{tag}

{/tag}

International Journal of Computer Applications

Volume 68 - Number 23

Year of Publication: 2013

Authors:

Jason Jordaan

10.5120/11722-7432

{bibtex}pxc3887432.bib{/bibtex}

Abstract

In most legal systems, it is crucial that evidence that is obtained for use in any judicial proceedings, especially criminal prosecutions, is obtained lawfully. In other words, no crimes should be committed in the obtaining and examining of any evidence, which will be later, be relied upon in court. Section 86 of the Electronic Communications and Transactions Act 25 of 2002 in South Africa creates a criminal offence of unauthorized access to data, which has a significant potential impact on the acquisition, examination, and analysis of digital evidence; in that traditional digital forensic processes, unless legally authorized, may potentially be in contravention of this law. The legal ramifications for both digital forensics practitioners and the cases that they are engaged on are identified, and appropriate legal solutions are provided to ensure that digital forensic practitioners do not contravene the existing legislation.

References

- Casey, E, (2004), Digital Evidence and Computer Crime, 2nd ed. London: Academic Press.
- Swanson, C R, Chamelin, N C, Territo, L, & Taylor, R W, (2006), Criminal Investigation, 9th ed. New York: McGraw-Hill.
- Peisert, S, Sishop, M, & Marzullo, K, (2008), "Computer Forensics in

Forensics," in Systematic Approaches to Digital Forensic Engineering, pp. 102-122.

- Van Der Merwe, D, Roos, A, Pistorius, T, & Eiselen, S, (2008), Information and Communications Technology Law. Durban: LexisNexis.
- Republic of South Africa, (2002), The Electronic Communications and Transactions Act 25 of 2002. Pretoria: Government Printer.
- Oxford University, (2002), Concise Oxford English Dictionary, 10th ed. , Judy Pearsall, Ed. Oxford: Oxford University Press.
- Oxford University, (2013), Oxford Dictionary of Law, 7th ed. , Jonathan Law and Elizabeth A Martin, Eds. Oxford: Oxford University Press.
- Vacca, J R, (2005), Computer Forensics: Computer Crime Scene Investigation, 2nd ed. Boston: Thomson.
- Solomon, M G, Barrett, D, & Broom, N, (2005,) Computer Forensics Jump Start. Alameda: Sybex.
- Jones, A & Valli, C, (2009,) Building a Digital Forensic Laboratory. Burlington: Syngress.
- McKemmish, R, (2008), "When is Digital Evidence Forensically Sound?," in Advances in Digital Forensics IV, Indrajit Ray and Sujeet Shenoi, Eds. Boston: Springer, pp. 3-15.
- Sansurooah, K, (2006), "Taxonomy of Computer Forensics Methodologies and Procedures for Digital Evidence Seizure," in Proceedings of the 4th Australian Digital Forensics Conference, Perth, pp. 67-77.
- Schwikkard, P J & Van Der Merwe, S E, (2002), Principles of Evidence. Cape Town: Juta.
- Republic of South Africa, (1996), The Constitution of the Republic of South Africa Act 108 of 1996. Pretoria: Government Printer, 1996.
- Joubert, C, (2001), Applied Law for Police Officials, 2nd ed. Lansdowne: Juta.

Index Terms

Computer Science Digital Forensics

Keywords

Digital forensics digital evidence legal liability authorization to access data admissibility of evidence.