Uchenna P Daniel Ani et al., J Forensic Res 2015, 6:5
http://dx.doi.org/10.4172/2157-7145.C1.018

OMICS International
conferenceseries.com

4th International Conference on
Forensic Research & Technology
September 28-30, 2015 Atlanta, USA

Log integrity: A conceptual approach towards enhancing the integrity for log evidence

Uchenna P Daniel Ani[1], **Musa A Muhammad**[2] and **Nneka C Daniel**[3]
[1]Cranfield University, UK
[2]Masmob Electric and InfoSec Nigeria Limited, Nigeria
[3]Independent IT, UK

Evidence Integrity is the backbone of any digital forensic process and no doubt, information stored in logs is treasured sources of such evidence in forensic examination. Given the significance of maintaining audit trails and log information in aiding the proving and or disproving facts in any litigation, a digital forensic perspective underscores the need to secure and preserve adequately evidentiary log information for the purpose of admissibility. It should be understood that the admissibility of evidence solely depends on the reliability and wholeness of such evidence which defines its integrity. This theory ensures that evidence acquired during investigation is not tampered with or compromised consciously or unconsciously either by human actions, inactions, adoptive procedures or as a result of the tools used. Leaning on an understanding of existing integrity models and approaches, our work employs a suiting abstract digital forensic model for the development of '*Log integrity*'; a log-centered evidence preservation framework. The methodology adopts a three-phased integrity application technique that explored integrations with Clark-Wilson's Integrity model and Casey's Certainty Scale; all for assuring the integrity of log information as forensic evidence. We also elaborate on a validation approach explored using a test scenario which satisfactorily and within the scope of the study yields estimable results in terms of integrity preservation enhancement of log files. Therefore, besides the secure acquisition of digital evidence of great importance also is the task of ensuring that the integrity of such evidence is not compromised at any stage of the investigation.

Biography

Uchenna P Daniel Ani received his B.Tech (Hons) degree in Computer Science from the Federal University of Technology Yola, Nigeria in 2009 and MSc degree in Computer Security and Forensics from the University of Bedfordshire, Luton-England, United Kingdom in March 2012. He is a Lecturer with the Department of Computer Science, Federal University Lokoja; Nigeria. He has worked in various capacities in the industry as Systems and Network Administrator before joining the academics. He is also a member of several professional organizations like IEEE, IET, SDIWC and IAENG. He is a recipient of the Nigerian NITDEF for Scholarship into Master's degree study in the UK IN 2010. He is the recipient of the Most Outstanding Postgraduate Academic Achievement in Computer Science 2012 for excellent performance from University of Bedfordshire, United Kingdom. He is currently a PhD Research Fellow in Cyber-Secure Manufacturing and Information Intelligence at the Manufacturing Informatics Centre, School of Aerospace Transport and Manufacturing, Cranfield University, United Kingdom. His research interests are in Cyber Security, Digital Forensics, Virtualization, Computer and Network Security, Mobile Adhoc Networks and Performance Optimization.

u.p.ani@cranfield.ac.uk
masmob@yahoo.com
agbanusin@gmail.com

Notes: