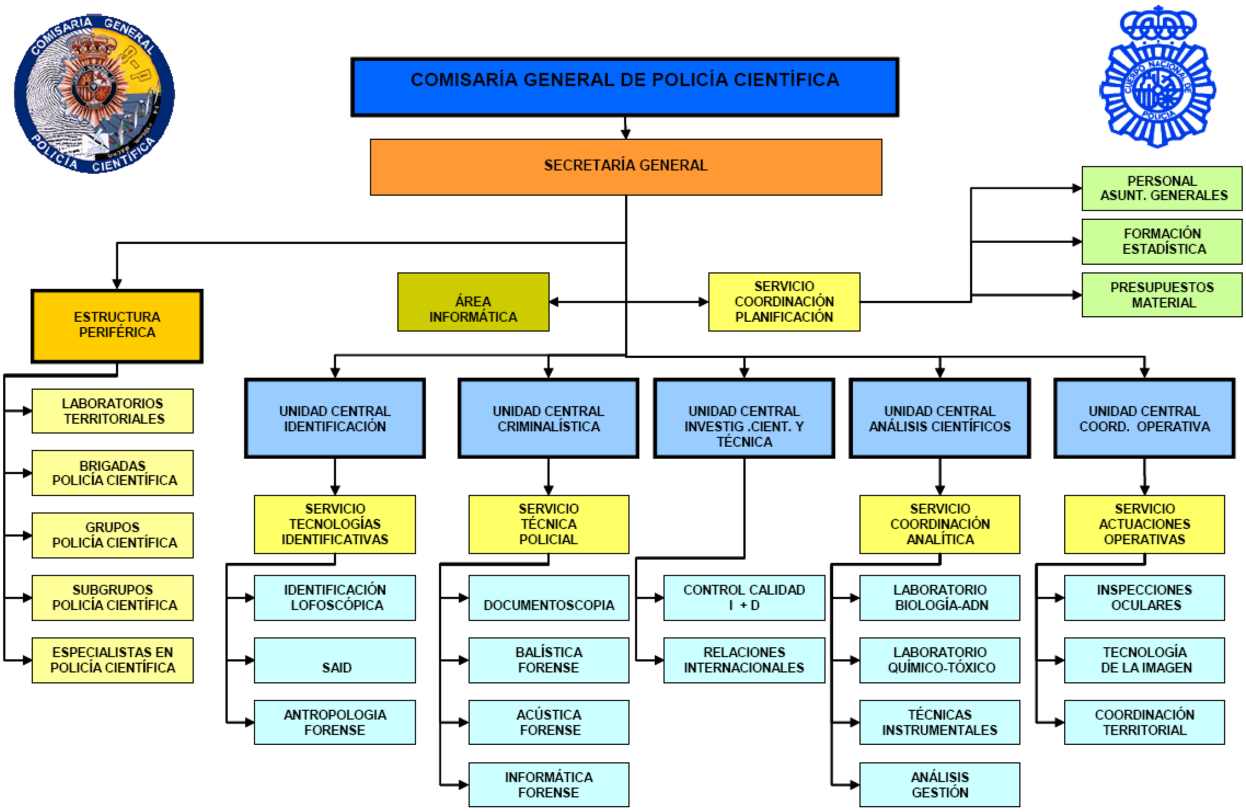
GENERAL DEPARTMENT OF FORENSIC SCIENCE

The Order INT/2103/2005, of 1 July, defining the organisational structure and functions of the Central and Auxiliary Services of the Police Department and Royal Decree 1181/2008 of 11 July which describes the basic organisational structure of the Ministry of the Interior establish that within the scope of the National Police Force, and subject to the coordination with the Deputy Operational Office, the mission of the General Department of Forensic Science is the **“provision of forensic services, and identification, analytical, scientific and technical investigation services, as well as the compilation of expert reports and documents commissioned**".

The duties of the Forensic Science department extend in theory and customary practice to the visual inspection of the scene of the crime, source of supply of evidence; to the collection and compilation of effects, documents, arms and instruments for their study and submission to the court; to the packaging, transport and reception of biological or physical samples with the due guarantees of custody; identification of the person charged, and the fingerprints, traces and remnants left at the scene of the crime; to the study and treatment of samples, ballistic elements, effects, and documents, phonic and phonographic recordings and photographs; to the compilation and drafting of documental and expert reports on these matters, at the request of the Courts of Justice, and the defence thereof in the oral hearing, where all evidence related activities culminate.

