Ensuring the Legality of the Digital Forensic Process

Jason Jordaan: CFCE, CFE, PMCSSA, ACE
MTech, BComHons, BSc, BTech
Digital Forensic Scientist
jason@digitalforensicscientists.com

Introduction

- Evidence is crucial in any case brought before a criminal or civil court, and no legal decisions can be made without evidence
- Generally, any evidence that is obtained illegally, or unconstitutionally, will not be admissible, and will not be considered in court
- If illegally obtained or unconstitutionally obtained evidence leads to other evidence, that will likely be excluded as well – fruits of a poisoned tree
- It is crucial that digital evidence is obtained legally to have any legal value

Unlawful Access to Data

- Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002 creates the criminal offence of unlawful access to data. Section 86(1) states that subject to the Interception and Monitoring Prohibition Act, a person who intentionally accesses of intercepts any data without authority or permission to do so is guilty of an offence
- The offence has three specific elements: access, data, authority or permission

Access

- According to the Concise Oxford English Dictionary, the term access in relation to computing means to “obtain, examine, or retrieve data”
- In terms of the offense created by Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002, due to the fact that access as a term is not specifically defined, the common usage of the term is considered to be an accurate general definition of what is meant by access to data, namely:
  - To obtain data
  - To examine data
  - To retrieve data
- Should a person do any of these actions in relation to data, then they will have accessed the data.

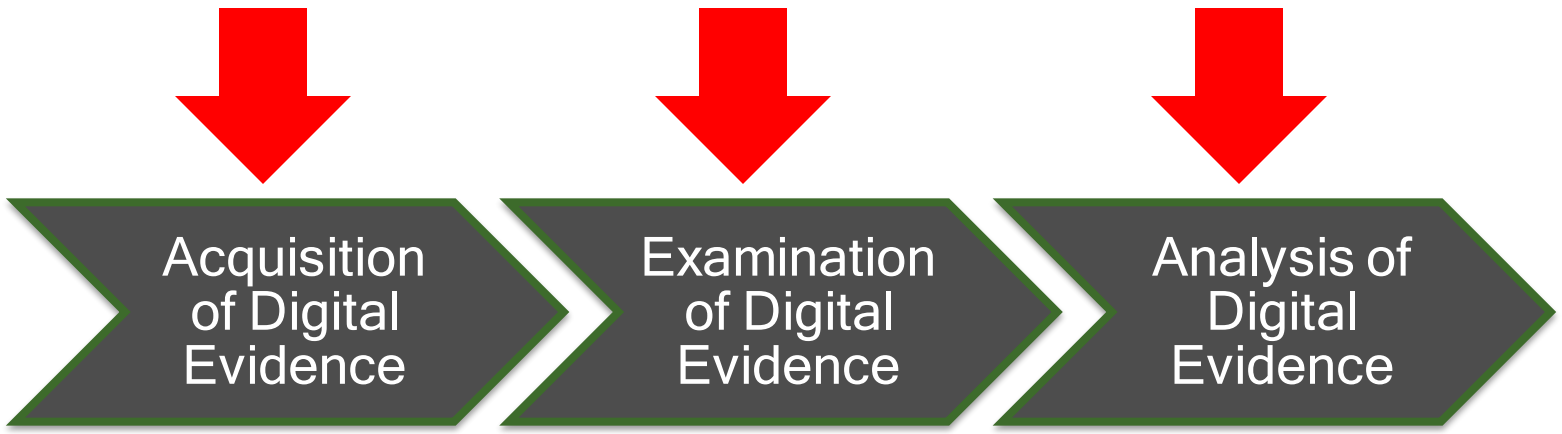
Data

- Section 1 of the Electronic Communications and Transactions Act 25 of 2002 defines data as the electronic representation of information in any form.
- According to the Concise Oxford English Dictionary, the term information means “what is conveyed or represented by a particular sequence of symbols”. At the most fundamental level, the data contained on a digital device or storage media exists in a binary numerical form, consisting of “1”and “0” in a sequence of such numbers, which are then represented at a byte level by hexadecimal numbers, and then, as human readable information. In other words it can be stated that so long as information is in a binary digital format at its most basic representation level, then it satisfies the legal definition of data.

Authority or Permission

- The Electronic Communications and Transactions Act 25 of 2002 does not defined authority (at least in terms of access to data), nor does it define permission.
- According the Oxford Dictionary of Law, it means “power delegated to a person or body to act in a particular way” [7]. To authorize is the process of giving authority, and in the Concise Oxford English Dictionary, it means “give permission for or approval to”. According to the Concise Oxford English Dictionary, the term permission means “authorization”, which is a derivative word of “authorize”.
- In other words, authorization or permission can be defined as when a person or organization that has power over something gives the authority to another to have power over that thing.

The Forensic Process



Digital Forensics and 86(1)

- The fundamental offense defined by Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002, is when anyone accesses any data without authorization or permission.
- Access is a fundamental part of the digital forensics process is always intentional; if this access occurs without the appropriate permission or authorization, then they commit a criminal offence.
- In other words, if any digital forensics process is performed in relation to any data (including forensic acquisition and imaging, examination, and analysis), and that they did not have permission or authority from an appropriate person or authority to do so; then they have contravened Section 86(1) of the Electronic Communications and Transactions Act.

Implications

- In general, evidence that has been obtained unlawfully, that is in contravention of the law, then it would probably be ruled inadmissible in a criminal prosecution, and may potentially be ruled inadmissible in civil proceedings as well.
- If the digital evidence has been obtained in contravention of Section 86(1) of the Electronic Communications and Transactions Act, then there is a probability that it could be ruled inadmissible in a court of law.
- If a digital forensic examiner does not have the appropriate authority or permission to access the data necessary for the digital forensic process, and they do so, then they face the risk of being criminally prosecuted in terms of Section 86(1), but the digital forensic practitioner could potentially be subject to civil litigation for delict.

Legal Authority

- To be able to conduct digital forensics, a digital forensics practitioner requires access to the data that they will conduct digital forensics processes on. This generally requires access to the physical electronic device or storage media containing the data, and the authority or permission to access these and thus the data contained thereon.
- There are three methods to obtain the necessary legal authority to gain access to the physical electronic devices and storage media which contain data which is necessary for digital forensic processes. These are:
  - Consent
  - Search Warrant/Anton Pillar
  - Subpoena

Conclusion

- The digital forensic process, unless performed on data that has been obtained with the appropriate legal authorization, satisfies all of the element necessary for a contravention of Section 86(1) of the Electronic Communications and Transactions Act 25 of 2002.
- This could result in digital evidence obtained as a result of these digital forensic processes being ruled inadmissible, or even potentially worse, the digital forensic practitioners involved being prosecuted or litigated against.