Orion Investigations
20th Floor, Unit 2001-2002, 29 Sukhumvit 63, North Klong Tan
Wattana, Bangkok 10110

Orion Investigations

Computer Forensics | Mobile Phone Forensics| Malware Investigations | Training |Data Recovery

Computer Forensics Services

What is Computer Forensics?

February 2012

Date: 02-02-2012

Author: Andrew Smith

What is Computer Forensics?

Computer forensics is the examination of electronic data stored on computers and other digital storage devices for evidence using a forensically sound method.

It is important at this stage to be clear on what we mean by the terms evidence and forensically sound method.

Evidence – is information that supports a conclusion.

Forensically sound method – is a method that does not alter the source evidence, except to the minimum extent necessary to obtain the evidence. The manner used to obtain the evidence must be documented and justified.

Computer forensics can be broken down into five stages.

Preservation – When dealing with digital data the investigator must do everything possible to preserve the data. This must be done in such a way that the actions of the investigator do not cause changes to the data. This typically involves creating a forensic image or a forensic clone of the original media. Digital data may be stored on hard drives, CD/DVD, floppy disks, pen drives, mobile phones, music players and assorted backup tapes.

Identification – Year on year the storage capacity of hard drives is growing. As a result the investigation may consist of hundreds of Gigabytes of digital data. In order to identify potential evidence the investigator will employ techniques such as keyword searches or the filtering of specific files such as documents, images or Internet history files.

Extraction – Once potential evidence has been identified it will need to be extracted from the forensic image. Depending on the size of the data it may be possible to print out hard copies such as documents. However data such as Internet history can amount to hundreds of pages and will need to be produced in an electronic format.

Interpretation – Identifying and extracting potential evidence is only part of the role for a forensic investigator. It is vital that correct interpretation of the evidence takes place. The investigator should never rely on a single automated tool. The investigator needs to have the skills to manually verify and understand the results produced by the forensic software.

Documentation of computer evidence - Once an investigation begins the investigator needs to maintain contemporaneous notes in relation to the handling of the digital media through to the steps undertaken throughout the investigation. The notes should contain sufficient details so a third party can reproduce the results. Producing key evidence will amount to nothing if the investigator cannot produce a clear well written report. It is important to avoid using technical jargon whenever possible and where technical terms need to be used, they should be clearly explained. The investigator may be required to present their evidence in court as an expert witness.

The UK Association of Chief Police Officers (ACPO) has produced a guide called **Good Practice Guide for Computer-Based Electronic Evidence.** The guide lays down four key principles.

Principle 1:

No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court.

Principle 2:

In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3:

An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4:

The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to.

The four principles represent best practice in relation to computer forensic investigations, whether it is a criminal, civil or corporate investigation. By adhering to the principles it will help ensure that no questions are raised in relation to the integrity of the evidence produced from digital data.