ACPO Principles of Digital Evidence Collection & Preservation

Computer-based electronic evidence is held to the same rules and expectations that apply to all other evidence types when presented before a court. The onus is on the prosecution to prove to a court that the evidence produced by them is no more and no less than it was when it was first taken into the possession of the Police at the point of seizure.

As computer and mobile phone operating systems and other programs present often alter, including create and delete files from a device and this can happen without the user being aware of it, simply by being switched on.

To comply with the ACPO principles of computer based evidence, where possible a full bit copy image of the memory present on the digital device should be taken. The ACPO guidelines for digital-based evidence also require that any data is acquired using a suitable write blocking hardware unit, however, on some occasions this is not possible, for example, when the original digital device itself requires access. In these circumstances, the individual who carries out this process is sufficiently competent to provide evidence in court to explain the actions undertaken.

When providing evidence to court, the individual must display objectivity and fairness whilst being able to explain each process completed with the digital evidence, including the acquisition and examination of it, so that a third party digital examiner/expert can repeat the same process if required and arrive at the same result as that presented to the court.

The main principles of the ACPO Good Practice Guide for Computer Based Electronic Evidence are:

ACPO Principle 1

That no action is taken that should change data held on a digital device including a computer or mobile phone that may subsequently be relied upon as evidence in court.

ACPO Principle 2

Where a person finds it necessary to access original data held on a digital device, that the person must be competent to do so, and able to explain their actions and the implications of those actions on the digital evidence to a Court.

ACPO Principle 3

That a trail or record of all actions taken that have been applied to the digital evidence should be created and preserved. An independent third party forensic expert should be able to examine those processes and reach the same conclusion.

ACPO Principle 4

That the individual that is leading the investigation has overall responsibility to ensure that the ACPO principles are followed throughout the investigation.

7 Topics | 4 Quizzes

IR4) Containment, Eradication, and Recovery Phase

Privacy & Cookies Policy

Privacy - Terms