Admissibility of digital evidence in court

ELIAS NEOCLEOUS & Co LLC

02 July 2019

Pantelis Mountrakis

Litigation, Cyprus

Michael Ioannou

- **Rise of digital forensics**
- **Principles of digital evidence**
- **Digital evidence handling**
- **Admissibility of evidence**

Rise of digital forensics

The rapid development of technology and the use of digital devices such as mobile phones, computers and tablets, which have become an indispensable part of modern society, have resulted in a significant transition from the creation of physical to digital data.

In conjunction with the proliferation of technology, there is a tendency to use information derived from digital devices for criminal activities (eg, cybercrimes like hacking, malware and internet fraud, but also traditional crimes such as homicide, drug trafficking and terrorism).

Consequently, the role of digital forensics in fighting crime is becoming ever more important and it is critical for law firms and courts to develop a well-thought-out strategy for such investigations. In *Penderhill*, the Supreme Court clarified that the courts must be appropriately responsive to the technical changes that are taking place.**(1)**

Digital forensics follows a similar process to crime scene forensics when collecting evidence for a potential trial. The digital forensics process involves collecting, analysing and reporting on digital data in a way that is legally admissible. Digital evidence can also be used to prove whether a person has been involved in crimes that are unrelated to technology, such as murder or larceny.

The main repositories of digital evidence are computers, storage devices, telephones, networks, cloud servers and emails. However, as the Internet of Things develops, many other devices will provide digital evidence.

This article aims to demystify this subject and define high-level criteria that can be used to identify the needs and admissibility of digital evidence in court.

Principles of digital evidence

Several best practices and guidelines developed by the Scientific Working Group on Digital Evidence, the UK Association of Chief Police Officers and the US National Institute of Justice have been developed to assist investigators in the collection and handling of digital evidence during forensic analysis. Evidence acquisition should always be performed to ensure that it will be admissible in legal proceedings. The key criteria for handling such evidence are as follows:

- Under no circumstances should evidence be altered. No action should alter data held on a computer, storage media or network which may subsequently be relied on in court. Changes on a computer may occur by merely turning it on or moving the mouse.
- Where a person finds it necessary to access original data held on a computer or storage medium, they must be competent to do so and be able to give evidence to explain the actions taken. This principle applies even though an investigation may be time critical and evidence must be examined immediately.
- An audit trail or record of all processes applied to computer-based electronic evidence should be created and preserved. A third party should be able to repeat these processes and replicate the results.
- The person in charge of the investigation has the overall responsibility for ensuring that the law and the above principles are adhered to.

Digital evidence handling

The following best practices should be followed with regard to digital evidence handling:

- Auditability – investigators should document all actions taken (Principle 3) to enable an independent assessor acting on behalf of an interested party to evaluate said actions.
- Justifiability – investigators should be able to justify all actions and methods used in handling digital evidence and demonstrate that the method chosen to obtain the potential evidence was the best choice by successfully reproducing or validating the actions and methods used.
- Repeatability – it should be possible for an independent assessor or the authorised interested parties to repeat or reproduce the tasks performed.
- Reproducibility – it may be necessary to obtain the same results in a different testing environment.

Admissibility of evidence

Evidence is legally admissible when it:

- is offered to prove the facts of a case; and
- does not violate the Constitution or other legal statutes.**(2)**

The golden rule of admissibility is that all evidence which could be relevant is admissible and evidence that is irrelevant is inadmissible.**(3)** Therefore, the courts must determine whether digital evidence could be relevant to the disputed facts of the case and whether it is suitable and safe to be admitted in proceedings. In practice, admissibility is a set of legal tests carried out by a judge to assess an item of evidence according to the following criteria:

- Relevance and reliability – digital evidence should be examined for traces of tampering, deletion or other changes. The system that gave the relevant results must

function properly and produce accurate results. In this respect, a recent Supreme Court decision upheld a first-instance judgment ordering the appointment of an IT expert who could obtain information from the server of a third party which was essential for the case.**(4)**

- Illegally obtained evidence – in principle, evidence obtained in violation of the Constitution is inadmissible. As a result, some forms of digital evidence, such as IP addresses, may not be accepted by the courts, as the IP address of a user is closely connected with their privacy, a human right that is protected under the Constitution.**(5)** However, pursuant to Law 183(I)/07, evidence concerning the privacy of a person may be given to the police for investigation purposes. The ability to obtain such evidence is limited to cases where the police are investigating felonies and a court order has been issued for that purpose.**(6)**
- Assessing authenticity of evidence – the courts must be satisfied that evidence was acquired from a specific system or location and a complete and accurate copy of digital evidence is needed. Further, evidence must remain unchanged from when it was collected. This can be achieved by hashing the digital evidence (Md5, SHA). If the hashed code is the same, it proves that the digital evidence has not been tampered with.
- Documents to demonstrate and support the authenticity of the evidence – a chain of custody to record the transfer of the evidence, integrity documentation to compare the digital fingerprint of the evidence, taken at the time of collection and the fingerprint in its current state are required.
- Best evidence – the best available evidence should be provided to the court. Courts generally accept identical duplicates, especially in cases where it is adequately proved that the original evidence has been lost or destroyed,**(7)** unless a question is raised about the authenticity of the original and the accuracy of the copy.
- Search warrants – evidence may not be admitted in court if it has been obtained without authorisation.
- Scientific evidence and process – the admissibility of digital evidence and the tools, methods and techniques used in the investigation can be challenged in court.

For further information on this topic please contact Pantelis Mountrakis or Michael Ioannou at Elias Neocleous & Co LLC by telephone (+357 25 110 110) or email (pantelis.mountrakis@neo.law or michael.ioannou@neo.law). The Elias Neocleous & Co LLC website can be accessed at www.neo.law.

Endnotes

(1) *Penderhill Holding Limited ao v Ioannis Kloukinas,* Civil Appeals 319/11 and 320/11, 13 January 2014.

(2) Takis Iliadis and Nicolas Santis, *Evidence Law* (2nd ed, Hippasus Publishing, 2016) p 66.

(3) Steven Powles, Lydia Waine, Radmila May, *May on Criminal Evidence* (6th ed, Sweet & Maxwell, 2015).

(4) *Metaquotes Software Ltd ao v Dababou,* Civil Appeal E324//2016, 14 November 2018.

(5) *Demetris Shiamishis v The Police*, [2011] 2 CLR 308.

(6) Retention of Telecommunication Data for the Purpose of the Investigation of Serious Crimes Law (L 183(I)/2007).

(7) *Gold Seal Shipping Company Ltd v Standard Fruit Company (Bermuda) Limited*, [2000] 1(C) CLR 1552.