STRUCTURE OF THE GENERAL POLICE DEPARTMENT OF FORENSIC SCIENCE

Pursuant to Order INT/2103/2005, of 1 July, defining the organisational structure and functions of the Central and Auxiliary Services of the Police Department, and Royal Decree 1181/2008 of 11 July which describes the basic organisational structure of the Ministry of the Interior it has been established that within the scope of the National Police Force, the General Department of Forensic Science has the following structure:


COMISARÍA GENERAL DE POLICÍA CIENTÍFICA
SECRETARÍA GENERAL
PERSONAL ASUNT. GENERALES
FORMACIÓN ESTADÍSTICA
PRESUPUESTOS MATERIAL
ESTRUCTURA PERIFÉRICA
ÁREA INFORMÁTICA
SERVICIO COORDINACIÓN PLANIFICACIÓN
LABORATORIOS TERRITORIALES
BRIGADAS POLICÍA CIENTÍFICA
GRUPOS POLICÍA CIENTÍFICA
SUBGRUPOS POLICÍA CIENTÍFICA
ESPECIALISTAS EN POLICÍA CIENTÍFICA
UNIDAD CENTRAL IDENTIFICACIÓN
SERVICIO TECNOLOGÍAS IDENTIFICATIVAS
IDENTIFICACIÓN LOFOSCÓPICA
SAID
ANTROPOLOGIA FORENSE
UNIDAD CENTRAL CRIMINALÍSTICA
SERVICIO TÉCNICA POLICIAL
DOCUMENTOSCOPIA
BALÍSTICA FORENSE
ACÚSTICA FORENSE
INFORMÁTICA FORENSE
UNIDAD CENTRAL INVESTIG .CIENT. Y TÉCNICA
CONTROL CALIDAD I + D
RELACIONES INTERNACIONALES
UNIDAD CENTRAL ANÁLISIS CIENTÍFICOS
SERVICIO COORDINACIÓN ANALÍTICA
LABORATORIO BIOLOGÍA-ADN
LABORATORIO QUÍMICO-TÓXICO
TÉCNICAS INSTRUMENTALES
ANÁLISIS GESTIÓN
UNIDAD CENTRAL COORD. OPERATIVA
SERVICIO ACTUACIONES OPERATIVAS
INSPECCIONES OCULARES
TECNOLOGÍA DE LA IMAGEN
COORDINACIÓN TERRITORIAL

GENERAL FORENSIC POLICE DEPARTMENT
HEAD OFFICE
(COL 1)
PERIPHERAL
STRUCTURE

TERRITORIAL LABORATORIES
FORENSIC POLICE BRIGADES
FORENSIC POLICE GROUPS
FORENSIC POLICE SUB GROUPS
FORENSIC SPECIALISTS

(COL 2)

CENTRAL IDENTIFICATION UNIT
IDENTIFICATION TECHNOLOGIES SERVICES
LOPHOSCOPIC IDENTIFICATION
SAID
FORENSIC ANTHROPOLOGY

(COL 3)
IT SECTOR
CENTRAL CRIMINALISTICS UNIT
TECHNICAL POLICE SERVICE
DOCUMENTOSCOPY
FORENSIC BALLISTICS
FORENSIC ACOUSTICS

COMPUTER FORENSICS

(COL 4)

PLANNING AND COORDINATION SERVICE
CENTRAL FORENSIC AND TECHNICAL INVESTIGATION UNIT
QUALITY CONTROL
R+D
INTERNATIONAL RELATIONS

(COL 5)
CENTRAL SCIENTIFIC ANALYSIS UNIT
ANALYTICAL COORDINATION UNIT
BIOLOGY-DNA LABORATORY
CHEMICAL-TOXIC LABORATORY
INSTRUMENTAL TECHNIQUES
ANALYSIS MANAGEMENT

(COL 6)

PERSONNEL
GENERAL MATTERS

TRAINING
STATISTICS

BUDGETS
MATERIALS

CENTRAL OPERATIONAL COORDINATION UNIT
OPERATIONAL ACTIVITIES SERVICE
VISUAL INSPECTIONS
IMAGING TECHNOLOGY
TERRITORIAL COORDINATION

- **CENTRAL DE IDENTIFICATION UNIT**

This department carries out duties relating to fingerprint and photographic records, automatic fingerprint and anthropological identification, as well as the drafting of expert reports for the police and the courts within the scope of their competence.

