Logintegrity: A conceptual approach towards enhancing the Integrity of log evidence

[1]Uchenna P. Daniel Ani, [2]Musa A. Muhammad, and [3]Nneka C. Daniel
[1]Researcher, Manufacturing Informatics Centre, SATM, Cranfield University, United Kingdom.
[2]Chief Information Officer, Masmob Electric and InfoSec Nigeria Limited, Nigeria.
[3]Independent IT/Risk Management Consultant, United Kingdom,

INTRODUCTION

Evidence Integrity is the backbone of any digital forensic process; and no doubt, information stored in logs are 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

OBJECTIVES

To present a conceptual methodology for the independent preservation of Integrity on log evidence.

RELATED WORKS

Audit logs refer to computing records and files that document program activities and events such as data manipulation, user access, error logs, security measures and Internet history. Any configured system or network accordingly should be capable of generating logs of events; which collectively form fundamental sources for the forensic investigation purposes, to ensure integrity. Such log documentations must be guaranteed not to be tampered with; from the time of registration to the presentation of the final report in a court Monteiro (2008). For the sake digital forensic procedures, log files serve as essential sources of information, which should be preserved; not only for reliability sake, but also for authenticity in enabling lawful prosecutions in court (Accorsi, 2009).

Propositional rules for handling evidential logs as evidence include that; Log files must be preserved in a way that guarantees they cannot be damaged, lost or modified, evidence must be obtained through the log files, and evidence must be prepared and documented with the original log files as well as media it was store in (Cesserini, 2001). When investigating on log files, the investigator must ensure that its Admissibility, Authenticity and reliability has been maintained throughout the examination.

In order to aid and guide the enhancement of integrity in systems and of the data within; that could be potentially be used as evidence, several models have been developed for the digital and forensic community. These include; Bell-la-Padulla, Biba Model, Brewer-Nash Model, Lipner Matrix Model, Goguen Model, Sutherland Model and Clark-Wilson model (Sonya, 2000; David, 2005; Nathan and Ishraq, 2004). Our work explores further the Clark-Wilson model, which emphasizes the concept of Constrained Data Items (High CDI) and Unconstrained Data Items (Low UDI). The model enforces integrity of digital data on the basis of two principles; the principle of well performed transactions and principle of separation of duties. These principles ensure that the original states of data are not altered intentionally or otherwise. Hence, this is the most preferable model used throughout this thesis because it contains rules that can be efficiently applied on digital evidence integrity.

METHODOLOGY

The model proposed is abstracted describes and explication of the preservation phase of the forensic evidence methodology (Mark, 2002). This methodology is particularly suitable for the log integrity enforcement considered. This phase principally explains the activities of ensuring that potential digital evidence; log files in our case are adequately secured and preserved from alteration.

Evidence Integrity Techniques

The techniques of evidence integrity consist of cyclic redundancy check, hashing, digital signatures, time stamp, and watermark.

Integrity Model

Clark-Wilson's integrity model comprises of several rules, procedures such as Transformation Procedures (TP), Integrity Verification Procedures (IVP), Constrained Data Items (CDI) and Unconstrained Data Items (UDI). There are also rules governing the integrity in Clark-Wilson Model, which includes C1, C2, C5, E1 and E4 that could be applied throughout the study. However, it should be noted that this study does adopt in its entirety, the Clark-Wilson's model, but just a part of it. The enforcement rules noted above do not apply to our study appropriately. The enforcement of validity, separation of duty, user identity and initiation do not conveniently fit into our study, thus have been excluded.

Transformation Procedure

This contains the processes that will take a system from one valid state to another, which could be applied to this project. These include; Imaging, Write-Protection, Hashing, and Extraction.

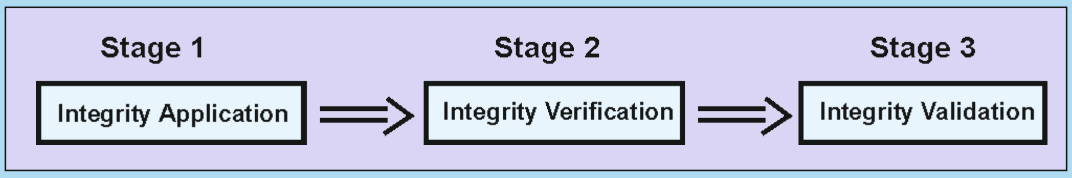
Integrity Verification Procedure (IVP)

These are the procedures that test the CDIs to conform integrity. The procedure here is a comparison where Hash value of the whole image is taken and preserved, same is also done to extracted logs. At the end of the investigation, the hashing procedures are repeated on same entities and a comparison is made of the initial and final fingerprints. The emergence of the slightest difference implies that alteration has occurred on the initial contents; which also implies that integrity had been compromised

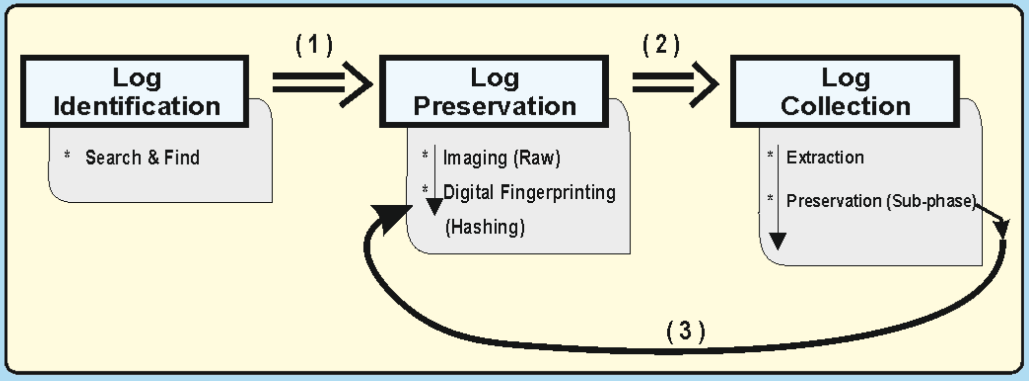
Constraint Data Item (CDI)

This contains data that are subject to integrity; it includes creation time, date when an event occurred and also the details of the computer used comprising the list of users.

