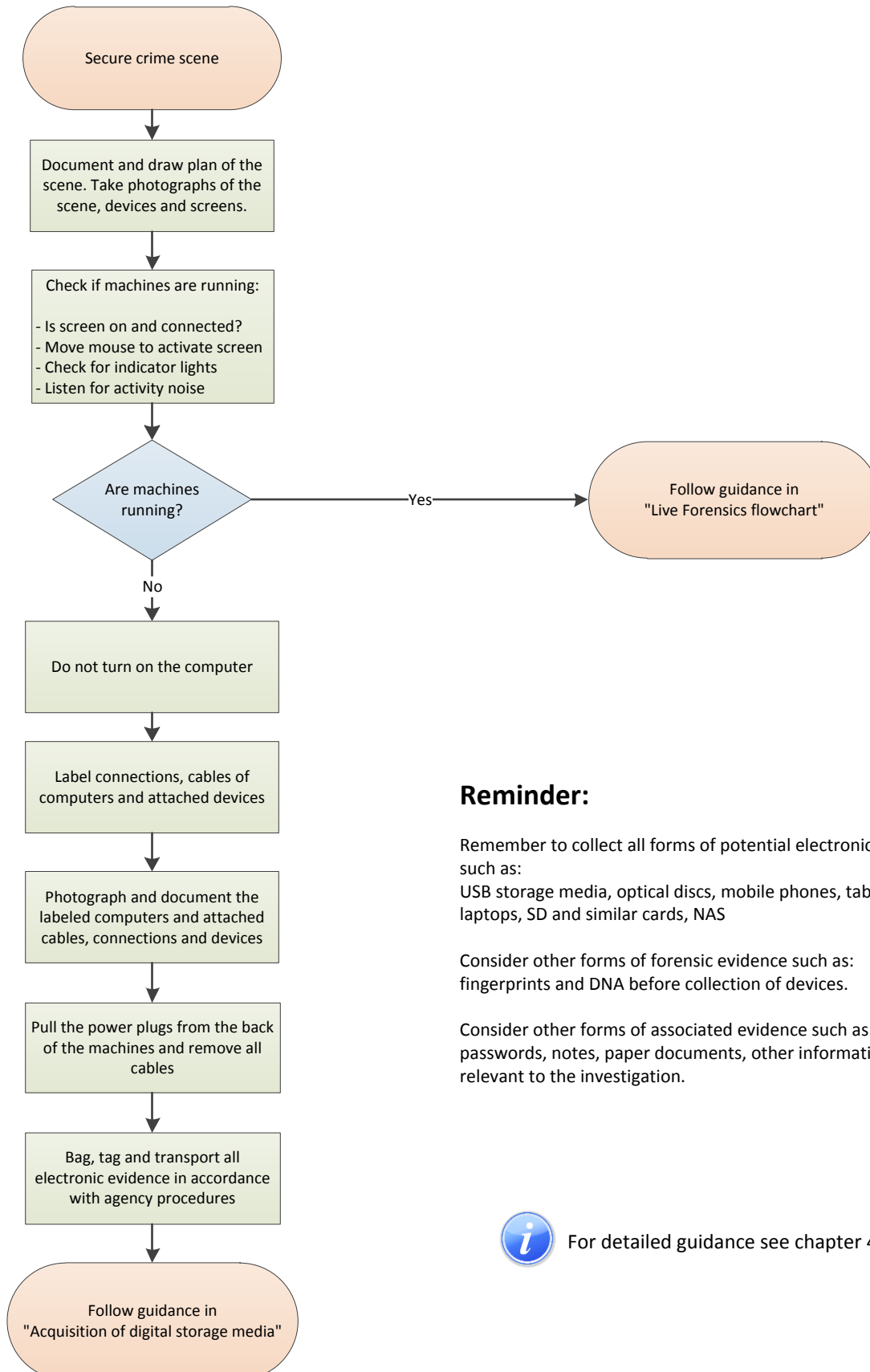
Appendix G - Custodian Questionnaire

Appendix H – Template exhibit labels

Appendix I – Acquisition sheet

Electronic Evidence Guide

Search and seizure flowchart



Reminder:

Remember to collect all forms of potential electronic evidence such as:

USB storage media, optical discs, mobile phones, tablets, laptops, SD and similar cards, NAS

Consider other forms of forensic evidence such as: fingerprints and DNA before collection of devices.

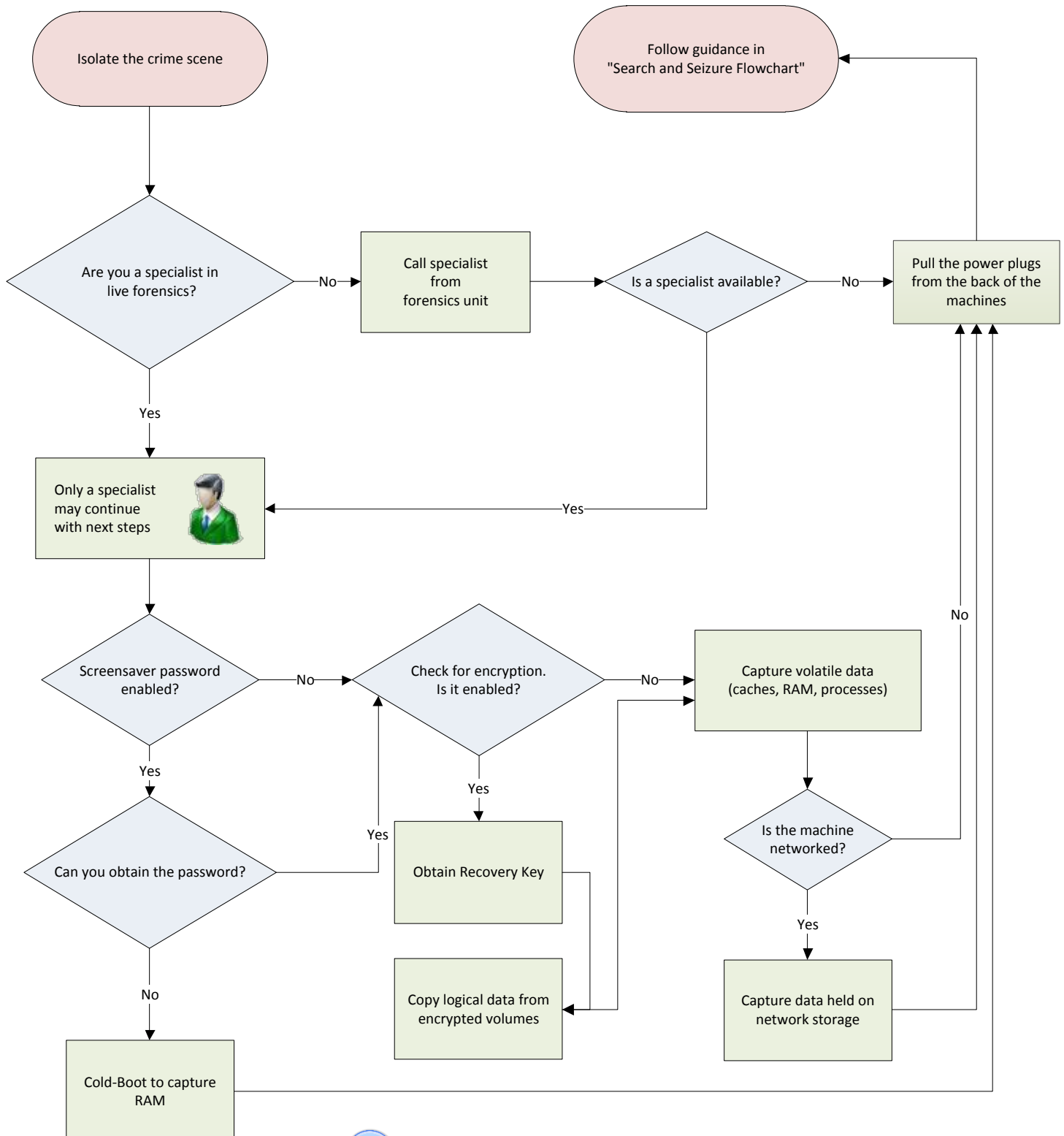
Consider other forms of associated evidence such as: passwords, notes, paper documents, other information relevant to the investigation.