- **CENTRAL CRIMINALISTICS UNIT**

This department is concerned with the analysis and compilation of expert reports for the police and the courts, in matters of document falsification, graphoscopy, forensic, identificative and operational ballistics, instrumental trace analysis, acoustics and computer forensics.

- **CENTRAL SCIENTIFIC AND TECHNICAL INVESTIGATION UNIT**

The duties of this department relate to scientific and technical investigation and quality control, as well as relations with other bodies and institutions, both at national and international levels, in forensic police matters and coordination in matters of international cooperation with the various Central Units of the General Police Force.

- **CENTRAL SCIENTIFIC ANALYSIS UNIT**

This department is responsible for the management of the Police Forensic Science laboratories in the areas of Biology, DNA, Chemistry and Toxicology, in addition to carrying out specialised analyses and drafting expert reports for the police and the courts, within the scope of their competence. In addition, it is concerned with the Analysis of Operational Management.

- **CENTRAL OPERATIONAL COORDINATION UNIT**

This department assumes the duties of coordinating Operational Services at a national level and those relating to imaging technology, and visual inspection; both in its operational aspect and in the formulation of technical methods and procedures for their performance and practice.

CENTRAL CRIMINALISTICS UNIT

The **COMPUTER FORENSICS SECTION** is part of the Police Forensic Science Department in the Central Criminalistics Unit and in turn part of the Technical Police Service.

Expertise first began to develop in this area in 1999, and over time a Computer Forensics Group was formed, which in 2008 was officially designated as a Section.

The Computer Forensics Section is organised in two separate groups:

1. SOFTWARE ANALYSIS GROUP

This department extracts information from digital supports, hard disks, diskettes, CD or DVDs and memory devices such as compact flash, memory stick, SD card, XD card and variants of the micro or dual type and USB devices such as pen drive, mp3, mp4, ipod or external hard disks; or firewire.

2. ELECTRONICS GROUP

This department extracts electronic devices and mobile telephones.; Iincluding both internal telephone memory and SIM card. Additional memory cards incorporated in some telephones could be classified as portable computer supports.

TERRITORIAL DISTRIBUTION

There is a trend today towards decentralisation to enable a response to all the petitions from different Spanish courts.

At present there are Computer Forensics groups in: the Forensic Police Department (based in Madrid and having national authority), Barcelona, Valencia, Sevillae, La Coruña, Murcia, Las Palmas de Gran Canaria Granada, Málaga, Oviedo, Cantabria, Palma de Mallorca, Vigo, Madrid Head Office, Zaragoza.

COMPUTER FORENSICS

Computer forensics is the science of procuring, preserving, obtaining and presenting electronically processed data which has been saved in an electronic medium, based on the laws of physics, electricity and magnetism. (Digital Evidence).

Due to electromagnetic phenomena, information can be stored, read or even recovered despite it having been ostensibly deleted.

Organised crime in terms of new technologies has been growing at an exponential rate. Computer expertise is one of the types of evidence that is increasingly used in civil, commercial and criminal proceedings.

This area is comes within the scope of competence of the Computer Forensics Laboratories.

REMIT OF THE COMPUTER FORENSICS SECTION

Its job is to analyse the content of digital supports, electronic devices or mobile telephone terminals, used in committing criminal acts, extracting evidence which will serve as judicial proofs, (files, images) relating to the case under investigation and submit such evidence in a clear and ordered manner in the Expert report in response to specific points of information requested by the Judge in each case.

Subsequently to defend the IP in the Oral Hearing.

Forensic IT researchers use a number of techniques to discover evidence, including software tools which automate and speed up analyses.

Electronic evidence may be compiled in various places and from various sources, and may be found in any element or system which is being used to transfer or store data.

