

## INTERNATIONAL STANDARD

### TITLE:

**Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence**

**Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves numériques**

### PREPARED BY:

**Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC27, IT Security techniques**

### DATE AND PLACE OF PUBLICATION:

**15 October 2012, Geneva**

### PUBLISHER:

**ISO/IEC**

### REFERENCE NUMBER:

**ISO/IEC 27037:2012**

The description of this document is available on the internet and set out under the rubric 'Scope':-

The Standard provides guidelines for specific activities in the handling of digital evidence, which are the identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value.

It provides guidance to individuals with respect to common situations encountered throughout the digital evidence handling process and assists organizations in their disciplinary procedures and in facilitating the exchange of potential digital evidence between jurisdictions.

The Standard offers guidance for the following devices and circumstances (this is an indicative list and is not exhaustive):

1. Digital storage media used in standard computers like hard drives, floppy disks, optical and magneto optical disks, data devices with similar functions,
2. Mobile phones, Personal Digital Assistants (PDAs), Personal Electronic Devices (PEDs), memory cards,
3. Mobile navigation systems,
4. Digital still and video cameras (including CCTV),
5. Standard computer with network connections,
6. Networks based on TCP/IP and other digital protocols, and
7. Devices with similar functions as above.