Safeguarding Forensic Integrity of Virtual Environment Evidence

Uchenna Peter Daniel
Dept. Computer Science
Federal University Lokoja, Nigeria

Gregory Epiphaniou
Department of Computer Science and Technology,
University of Bedfordshire, UK.

ABSTRACT

Virtual machine technology has emerged with powerful features, offering several benefits and promising revolutionary outcomes. It is one technology that combines into one package several computing concepts like resource management, emulation, time-sharing, isolation and partitioning. These features have made evidence acquisition and preservation difficult and in some cases unfeasible. The aftermath is that conventional approaches to integrity preservation have not yielded the best results required to facilitate acceptability. Subjects around virtualization forensics, its affiliation with digital evidence integrity, and impacts on admissibility have been decisively examined. A part of this discourse dwelt on recognising potential threats to the integrity and reliability of evidence from a virtual environment; specifically using VMware Virtual Machine Monitor as a case study. A theoretical framework for preserving the integrity of digital evidence from such environments is introduced. This structure highlights guidelines, processes and parameters essential for keeping the accuracy, consistency and trustworthiness of digital evidence, made possible via abstractions from eminent integrity principles of well-formed transactions and separation of duties as proposed by Clark and Wilson. Key parameters in the model include; strength of hash functions, number of evidence attributes, and number of evidence cycle covered; all represented conceptually in a mathematical model. This is further consolidated with the introduction of an integrity rating factor/threshold and the definition of an integrity enforcement process in line with globally recommended standards. While still working on practical demonstration of the proposed model, the work done so far is seen to open a path for unification and amplification of trust levels required for the admissibility of virtual environment evidence.

General Terms

Computer Forensics, Digital Forensics, Virtual Forensics.

Keywords

Evidential Integrity, Virtualisation Machine Forensics, Evidence Reliability, VMware evidence, Integrity Preservation

1. INTRODUCTION

Years back in the world of investigations, unravelling crimes was a somewhat easy task that involved the pursuit of laid-down rules and procedures. Why was it so? This was because crimes and their facets took just physical dimensions. Managing prohibited acts required nearly only possible with the physical and instantaneous involvement and presence of a human entities. Investigations of crimes and the act of discerning plausible evidence and proving culpability were relatively strict and straight-forward. Then came the era of technological revolution, computerization and digitalization; these became the order of the world and human endeavours and activities took a leap from physical to digital (electronic) environments; the world had turned into a global village. Information and Communication Technology had emerged, making interactions spontaneous and more interesting that it ever was. Every facet of human endeavour obtained its fair share of the explosion; and it was 'welcome to the digital age'. From then on, information technology has continued to release benefits, bridging divides, proffering solutions, while generating new problems.

Today, the digital age is on the fastest speed lane with ever more information being generated and transformed via systems and processes [1] and [2]. These transformations have also left their marks on crime and forensic science; the act of investigations. With the proliferation of digital devices and digital environments, the potential for obtaining crime information in digital formats is high; hence experts and investigators are called on to awaken from this erstwhile staid movement, hence to ensure that appropriate skills and measures are adopted to meet the growing change. However, technologies keep emerging and each instance introduces new dimensions to issues that cannot be ignored.

Virtualization is one such technology that has unravelled powerful features, offering several benefits and promising revolutionary outcomes. It is one technology that has combined in one package several computing concepts like resource management, emulation, time-sharing, isolation and partitioning [3]. Virtualization comes as a lighter alternative to the likes of green computing [4] with cost-effective solutions relative to management of multiple operating platforms and complexities in disaster recovery and business continuity [5]. Salient capabilities of this technology include mobility, roll-backs, restarts, remote replications, time and hardware reductions for the completion of repetitive tasks on multiple physical (host) machines, not excluding a means for the exploitation of multi-socket and multi-core systems [6].