In a digital forensic investigation, special attention is given to handling the supports under analysis, in order to maintain the integrity of the evidence. Digital evidence is subject to numerous and serious hazards which are exacerbated by computer viruses, electromagnetic or mechanical deterioration of the support, and also the presence of traps set by the hacker.

The basic rules which help to ensure that evidence is not destroyed or altered during the investigation are:

1. Use only tools and methods which have been previously proven and evaluated in order to determine their accuracy and real sensitivity;

2. Handle the original evidence as little as possible in order to avoid any change in the data;

3. Establish and maintain a chain of custody;
4. Document all activities carried out.

In order to avoid any alteration of the original evidence, a **Procedural and Standards Manua**l has been drafted, detailing the operations involved in each process which standardises and systemises the processing of evidence, and which must be complied with at all levels of competence and authority.

ILLEGAL ACTIVITIES

Crimes which are habitually investigated include:

- Threats, slander, calumny through e-mail, SMS message, notice boards, forums, chat rooms.
- Child protection: production, distribution and possession of child pornography
- Currency counterfeiting and bank fraud:

  Bank carding: use of stolen or fraudulent credit cards

  Phishing: Redirection by e-mail of bogus websites (common among the Russian mafia)

  Nigerian e-mail scams (second source of income in the country after oil according to the FBI)
- Falsification of documents
- Illegal immigration
- Cash point manipulation
- Sexual aggressions
- Many other kinds of crime are also relevant: Homicides, Drug Trafficking, kidnapping, extortion etc.

Aside from the crimes described, any other offence which could leave traces on a digital support and today this could include all crimes.

DIGITAL EVIDENCE

Digital evidence should be considered to be any support which contains extractable information and which can be reproduced in an expert report. Computer evidence of interest is that in which the device under analysis contains user information, and not simply information designed for tasks or functions required for the machine.

TYPES OF EVIDENCE

It is possible to establish three types of support:

- **Computer Supports**

  1.- Portable supports: Those which have a casing permitting their movement ensuring the integrity of the information that they contain, therefore we are talking about CD or DVDs and memory devices such as compact flash, memory stick, SD card, XD card and variants of the micro or dual type and USB devices (such as pen drive, mp3, mp4 , ipod or external hard disks); or firewire.

  2.- Supports contained in desk top or portable equipment; this mainly concerns hard disks located inside computer equipment, hard disks of the IDE , SCSI or SATA type, in their various sizes: 3.5", 2.5" and 1,.8" or microdrive. This type of device may also include PDA or PALM top.

- **Mobile telephone terminals .** Including both internal telephone memory and SIM cards. Additional memory cards incorporated in some telephones could be classified as portable computer supports.

- **Electronic devices.** This group includes any electronic device able to store information, such as skimmers used in card falsification, television payment cards etc.

FORENSIC ANALYSIS OF A DIGITAL SUPPORT

The aim is to discover all the information relating to the matter under investigation which is stored in the support analysed. In the first place the type of support to be analysed should be considered, its physical state, operating system etc.

The stages of a forensic analysis are as follows:

1. **Duplication**
2. **Analysis**
3. **Presentation: Drafting of the Expert Information Report**

Duplication means to make an exact copy of the evidence in order to analyse it. There are two ways of doing this:

➢ **Dumping:** Transfer of original data to a format suitable for processing by the analysis tool to be used.

➢ **Cloning:** Exact copy of the original made bit to bit.

Duplicating the evidence (IMAGING) presents a series of disadvantages, such as the time required and the need for a support to transfer it to; however it turn it has many advantages such as preserving the integrity of the evidence and the possibility of repeating the analysis as often as necessary.

An analysis of this information poses a number of difficulties including:

- Sample size.
- Files of an unknown type.

- Lack of knowledge regarding how computer applications work, therefore ongoing training is important in order to keep up to date.

- Changes in the appearance of information (file extensions/signatures).

- Deleted files.

- Protected files.

- Coded files.

- Steganography.

EXPERT REPORT

This report is submitted as evidence and consists of a statement of a knowledgeable opinion issued by a person who is not necessarily part of the proceedings, based on the facts, circumstances or personal conditions inherent in a punishable act, known within the process and intended for the purpose of evidence and for which it is necessary to be in possession of specific scientific, artistic or practical knowledge.

