Forensics

This page is from APP, the official source of professional practice for policing.

First published 2 July 2017 Updated 21 February 2022
Written by College of Policing
10 mins read

Investigating a crime scene and forensic analysis using specialist procedures and techniques can provide evidence to:

- prove that a crime has been committed
- exclude a suspect from a scene
- link a suspect with a scene
- establish the identity of a victim, suspect or witness
- corroborate or disprove witness accounts
- interpret the scene in relation to movements within the scene and sequences of events
- link crime scene to crime scene and provide intelligence on crime patterns

The principle of exchange

Dr Edmond Locard formulated the principle of exchange. This means anyone who enters a scene both takes something of the scene away with them and leaves something of themselves behind. Every contact leaves a trace, however minuscule. This could be, for example:

- fingerprints
- DNA
- fibres
- footwear marks

This trace is normally caused by objects or substances coming into contact with one another and leaving a minute sample on the contact surfaces.

When a foreign object or piece of material has been brought to a crime scene, tracing its origin can assist an investigation. Similarly, finding trace evidence from the victim or crime scene on a suspect can also have a strong impact on a case.

This principle can also result in **cross contamination** of material if procedures and practices are not adopted to prevent it.

Streamlined Forensic Reporting (SFR) is a process designed to enable investigators, scientists and prosecutors to comply with the Criminal Procedure Rules.

Information on Streamlined Forensic Reporting is available from the **Forensic Capability Network**.

For further information see:

- **Crime scene DNA: anti-contamination guidance**

For forensic learning programmes and role profiles see the **College of Policing website**.

Forensic Science Regulator

The **Forensic Science Regulator (FSR)** ensures that the provision of forensic science services across the criminal justice system is subject to an appropriate regime of scientific quality standards. These are organisational standards.

The FSR has published codes of practice and conduct for forensic service providers and practitioners. It has also published several accompanying subject-specific appendices that set out required standards and extension of scope to existing standards ISO17025 and ISO17020.

An organisation is assessed against the ISO standards and the FSR's codes of practice. Successful assessment results in an organisation becoming an accredited supplier of forensic science services. Accreditation is an ongoing organisational requirement and subject to regular review.

Forces are assessed against relevant standards by the **United Kingdom Accreditation Service (UKAS)**, the sole national accreditation body recognised by government to assess against agreed standards.

Codes of conduct and practice

Forensic science providers: Codes of practice and conduct.

For further information, see the **Forensic Science Regulator**.

Crime scene investigation

The police service employs a number of forensic services to enable appropriate processing of a wide range of crime scenes.

External services (for example, Home Office pathologists, forensic service providers) may also assist. Further guidance relating to the support available to investigators in serious or major cases can be obtained from the **National Crime Agency Major Crime Investigative Support**.

The specific circumstances that a crime scene investigator (CSI) encounters at a crime scene dictate the approach required. The forensic approach to a volume crime scene varies from that of a major crime scene. The processes implemented, however, are mainly similar. In serious or major cases, a formal strategy for the forensic response is compiled by a forensic manager in consultation with, and agreed by, the senior investigating officer. The strategy includes:

- identifying health, safety and security issues and establishing the dimensions of the scene
- coordinating and communicating with relevant personnel
- an initial walk-through of the scene identifying key areas of interest
- documenting and recording the scene at all stages of the examination process
- recovering and recording material of interest using appropriate specialists and techniques
- a secondary walk-through of the scene and a review

See:

- FSS (2004) Scenes of Crime Handbook – available through local CSI department
- **ENFSI Crime Scene Best Practice Manual**

For further information on scene identification and preservation, see **Scene strategy**.

Photography and imaging

Photography is used to illustrate the crime scene for anyone who has not attended or cannot attend the scene. Photographs taken at a crime scene should include general views, scaled imagery of identifying marks and contextual photographs showing the location of areas of interest, including:

- general photographs to record comprehensive views of the scene

- scaled photographs to record identifying marks, for example, fingerprints, footwear marks or tool marks – scaled photographs may be taken before, during and after any processes which may be carried out on the item
- contextual photographs to record the location of any seized exhibits or areas of interest, while also demonstrating their orientation and relevance to the scene itself

Where needed, a series of photographs may be uploaded onto computer software to create a panoramic 360° view of the crime scene. This image can be navigated on screen, and can help the viewer contextualise the scene. Videos may also be used. These tools can be valuable when briefing others and may also be used for evidential purposes.

See also: **Home Office (2007) guidance: Storage, Replay and Disposal of Digital Evidential Images (Publication No 53/07**)

Community forums are available on the Forensics Community and the **Imaging and Identification Community** (these links are available to **authorised users** who are logged on to the Knowledge Hub).

Fire investigation

Investigating fire scenes is a specialist aspect of the CSI's role.

See:

- FSR Protocol for Investigators of Fires and Explosions for the Criminal Justice Systems in the UK (forthcoming).
- **ENFSI Best practice manual for the investigation of fire scenes**

Fingerprint analysis and comparison

Fingerprint impressions recovered from crime scenes or from items submitted to a fingerprint enhancement laboratory are subjected to analysis and comparison by a force/regional fingerprint bureau.

