{tag} {/tag}
International Journal of Computer Applications
© 2013 by IJCA Journal
Volume 68 - Number 23
Year of Publication: 2013

Authors:
Veronica Schmitt

Jason Jordaan

10.5120/11723-7433
{bibtex}pxc3887433.bib{/bibtex}

Abstract

MD5 and SHA-1 cryptographic hash algorithms are a standard practice in digital forensics that is used in the preservation of digital evidence and ensuring the integrity of the digital evidence. Recent studies have shown that both MD5 and SHA-1 have vulnerabilities and collisions. Based on this, the use of MD5 and SHA-1 hash algorithms in the practice of digital forensics to preserve and ensure the integrity of digital evidence has been questioned in certain instances. Using experimentation, the researcher proves the validity of using either MD5 or SHA-1 hashing algorithms to ensure the integrity of seized digital evidence, from the moment of seizure of the evidence, through to eventual presentation and use of the evidence in court; thus demonstrating that the use of hashing remains a valid forensic methodology to ensure the integrity of digital evidence.

References

- Phillip, A. , Cowen, D. , & Davis, C. (2010). Hacking Exposed Computer Forensics Second Edition. New York: McGraw Hill.
- Thompson, E. (2005). MD5 Collisions and the Impact on Computer Forensics. Digital

Investigation (2), 36-40.

- Prosise, C. , & Mandia, K. (2003). Incident Response and Computer Forensics (2nd Edition). New York: McGraw Hill.
- Roussev, V. (2011). An Evaluation of Forensic Similarity Hashes. The Proceedings of the Eleventh Annual DFRWS Conference (pp. S34-S41). Elsevier.
- Wang, X. , & Yu, H. (2005). How to Break MD5 and other Hash Functions. Advances in Cryptology - EUROCRYPT 2005 (pp. 19-35). Berlin: Springer.
- Wang, X. , Yin, Y. L. , & Yu, H. (2005). Findings Collisions in the Full SHA-1. CRYPTO &apos;05 Proceedings of the 25th Annual International Conference on Advances in Cryptography (pp. 17-36). Berlin: Springer.
- Joubert, C. (2001). Applied Law for Police Officials (2nd Edition). Lansdowne: Juta.
- Casey, E. (2004). Digital Evidence and Computer Crime (2nd Edition). London: Academic Press.
- Carrier, B. (2005). File System Forensic Analysis. Upper Saddle River: Addison-Wesley.
- Solomon, M. G. , Barrett, D. , & Broom, N. (2005). Computer Forensics Jump Start. Alameda: Sybex.
- 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.
- Schwikkard, P. J. , & Van Der Merwe, S. E. (2002). Principles of Evidence. Cape Town: Juta.
- Saunders, M. , Lewis, P. , & Thornhill, A. (2009). Research Methods for Business Students (5th Edition). Essex: Prentice Hall.

Index Terms

Computer Science Security

Keywords

Digital forensics integrity of digital evidence hash collisions MD5 SHA-1 manipulation of digital evidence