For detailed guidance see chapter 4

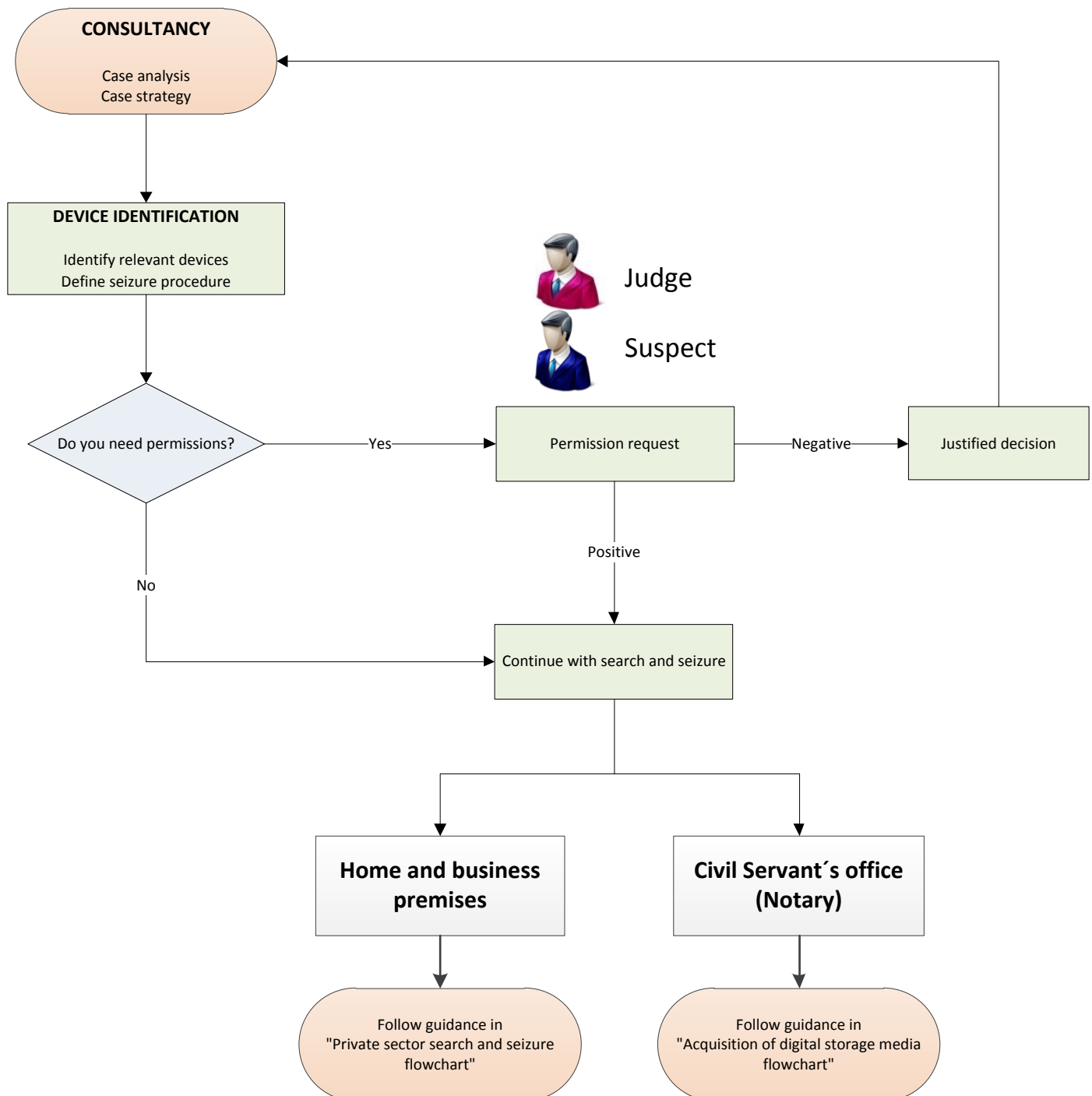
Electronic Evidence Guide

Live Data Forensics Flowchart



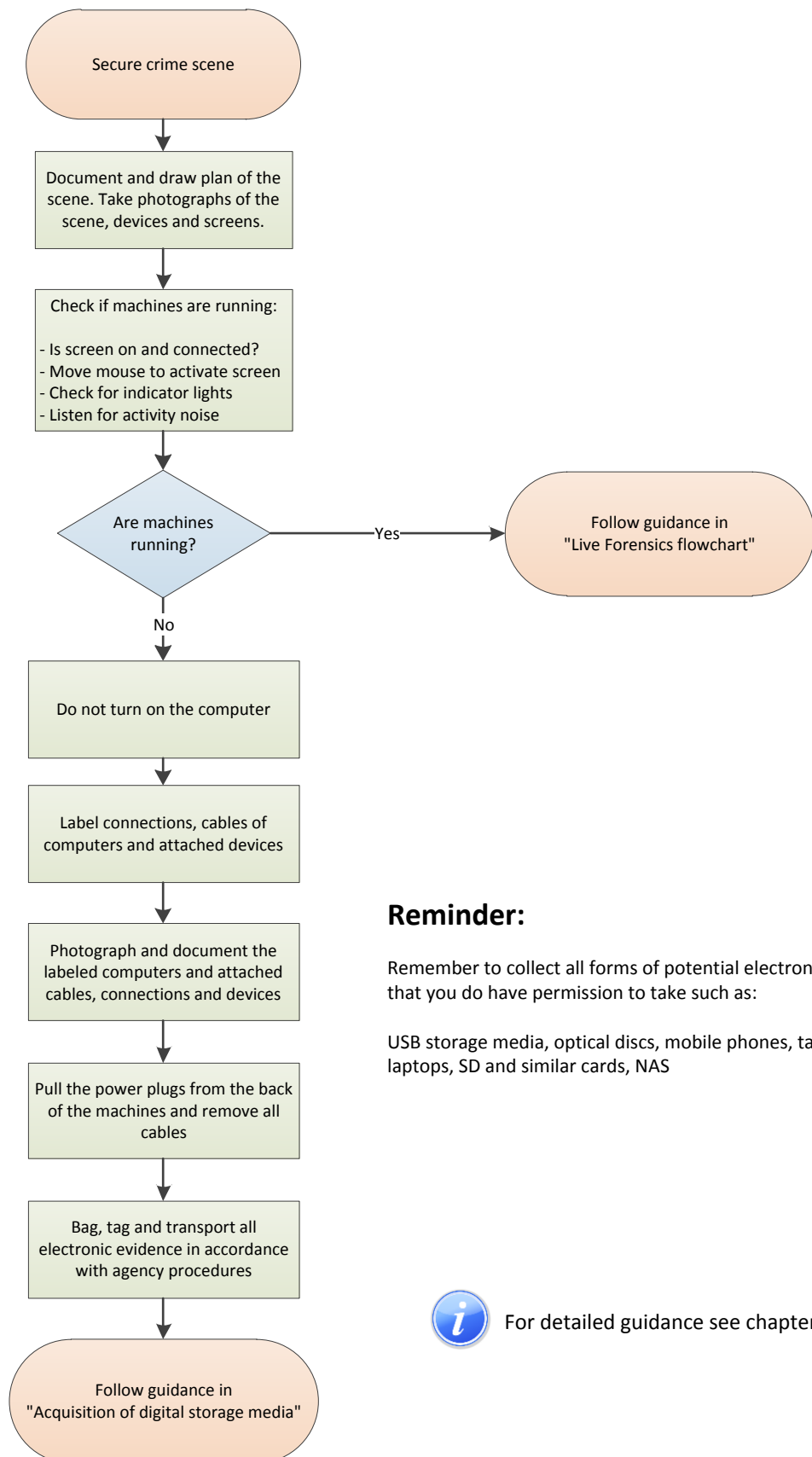
Electronic Evidence Guide

Private sector preparation flowchart



Electronic Evidence Guide

Private sector search and seizure flowchart



Reminder:

Remember to collect all forms of potential electronic evidence that you do have permission to take such as:

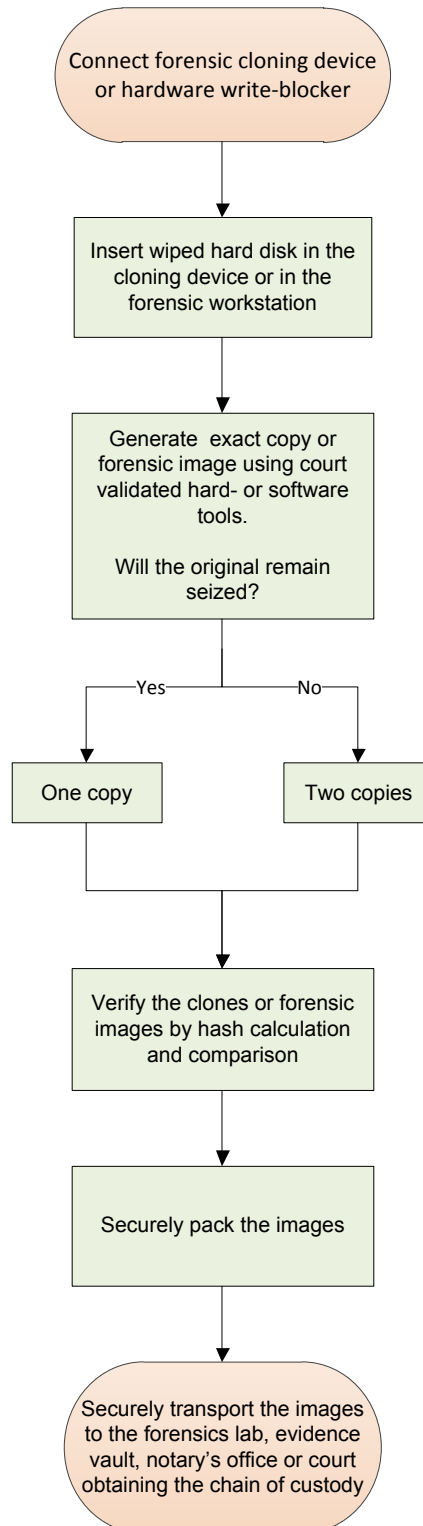
USB storage media, optical discs, mobile phones, tablets, laptops, SD and similar cards, NAS



For detailed guidance see chapter 9.4

Electronic Evidence Guide

Acquisition of digital evidence flowchart



Funded
by the European Union



Implemented
by the Council of Europe

Electronic Evidence Guide

CHAIN OF CUSTODY RECORD

Case Reference

Book **of**

GENERAL GUIDANCE REGARDING USE OF THIS BOOK

This book is intended for use in any situation where an item is to be seized (or in the case of imaging on site, the image created) and may subsequently be required to be produced as evidence in court.

It is essential that the chain of custody relating to exhibits is unbroken and therefore the storage and security of exhibits must remain paramount throughout the investigation.

Care should be taken to ensure that items seized during the course of an investigation have been obtained legitimately and where necessary the consent section (pages 10 to 11) should be utilised.

The sections laid out in this booklet have been included in an effort to provide for every eventuality and therefore operatives should be aware that some sections do not require completion in every case.

Likewise it must be noted that questions outlined within this booklet are by no means intended to be comprehensive and some will not apply in all cases. Additional notes space has been provided to cater for additional specific questions, however where this is used up further questions and answers can be recorded in the 'Scene Notes' section (pages 12 to 15).

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.

INFORMATION FROM MAIN PERSON AT LOCATION

| | |
|----------------------------|-----------------------|
| Name | |
| Age | |
| Date of Birth | / / |
| Nationality | |
| Address | |
| Phone | |
| Mobile | |
| Position/Occupation | |
| Other Information | |
| | |
| | |

| | | | | | |
|-------------------------------|-------------------------------|---------|--------------------------|--|---------|
| Informed about case as | <input type="checkbox"/> | WITNESS | <input type="checkbox"/> | | SUSPECT |
| Interview commenced | / hrs (Beginning) | | | | |

ADDITIONAL NOTES

GENERAL

The following devices are in place:

Stand-alone computers (number)

Portable computer/s (e.g., notebooks, laptops) (number)

Computers in a network Workstations Servers

Other

Question:

Who is familiar with the use of the computer systems?

☐

I am

☐

.....

☐

.....

Question:

Who takes care of system / network administration?

.....

.....

Question:

Which operating system(s) are installed on these devices?

Name, Version

(e.g., PC: Windows, Unix, Linux, Mac OS etc)

SYSTEM / NETWORK INFORMATION

Question:

Is the system backed up at regular time intervals? If yes:

Backup software

Backup recovery agent software

Question:

Is there a network in place ? If yes:

Question:

Is there a network plan? (If not, ask them to draw one).

Question:

Which network operating system(s) is installed on the device?

Name Version

Question:

Who takes care of network administration?

.....

.....

ADDITIONAL NOTES

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

SYSTEM SECURITY INFORMATION

Question:

Is the computer protected against unauthorized access?

☐

YES

☐

NO

Question:

What type of protection is in place?

BIOS-Password:

Other features that are password-protected:

Keyboard lock:

Screen lock:

Screen saver(s):

Other software protection:

Other hardware protection:

Secret question and answer for password:

Question:

Are the software and/or data on the device protected from unauthorized access?

☐

YES

☐

NO

Program/file

Password:

Program/file:

Password:

Program/file:

Password:

Program/file:

Password:

Program/file:

Password:

.....

.....

.....

.....

.....

This image shows a full page of white paper designed for handwriting practice. It features 20 evenly spaced horizontal dotted lines running across the width of the page. There are no margins, text, or other markings present.

INTERNET INFORMATION

Question:

Do you have Internet access?

Internet service provider:

Login name/user name:

Password:

Secret question and answer for password

.....

.....

E-mail address:

POP/SMTP server:

Web space, Free space (virtual drive)

.....

.....

OTHER NETWORK CAPABLE DEVICES

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Interview ended / hrs (End Time)

CONSENT

| | | |
|---|-------------|----------------|
| 1 | Print Name: | Organisation: |
| I hereby authorize (insert agency name) (and their representatives) to take possession of all computer equipment and items necessary for their investigation. | | |
| Signature: | | Date / Time: / |
| Entry No.(s): | | |

| | | |
|---|-------------|----------------|
| 2 | Print Name: | Organisation: |
| I hereby authorize (insert agency name) (and their representatives) to take possession of all computer equipment and items necessary for their investigation. | | |
| Signature: | | Date / Time: / |
| Entry No.(s): | | |

| | | |
|---|-------------|----------------|
| 3 | Print Name: | Organisation: |
| I hereby authorize (insert agency name) (and their representatives) to take possession of all computer equipment and items necessary for their investigation. | | |
| Signature: | | Date / Time: / |
| Entry No.(s): | | |

| | | |
|---|-------------|----------------|
| 4 | Print Name: | Organisation: |
| I hereby authorize (insert agency name) (and their representatives) to take possession of all computer equipment and items necessary for their investigation. | | |
| Signature: | | Date / Time: / |
| Entry No.(s): | | |

| | | |
|---|-------------|----------------|
| 5 | Print Name: | Organisation: |
| I hereby authorize (insert agency name) (and their representatives) to take possession of all computer equipment and items necessary for their investigation. | | |
| Signature: | | Date / Time: / |
| Entry No.(s): | | |

| | | |
|---|-------------|----------------|
| 6 | Print Name: | Organisation: |
| I hereby authorize (insert agency name) (and their representatives) to take possession of all computer equipment and items necessary for their investigation. | | |
| Signature: | | Date / Time: / |
| Entry No.(s): | | |

| | | |
|---|-------------|----------------|
| 7 | Print Name: | Organisation: |
| I hereby authorize (insert agency name) (and their representatives) to take possession of all computer equipment and items necessary for their investigation. | | |
| Signature: | | Date / Time: / |
| Entry No.(s): | | |

| | | |
|---|-------------|----------------|
| 8 | Print Name: | Organisation: |
| I hereby authorize (insert agency name) (and their representatives) to take possession of all computer equipment and items necessary for their investigation. | | |
| Signature: | | Date / Time: / |
| Entry No.(s): | | |

| | | |
|---|-------------|----------------|
| 9 | Print Name: | Organisation: |
| I hereby authorize (insert agency name) (and their representatives) to take possession of all computer equipment and items necessary for their investigation. | | |
| Signature: | | Date / Time: / |
| Entry No.(s): | | |

| | | |
|---|-------------|----------------|
| 10 | Print Name: | Organisation: |
| I hereby authorize (insert agency name) (and their representatives) to take possession of all computer equipment and items necessary for their investigation. | | |
| Signature: | | Date / Time: / |
| Entry No.(s): | | |

SCENE NOTES

Time notes began **Time notes completed**

Location notes made

Person completing notes

This image shows a full page of white paper designed for handwriting practice. It features approximately 20 evenly spaced horizontal dotted lines running from left to right across the entire width of the page. There are no margins, text, or other markings present.

[illegible]

[illegible]

[illegible]

PERSONS AT LOCATION

| | |
|--|--|
| 1. Name Age D.o.B Address Position/Occupation Time Present Other Information | 2. Name Age D.o.B Address Position/Occupation Time Present Other Information |
| 3. Name Age D.o.B Address Position/Occupation Time Present Other Information | 4. Name Age D.o.B Address Position/Occupation Time Present Other Information |
| 5. Name Age D.o.B Address Position/Occupation Time Present Other Information | 6. Name Age D.o.B Address Position/Occupation Time Present Other Information |
| 7. Name Age D.o.B Address Position/Occupation Time Present Other Information | 8. Name Age D.o.B Address Position/Occupation Time Present Other Information |

ANY RELEVANT INFORMATION REGARDING PERSONS PRESENT

[illegible]

| Entry No. | Exhibits | i. ii. Where found Who found by | iii. iv. Time seized 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. vi. vii. Where sealed Who by Seal No. | viii. ix. x. Place deposited Person depositing 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

.....
.....
.....
.....

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

.....
.....
.....
.....

| Entry No. | Exhibits | i. ii. Where found Who found by | iii. iv. Time seized 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. vi. vii. Where sealed Who by Seal No. | viii. ix. x. Place deposited Person depositing 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

.....
.....
.....
.....

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

.....
.....
.....
.....

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

.....
.....
.....
.....

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

.....
.....
.....
.....

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

.....
.....
.....
.....

| Entry No. | Exhibits | i. ii. Where found Who found by | iii. iv. Time seized 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. vi. vii. Where sealed Who by Seal No. | viii. ix. x. Place deposited Person depositing 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

.....
.....
.....
.....

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

.....
.....
.....
.....

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

.....
.....
.....
.....

RECEIPT SECTION

| | | | | | | | | | | |
|---|--|--|--|--|--|----------------------------|--|--|--|--|
| Received from _____ the _____ <i>(number)</i> of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | |
| Print Name: | | | | | | Organisation: | | | | |
| Signature: | | | | | | Date / Time: _____ / _____ | | | | |

| | | | | | | | | | | |
|---|--|--|--|--|--|----------------------------|--|--|--|--|
| Received from _____ the _____ <i>(number)</i> of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | |
| Print Name: | | | | | | Organisation: | | | | |
| Signature: | | | | | | Date / Time: _____ / _____ | | | | |

| | | | | | | | | | | |
|---|--|--|--|--|--|----------------------------|--|--|--|--|
| Received from _____ the _____ <i>(number)</i> of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | |
| Print Name: | | | | | | Organisation: | | | | |
| Signature: | | | | | | Date / Time: _____ / _____ | | | | |

| | | | | | | | | | | |
|---|--|--|--|--|--|----------------------------|--|--|--|--|
| Received from _____ the _____ <i>(number)</i> of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | |
| Print Name: | | | | | | Organisation: | | | | |
| Signature: | | | | | | Date / Time: _____ / _____ | | | | |

| | | | | | | | | | | |
|---|--|--|--|--|--|----------------------------|--|--|--|--|
| Received from _____ the _____ <i>(number)</i> of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | |
| Print Name: | | | | | | Organisation: | | | | |
| Signature: | | | | | | Date / Time: _____ / _____ | | | | |

| | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|-----|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | | Organisation: | | | | | | | | | | |
| Signature: | | | | | | | | | | | | Date / Time: / | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|-----|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | | Organisation: | | | | | | | | | | |
| Signature: | | | | | | | | | | | | Date / Time: / | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|-----|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | | Organisation: | | | | | | | | | | |
| Signature: | | | | | | | | | | | | Date / Time: / | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|-----|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | | Organisation: | | | | | | | | | | |
| Signature: | | | | | | | | | | | | Date / Time: / | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|-----|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | | Organisation: | | | | | | | | | | |
| Signature: | | | | | | | | | | | | Date / Time: / | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|----------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | | | | | | | | | | | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | Organisation: | | | | | | | | | | | | | | | | | | | | | |
| Signature: | | | | | | | | | | | Date / Time: / | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|----------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | | | | | | | | | | | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | Organisation: | | | | | | | | | | | | | | | | | | | | | |
| Signature: | | | | | | | | | | | Date / Time: / | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|----------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | | | | | | | | | | | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | Organisation: | | | | | | | | | | | | | | | | | | | | | |
| Signature: | | | | | | | | | | | Date / Time: / | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|----------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | | | | | | | | | | | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | Organisation: | | | | | | | | | | | | | | | | | | | | | |
| Signature: | | | | | | | | | | | Date / Time: / | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|----------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | | | | | | | | | | | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | Organisation: | | | | | | | | | | | | | | | | | | | | | |
| Signature: | | | | | | | | | | | Date / Time: / | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|----------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | | | | | | | | | | | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | Organisation: | | | | | | | | | | | | | | | | | | | | | |
| Signature: | | | | | | | | | | | Date / Time: / | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|----------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | | | | | | | | | | | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | Organisation: | | | | | | | | | | | | | | | | | | | | | |
| Signature: | | | | | | | | | | | Date / Time: / | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|----------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | | | | | | | | | | | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | Organisation: | | | | | | | | | | | | | | | | | | | | | |
| Signature: | | | | | | | | | | | Date / Time: / | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|----------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | | | | | | | | | | | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | Organisation: | | | | | | | | | | | | | | | | | | | | | |
| Signature: | | | | | | | | | | | Date / Time: / | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|----------------|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
| Received from | | | | | | | | | | | the | | | | | | | | | | | (number) of items listed by Entry No. below. | | | | | | | | | | |
| Entry No.(s): | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Print Name: | | | | | | | | | | | Organisation: | | | | | | | | | | | | | | | | | | | | | |
| Signature: | | | | | | | | | | | Date / Time: / | | | | | | | | | | | | | | | | | | | | | |

[illegible]

Funded
by the European Union



Implemented
by the Council of Europe

Custodian Questionnaire

CONFIDENTIAL

| | |
|----------------------|--|
| Project Name | |
| Custodian Name | |
| Project ID Reference | |

PERSONAL INFORMATION

| | | | |
|---|--|--------------------------|--|
| Family Name | | | |
| First Given Name | | Other Given Names | |
| Company | | | |
| Address | | | |
| | | | |
| Phone | | | |
| Phone | | | |
| Mobile | | | |
| Primary E-mail Address | | | |
| Additional E-mail Address es) | | | |
| Current Position / Rank / Grade: | | | |
| Duration in Post: | | | |
| | | | |

CONSENT

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

| | |
|------------|------------|
| Signature | Position |
| Print Name | Date /Time |

COMPUTER INFORMATION

| | | |
|---|--|-----------------------------|
| Personal Computer Make and Model | | |
| Serial Number | | |
| Aon Number | | |
| Image Hard Drives | <div style="display: inline-block; border: 1px solid black; padding: 2px 10px;">YES</div> <div style="display: inline-block; border: 1px solid black; padding: 2px 10px;">NO</div> | Date Completed |
| Laptop Computer Make and Model | | |
| Serial Number | | |
| Aon Number | | |
| Image Hard Drives | <div style="display: inline-block; border: 1px solid black; padding: 2px 10px;">YES</div> <div style="display: inline-block; border: 1px solid black; padding: 2px 10px;">NO</div> | Date Completed |
| Network Directories | | |
| To which Domain do you belong | | |
| What is your Network ID | | |
| Home Directory | | |
| Do you have access to a Home Directory on a file share | | |
| If Yes – What is the Home Directory | | |
| Capture Home Directories | <div style="display: inline-block; border: 1px solid black; padding: 2px 10px;">YES</div> <div style="display: inline-block; border: 1px solid black; padding: 2px 10px;">NO</div> | Date Completed |
| Shared Directories | | |
| Have you created any shared directories or subfolders on a Network File Server | | |
| If Yes – What are their names | | |
| Capture Shared Directories | <div style="display: inline-block; border: 1px solid black; padding: 2px 10px;">YES</div> <div style="display: inline-block; border: 1px solid black; padding: 2px 10px;">NO</div> | Date Completed |
| Email | | |
| Capture Current Mailbox | <div style="display: inline-block; border: 1px solid black; padding: 2px 10px;">YES</div> <div style="display: inline-block; border: 1px solid black; padding: 2px 10px;">NO</div> | Date Completed |