A fingerprint bureau has three main functions:

- to maintain the National Fingerprint Collection
- to identify finger, palm and foot prints recovered from crime scenes
- to prepare and present expert evidence in courts of law

See:

- **Codes of Practice and Conduct: Fingerprint comparison, FSR-C-128**
- **Fingerprint Examination – Terminology, Definitions and Acronyms, FSR-I-402**
- **LiveScan Good Practice Guide Issue 2 November 2010**
- **ACPO/NPIA (2008) Best Practice Manual – Remote Transmission of Crime Scene Marks**
- **ENFSI (2015) Best Practice Manual for Fingerprint Examination**

Fingerprint enhancement

Some items recovered from a crime scene may be submitted to a force fingerprint enhancement laboratory (FEL) for processing to recover fingerprint evidence. FEL practitioners subject the items to a range of visual, physical and chemical processes to visualise and recover further fingerprint evidence. When warranted by the investigation, FEL practitioners may attend crime scenes to carry out a limited range of processes.

See the Home Office Centre for Applied Science and Technology (2014) Fingerprint Visualisation Manual, available from force fingerprint enhancement laboratories.

Footwear

Footwear marks recovered from a crime scene or from a suspect can be analysed and interpreted to provide intelligence. Footwear marks recovered from crime scenes can be linked to other crime scenes and be used to support other forms of intelligence to help identify prolific, persistent offenders. Following a suspect’s arrest, footwear marks can also be used to identify additional outstanding offences.

Some crime scene marks can be compared with a suspect’s footwear or other crime scene marks. The initial aim of the comparison is to exclude any links between the items being compared. If it is not possible to exclude a link between the items, practitioners consider and evaluate the levels of correspondence between items. Suitably qualified practitioners can provide evidence of opinion on the value of footwear comparisons.

See also:

- **NPIA (2007) Footwear Marks Recovery Manual**
- **ACPO (2007) Footwear Intelligence Guidance for Scientific Support**

Forensic submissions

The forensic submissions team provide a centralised force submissions service to meet the requirements of the criminal justice system and obtain best value from available forensic resources.

The service includes:

- forensic strategy advice and documentation, at both submission level and in complex and major crime, for example, attending strategy meetings
- risk assessments and case coordination
- collating and sharing good practice
- commissioning services
- contract and budget management
- advising on **Protection of Freedoms Act** issues and coordinating responses
- advising on DNA issues, for example, speculative searches, mixtures, partials and intelligence-led screening
- developing and delivering forensic packages for example, DNA, footwear

Note: some forces now adopt a collaborative approach to this function.

See:

- **NPIA (2012) Forensic Submissions Good Practice Guide**

Digital forensics

The NPCC Digital Forensics portfolio board has defined digital forensics as:

the application of science to the identification, collection, examination and analysis of electronic data whilst preserving the integrity of the information and maintaining the chain of custody of that data.

The Forensic Science Regulator defines it as:

Digital forensics is the process by which information is extracted from data storage media (for example, devices, remote storage and systems associated with computing, imaging, image comparison, video processing and enhancement [including CCTV], audio analysis, satellite navigation, communications), rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings. The definition is intentionally wide and any exclusions will be explicit. Automatic number plate recognition, manual classification of indecent images of children, crime scene photography, eFit, recovery from a working CCTV system, CCTV replay for viewing with no further analysis (acknowledging that there may be quality limitations to the material viewed) all should be conducted by competent staff using methods approved by the organisation, but are excluded from the ISO/IEC 17025 requirement.

FSR Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, Issue 3 (2016).

The Forensic Regulator requires compliance by forces with **quality standards** for digital forensics by 2017.

Digital evidence can help progress investigations and may be used in criminal proceedings.

Examples of digital evidence include communications data on mobile phones, data contained in personal computers, laptops, tablets and other mobile devices. This also includes all storage media, for example, SD cards, USB flash drives and other forms of external storage devices.

The emergence of cloud computing and other technologies for storing data on the internet has introduced new challenges for digital forensic practitioners. The use of social media applications requires that electronic evidence is captured in real time or the opportunity to seize that evidence may be lost. This has introduced the concept of online digital forensics, where data can be captured and analysed in real time, supported by appropriate legal authority.

Identifying and preserving digital evidence

The Association of Chief Police Officers (ACPO) published a **Good Practice Guide** that provides guidance on how to identify, preserve and recover electronic evidence.

The four principles from the good practice guide are applicable to all forms of digital evidence. For these principles, see **computer-based electronic evidence**.

See also:

FSR guidance

- **Codes of practice and conduct: Speech and audio forensic services FSR-C-134**
- **Codes of practice and conduct: Video analysis FSR-C-119**
- **Codes of practice and conduct: Cell site analysis FSR-C-135**
- **Method Validation in Digital Forensics FSR-G-218**

CCTV guidance

- **APP Investigation – Passive data generators**

Community forums are available on the Knowledge Hub **CCTV, Imaging and Identification** and **eForensics** communities (these links are available to authorised users who are logged on to the **Knowledge Hub**).

Other sources of information and guidance

Other publications include:

- **FCN (2021) DNA Good Practice Manual**
- **ILAC G19:08/2014 Modules in a Forensic Science Process**
- **Criminal Procedure Rules and Criminal Practice Directions (2015) – these are updated each year**
- **NPCC Retention, Storage and Destruction of Materials and Records relating to Forensic Examination guidance**

Other relevant organisations include:

- **The Chartered Society of Forensic Sciences**
- **European Network of Forensic Science Institutes**
- **The Faculty of Forensic and Legal Medicine**

Tags

Investigation