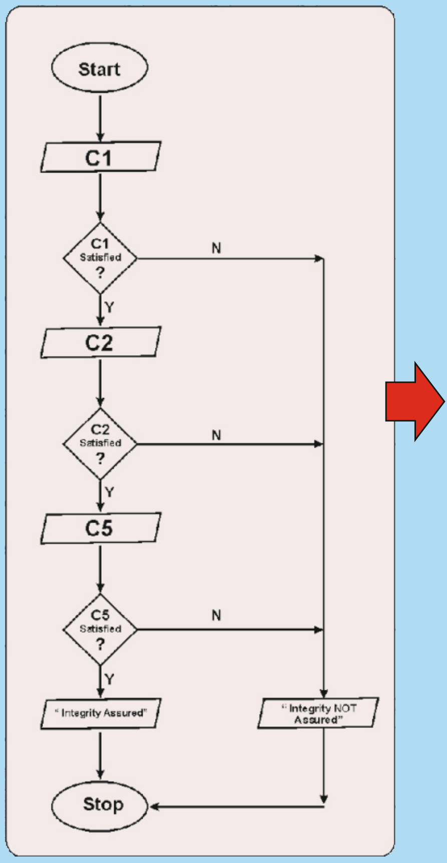
- **Creation time**: At this phase, a lookout will be made to identify the time when an event occurred on the system, which also infers when event-related logs are generated.
- **Log contents**: This implies checking the information about the computer
- **User**: This stage will involve identifying whether an authorized or unauthorized user got access to the system.
- **System used**: This phase will involve identifying the type of computer used and operating system installed and all other information about the system.


Stage 1
Integrity Application
Stage 2
Integrity Verification
Stage 3
Integrity Validation

Stage 1


(1)
(2)
(3)
Log Identification
* Search & Find
Log Preservation
* Imaging (Raw)
* Digital Fingerprinting (Hashing)
Log Collection
* Extraction
* Preservation (Sub-phase)

Stage 2


Start
C1
C1 Satisfied ?
N
Y
C2
C2 Satisfied ?
N
Y
C5
C5 Satisfied ?
N
Y
" Integrity Assured"
" Integrity NOT Assured"
Stop

Certainty Level	Description/Indicators	Commensurate Qualification
C0	Evidence contradicts known facts.	Erroneous / Incorrect
C1	Evidence is highly questionable.	Highly Uncertain
C2	Only one source of evidence that is not protected against tampering.	Somewhat uncertain
C3	The source(s) of evidence are more difficult to tamper with but there is not enough evidence to support a firm conclusion or there are unexplained inconsistencies in the available evidence.	Possible
C4	Evidence is protected against tampering or multiple, independent sources of evidence agree but evidence is not protected against tampering.	Probable
C5	Agreement of evidence from multiple, independent sources that are protected against tampering. However small uncertainties exist (e.g., temporal error, data loss).	Almost Certain
C6	The evidence is tamper proof and unquestionable.	Certain

Evidence Integrity with reference to log files remain a property that cannot and should not be traded for any other. Given that relevance is accorded to digital evidence based upon its level of correctness, completeness and reliability, which collective define its integrity. It must be noted that log file evidence can only retain its name as evidence if its integrity is assured. As a result, irrespective of the forensic investigation methodology adopted, Integrity-consciousness is a point that must remain ever green

References.

Accorsi, R., (2009). Log data as digital evidence: what secure logging protocols have to offer. 2009 33rd Annual IEEE international computer software and applications conference, 1(3), pp.398-403.

Cesserini, T (2001). Maintaining the forensics viability of log files", Global information Assurance Certification Paper [Online] Available at: http://www31.giac.org/paper/gsec/801/maintaining-forensic-viability-log-files/101724 [Accessed: 22 April 2015].

David, Elliot B. (2005). Looking back at Bell-La Padula Model. Reston VA. Available at: http://www.acsac.org/2005/papers/Bell.pdf [Accessed 14 February 2015].

Kawaguchi, N., Ueda, S., Obata, N., Miyaji, R., Kaneko, S., Shigeno, H. and Okada, K. (2004). A secure logging scheme for forensic computing, pp. 386–393.

Mark, R., Clint, C., Gregg G. (2002). An examination of digital forensic models. International journal of digital evidence. 1(3).

Monteiro S. and Erbacher, R. (2008). An authentication and validation mechanism for analyzing syslogs forensically. SIGOPS Oper. Syst. Rev, 42(3,), pp. 41–50.

Nathan, B., and Ishraq, T., (2004). *Biba Integrity Model*, Lecture Notes, [Online] Available at: http://www.google.co.uk/search?aq=f&sourceid=chrome&ie=UTF-8&q=Biba+Integrity+Model [Accessed 26 August 2014].

Sonya Q., (2000). "The Clark-Wilson security Model", Indiana University, Pennsylvania, [online] Available at: http://www.lib.iup.edu/comscisec/sanspapers/blake.htm [Accessed 22 December 2014].