| ADDITIONAL INFORMATION | |
|------------------------|--|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | |
| 8 | |
| 9 | |
| 10 | |
| 11 | |
| 12 | |
| 13 | |
| 14 | |
| 15 | |
| 16 | |
| 17 | |
| 18 | |
| 19 | |
| 20 | |
| 21 | |
| 22 | |
| 23 | |
| 24 | |
| 25 | |
| 26 | |
| 27 | |
| 28 | |
| 29 | |
| 30 | |
| 31 | |
| 32 | |
| 33 | |
| 34 | |
| 35 | |
| 36 | |
| 37 | |
| 38 | |
| 39 | |
| 40 | |
| 41 | |
| 42 | |
| 43 | |
| 44 | |
| 45 | |
| 46 | |
| 47 | |
| 48 | |
| 49 | |
| 50 | |
| 51 | |
| 52 | |
| 53 | |
| 54 | |
| 55 | |
| 56 | |
| 57 | |
| 58 | |
| 59 | |
| 60 | |
| 61 | |
| 62 | |
| 63 | |
| 64 | |
| 65 | |
| 66 | |
| 67 | |
| 68 | |
| 69 | |
| 70 | |
| 71 | |
| 72 | |
| 73 | |
| 74 | |
| 75 | |
| 76 | |
| 77 | |
| 78 | |
| 79 | |
| 80 | |
| 81 | |
| 82 | |
| 83 | |
| 84 | |
| 85 | |
| 86 | |
| 87 | |
| 88 | |
| 89 | |
| 90 | |
| 91 | |
| 92 | |
| 93 | |
| 94 | |
| 95 | |
| 96 | |
| 97 | |
| 98 | |
| 99 | |
| 100 | |

This image shows a single page of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There is no handwriting or other markings on the paper.



| | |
|--------------------------|-----------------|
| Exhibit Reference No. | |
| Custody Record Entry No. | Other Reference |

Description of exhibit:.....

.....

Source:

.....

Date:.....Time:.....

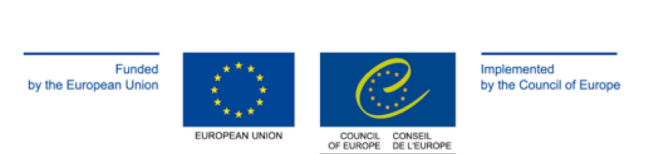
I IDENTIFY THIS EXHIBIT

Signature:

Print Name:

Signature(s) of additional witness(es)

.....



| | |
|--------------------------------|-----------------|
| Exhibit Reference No. | |
| Custody Record Entry Entry No. | Other Reference |

Description of exhibit:.....

.....

Source:

.....

Date:.....Time:.....

I IDENTIFY THIS EXHIBIT

Signature:

Print Name:

Signature(s) of additional witness(es)

.....

| | |
|--------------------------------|-----------------|
| Exhibit Reference No. | |
| Custody Record Entry Entry No. | Other Reference |

Description of exhibit:.....

.....

Source:

.....

Date:.....Time:.....

I IDENTIFY THIS EXHIBIT

Signature:

Print Name:

Signature(s) of additional witness(es)

.....



| | |
|--------------------------------|-----------------|
| Exhibit Reference No. | |
| Custody Record Entry Entry No. | Other Reference |

Description of exhibit:.....

.....

Source:

.....

Date:.....Time:.....

I IDENTIFY THIS EXHIBIT

Signature:

Print Name:

Signature(s) of additional witness(es)

.....

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): <input type="checkbox"/> Desktop <input type="checkbox"/> Laptop <input type="checkbox"/> Server <input type="checkbox"/> Other: |
| Evidence Type (8): <input type="checkbox"/> Hard Drive <input type="checkbox"/> CD/DVD <input type="checkbox"/> Floppy <input type="checkbox"/> RAID <input type="checkbox"/> Other: |
| System State (9): <input type="checkbox"/> On <input type="checkbox"/> Off <input type="checkbox"/> Logged On <input type="checkbox"/> 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): <input type="checkbox"/> Yes <input type="checkbox"/> 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 on Page 4

| 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): | <input type="checkbox"/> EnCase (v.) <input type="checkbox"/> FTK (v.) <input type="checkbox"/> Backup (Software): <input type="checkbox"/> dd Image <input type="checkbox"/> Logical File Copy <input type="checkbox"/> Other: | | | | |
| Acquisition Hardware (24): | <input type="checkbox"/> Fastblock <input type="checkbox"/> Firewire W/B <input type="checkbox"/> Bootdisk <input type="checkbox"/> Direct Connection <input type="checkbox"/> SCSI-IDE W/B <input type="checkbox"/> XOver Cable <input type="checkbox"/> Other: | | | | |
| Evidence Media (25): | <input type="checkbox"/> Hard Drive <input type="checkbox"/> Other: | | | | |
| Serial Number (25): | | | | | |
| Evidence Disk Drive ID Number (25): | | | | | |
| Size of Hard Drive (26): | <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 50px; text-align: center;">GB</td> <td style="width: 50px; text-align: center;">MB</td> </tr> </table> (indicate one) | GB | MB | | |
| GB | MB | | | | |
| Size of Image (27): | <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 50px; text-align: center;">GB</td> <td style="width: 50px; text-align: center;">MB</td> </tr> </table> (indicate one) | GB | MB | | |
| GB | MB | | | | |
| Image Verified (28): | <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 50px; text-align: center;">Yes</td> <td style="width: 50px; text-align: center;">No</td> </tr> </table> Errors (29): <table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 50px; text-align: center;">Yes</td> <td style="width: 50px; text-align: center;">No</td> </tr> </table> | Yes | No | Yes | No |
| Yes | No | | | | |
| Yes | No | | | | |
| Hash Value (30): | | | | | |

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.

[illegible]

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.