G8 Proposed Principles For The Procedures Relating To Digital Evidence

In March 1998, IOCE was appointed to draw international principles for the procedures relating to digital evidence, to ensure the harmonization of methods and practices among nations and guarantee the ability to use digital evidence collected by one state in the courts of another state.

In March 2000, the first report of IOCE was presented to the subgroup, proposing a series of definitions and principles, following the International high-tech crimes and forensics conference in London in October 1999.

After review by the experts of the subgroup, the following recommendations are made:

1. Each member State is encouraged to consider the following principles when establishing procedures for the collection, preservation and use of digital evidence, according to its national law and standards bodies, and to be aware of potential differences when collecting evidence at the request of other States.
2. These principles should be submitted by IOCE to other national, regional and international standards making bodies and organizations responsible for the promotion of procedures relating to digital evidence for review.
3. IOCE should develop in consultation with the above-mentioned bodies, a generic good practice guide for the collection, preservation and use of digital evidence, encompassing the range of existing sources of digital evidence.
4. The high-tech crime subgroup should review regularly the work of IOCE.

Principles

- **When dealing with digital evidence, all of the general forensic and procedural principles must be applied.**
- **Upon seizing digital evidence, actions taken should not change that evidence.**
- **When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.**
- **All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.**
- **An Individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.**
- **Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles**

General Definitions relating to digital evidence

Digital Evidence
Information stored or transmitted in binary form that may be relied upon in court.
Original Digital Evidence
Physical items and those data objects, which are associated with those items at the time of seizure.
Duplicate Digital Evidence
A duplicate is an accurate digital reproduction of all data objects contained on the original physical item.
Copy
A copy is an accurate reproduction of information contained in the data objects independent of the original physical item.