© 2013 FIZ Karlsruhe

io-port 05971683

De Santis, Alfredo; Castiglione, Aniello; Cattaneo, Giuseppe; De Maio, Giancarlo; Ianulardo, Mario

Automated construction of a false digital alibi.

Tjoa, A Min (ed.) et al., Availability, reliability and security for business, enterprise and health information systems. IFIP WG 8.4/8.9 international cross domain conference and workshop, ARES 2011, Vienna, Austria, August 22–26, 2011. Proceedings. Berlin: Springer (ISBN 978-3-642-23299-2/pbk). Lecture Notes in Computer Science 6908, 359-373 (2011).

Summary: Recent legal cases have shown that digital evidence is becoming more widely used in court proceedings (by defense, accusation, public prosecutor, etc.). Digital tracks can be left on computers, phones, digital cameras as well as third party servers belonging to Internet Service Providers (ISPs), telephone providers and companies that provide services via Internet such as YouTube, Facebook and Gmail. This work highlights the possibility to set up a false digital alibi in a fully automatic way without any human intervention. A forensic investigation on the digital evidence produced cannot establish whether such traces have been produced through either human activity or by an automated tool. These considerations stress the difference between digital and physical – namely traditional – evidence. Essentially, digital evidence should be considered relevant only if supported by evidence collected using traditional investigation techniques. The results of this work should be considered by anyone involved in a Digital Forensics investigation, due to it demonstrating that court rulings should not be based only on digital evidence, with it always being correlated to additional information provided by the various disciplines of Forensics Sciences.

Keywords: digital evidence; digital investigation; digital forensics; anti-forensics; counter-forensics; false digital evidence; automated alibi; false alibi; digital alibi
doi:10.1007/978-3-642-23300-5_28