No surprise at its rising adoption in the world of IT. No right thinking business and service-oriented organization would ignore such delectable prospects and IT potentials; there is hardly a field of computing for which virtualization has not offered improvement, which results in for its wide acceptance and utilization as a low-cost, service-oriented technology. Gartner Inc. report that fewer than five million computers were 'virtualised' in 2006. The same source maintained that in 2009, 18% of server workloads ran on 'virtualised' servers and growth was estimated to reach 28% in 2010 and 50% in 2012. The hosted virtual desktop market worldwide was projected to reach about 49 million units by 2013, accelerating from the 500,000 units recorded in 2009 [7] and [8] in [9].

Again the question 'why the startling numbers, why the geometric upswing?' Possible answers could be tied to the purported open benefits accrued with adopting the technology; most particularly the cost. Virtualization presents a platform that requires minimum support by making light the activities of maintenance and testing. With the client architecture, multiple operating environments permit applications support services for the client machine. And as earlier noted, the gains are seen in the decrease in cost for system upgrades and uniformity in desktop environment [9]. Virtualization has similarly seen extensions to mobile devices and thrives so well in that architecture that estimations were that by 2012 more than half of all new smart phones will include hardware virtualization support.

Conversely, virtualization has also yielded problems that cannot be ignored, especially in the fields of crime, computer and (or) digital forensics. So should eye-brows be raised? Why? The response comes affirmative; also because while computing experts are leveraging the power of virtualization for their legitimate gainful purposes, malicious users have also hewed their way exploring the same virtualization might for their illegitimately rewarding ends. What was good for the goose has come even better for the gander. We see current trends in digital forensics revealing that the applications of virtualization tools, the challenges these pose to digital investigations and the admissibility of consequential evidence are dealing obfuscation to traditional forensic approaches [10]. Several resistances have been laid bare in the handling of digital evidence relative to virtualized environments which has not been the case with physical (host) machines. For instance, most digital applications treat unrecognised virtual machine files as unknown file types, making it difficult if not impossible to discover potential virtual machine related files or evidence. Virtual machine states can be altered through exportation or loading into other virtual machines; justifying any eventual questions of integrity. Besides, a virtual machine resident inside a forensic image can only be examined properly by a forensic application if such an application is able to interpret the file extensions [9], and not many such applications are readily available.

From a technical point of view, the terms versioning, isolations and encapsulation are key features of virtual environments (machines) that retain strict anti-forensic potentials [11] and [4]. The versioning feature unveils the capacity to revert back to an untainted copy, called a snapshot, of a system after any computer misdeed. Isolation enables orthogonal privilege that spontaneously fixes access control power to a virtual machine owner devoid of interference by the physical machine or any external entity (hardware or operating system). Encapsulation allows for flexibility of virtual machine movements, deletions and (or) destruction [12].

So again the question goes, 'Any need for raised brows'? Emphatically, YES. Firstly, because of the lack of and need for well-ordered knowledge on the functions, features and forensic applications of virtual machines, the documentary procedures that could aid successful handling and(or) preservation of virtual machine evidence [13], and capable tools (software and hardware) that could be used to implement the procedures. The brows of digital forensic experts and investigators must rise to the reality that the entity that form the nucleus of digital forensics is being jeopardised. As it is, virtualisation is dealing powerful blows to the flexibility of access to, and the integrity of digital evidence. A swift and all-responsive attitude is necessary to the study, acquisition, analysis and preservation of virtual machine evidence for admissibility [14].

2. DIGITAL FORENSICS AND VIRTUALIZATION

The objective of any forensic process has always been to discover and establish evidence. It is only reasonable to suppose that if a crime happens within a digital environment, much of the required evidence of such a crime cannot be found outside that same environment. However, digital evidence and environments have been noted to be volatile and could be effortlessly compromised by poor or unknowledgeable handling. The chances of successful prosecution are greatly dependent on the availability of 'strong' or 'complete' evidence, the absence of which precipitates failed civil litigations [15], yielding financial losses and reputational damage. Thus, digital evidence is described as an interpretation of data, either at rest (in storage) or on transit (network communication) or the combination of both [16]. It is worth noting that, the true value of digital evidence is in its interpretation as information [16]. It is such interpretation that determines whether such evidence could be regarded as 'strong', 'complete' or otherwise something that aids acceptance in court.

