Establishing the Validity of Md5 and Sha-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in These Algorithms

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

Investigation (2), 36-40.

Index Terms

Computer Science  Security

Keywords

Digital forensics  integrity of digital evidence  hash collisions  MD5  SHA-1  manipulation of digital evidence
Establishing the Validity of Md5 and Sha-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in These Algorithms