The following characteristics are essential requisites: It should be ordered, systematic, precise and logical.

Compiling such a report is done in two parts:

1. Laboratory study written up in report form.
2. Vocal explanation given before a Court in the Oral Hearing.

Legal basis: Chapter VII: Expert Report

Art.456 LECr.: The Judge shall decide on the Expert Report when, in order to discover or consider a specific fact or important circumstance in the Proceedings, scientific or artistic knowledge is necessary or appropriate.

Art^{o} 478 LECr: The Expert Report shall comprise:

a) A description of the person or thing who or which is the subject of the report in the state or mode in which they are found.

b) Detailed list of all the actions taken by the experts and their result, written and authorised in the same manner as described previously.

c) Conclusions which the experts have reached pursuant to the principles and rules of their science or art regarding such data.

The basic structure of the Expert Report is drawn up as follows:

1) BACKGROUND.– providing information on the requesting body, the object of the report and the material examined.

2) STUDY PERFORMED – Details of the person drafting the report and analysis of the material.

3) CONCLUSIONS: Explanation of the implications, description of the elements that make up the report, date and signature of the acting experts.

CLONING OF CARDS WITH MAGNETIC BANDS - SKIMMING

One of the studies carried out by the Electronic Group of the Computer Forensics Section is the study of magnetic band readers and bank keyboards used for cloning of bank cards.

As members of the University Institute of Investigation into Forensic Science (IUICP) in conjunction with the University of Alcalá de Henares and the collaboration of the Guardia Civil, both software (programme) and hardware (the physical part of the system) have been developed to enable the recovery and reading of information stored by MP3 skimmers (a type of false magnetic band reader which adapts to the card insertion slots in cash point machines in order to record the magnetic band readings) and thus discover the card numbers which have been copied.

The *Electronic Group in this Section* is able to obtain full information from the MP3 devices coupled to the cash point machines and which is recorded in the form of a sound archive.

The information contained in magnetic cards or credit/debit cards are read through a band reader head which reads the DOS track of the cards (track which contains the card numeration) and recorded in the MP3 in analogue form by the micro entry connector, thus recording the data in a sound archive.

The importance of this development for data recovery from the MP3 skimmers has made them pioneers in Europe in this field, having developed a programme which enables data access and the possibility of decoding it in order to obtain information on magnetic bands.

TELEPHONES

The most interesting aspect from the forensic perspective is their information storage capacity. An intelligent telephone generally consists of the following components which are able to store information:

1. A terminal
2. One or various SIM cards
3. One or various additional memory cards

A **mobile telephone terminal** contains two types of memory: volatile and non volatile memory The volatile memory is similar to that with which we are all familiar as RAM memory in personal computers. It is information which is lost when the electrical current is interrupted. The non- volatile memory is that content which is not lost when the electrical supply is interrupted It is this latter type of memory which is to be considered here.

In the non- volatile memory of a mobile telephone the data relating to the operating system and programmes is stored, however, also the user data such as :

- Text files, images sound, vídeo.
- Telephone directory, register of calls, SMS messages or multimedia
- E-mails, register of visits to websites

- Personal Agenda, notes, appointments, etc.

The structures of these memories also vary between manufacturers and between different models and versions of terminals of each manufacturer. This is the biggest problem we encounter when attempting to access the data contained in these devices.

The **SIM card** is a removable component which contains essential information on the subscriber. The main purpose of the SIM card is to authenticate the mobile telephone user's identity when connecting to the network to access the contracted services.

Access to SIM cards is protected by means of a personal identification code (PIN number). The PIN code (a four figure number) may be changed by the subscriber, so that he/she is the only person who knows it.

The unlocking code is known as the PUK code and is provided by telephone companies who manage the blocked SIM.

Data contained in a SIM card:

1. Information relating to the service provided by the telephone company.
2. Telephone directory and information on calls, made, received and missed.
3. Information on text messages both SMS (normal text messages) and EMS (improved SMS containing animations, tunes, sounds etc) and multimedia messages.
4. Localisation information.