# Digital forensics DGFS

Recovering and investigating material found in digital devices.

|  |
| --- |
| **Guidance Notes:**Activities may include, but are not limited to:* collecting, processing, preserving and analysing material
* presenting forensic evidence based on the totality of findings.

The scope of digital forensics includes finding evidence on computers and any device capable of storing digital data. The evidence may be used in support of security vulnerability mitigation, criminal, fraud, counterintelligence, or law enforcement investigations. |

## Level 2

Assists with digital forensic investigations under routine supervision.
Helps recover damaged, deleted, or hidden data from devices.
Helps collect information and evidence.

## Level 3

Supports digital forensic investigations by applying standard tools and techniques to investigate devices.
Recovers damaged, deleted or hidden data from devices.
Maintains integrity of records and collects information and evidence in a legally admissible way.

## Level 4

Designs and executes complex digital forensic investigations on devices.
Specifies requirements for resources and tools to perform investigations.
Processes and analyses evidence in line with policy, standards and guidelines and supports the production of forensics findings and reports.

## Level 5

Conducts investigations to correctly gather, analyse and present findings, including digital evidence, to both business and legal audiences.
Collates conclusions and recommendations and presents forensics findings to stakeholders.
Plans and manages digital forensics activities within the organisation. Provides expert advice on digital forensics.
Contributes to the development of digital forensics policies, standards and guidelines. Evaluates and selects digital forensics tools and techniques.

## Level 6

Plans and leads the organisation’s approach to digital forensics.
Sets policies, standards and guidelines for how the organisation conducts digital forensic investigations.
Leads and manages high risk, large or wide-ranging digital forensics investigations engaging additional specialists if required.
Authorises the release of formal forensics reports.