What then is strong or complete evidence? First is the submission that digital evidence must possess all the attributes of other types of admissible evidence, and every evidence presented in court has to satisfy tests of admissibility and weight [15]. The test of admissibility and weight puts upon the court the tasks of considering and determining the assurance(s) and the extent to which what is presented represents the true nature of the idea portrayed. Then through severe legal scrutiny and reference to similar known antecedences, the court resolves the relevance and acceptability of such evidence. Hence, only when evidence satisfies both tests, is it likely to be referred to as '*strong*' or '*complete*'. Since the true value of evidence lies in its interpretation, and such interpretation is dependent and made out from relative attributes therein, the submission is that better interpretation could be obtained with several expository attributes in evidence rather than less. Technically, '*strong*' or '*complete*' evidence retains answers to the questions of 'what', 'where', 'when', 'who' and 'how'. Each of these tell different, partial stories about the same evidence; stories that can be combined to make one better story; a story about the integrity of the evidence. This is what makes for 'complete' evidence.

2.1 Digital Integrity

Digital integrity is defined as "the property whereby digital data has not been altered in an unauthorised manner since the time it was created, transmitted, or stored by an authorised source" [17] in [18]. Again, a reminder that digital evidence must be able to sustain or disprove a hypothesis [19] while emphasizing integrity. This condition is much desirable and unavoidable in any or very digital forensic process since an evidence can scarcely enjoy court acceptance if it is considered devoid of resounding level of integrity. Hence, integral to the duties of a forensic expert is the task of substantiating the integrity of any digital evidence [11]. So notwithstanding the environment or architectural build or

setup of any alleged crime scene, digital evidence identified must be acquired and preserved accordingly.

2.2 Virtualization

Virtualization revolves around the concept of having a logical machine that runs programs in a fashion analogous to physical machines or real computers [5]. It is a complex setup of software that enables the creation and running of multiple, self-regulating working environments that produce (logically) independent sets of hardware and software entities [20]. Given this description, virtualization via the virtual machine approach is able to replicate the typical workings of any known client or remote computer, and in more complex form, the usual job-sharing features in large-scale mainframes. Virtual machines have been described as efficient, isolated replicas of real machines [21].

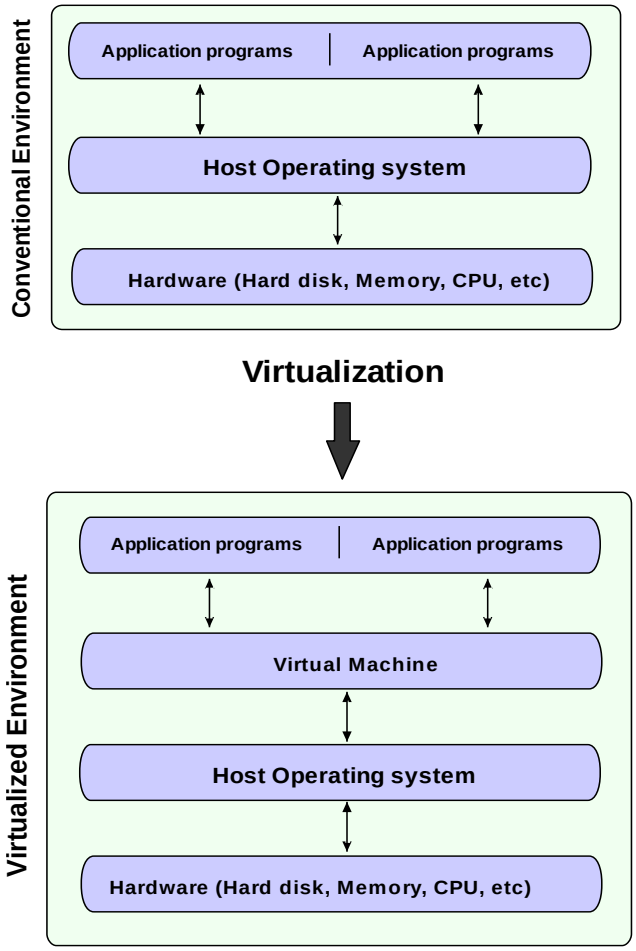

Figure 1: Virtualization Concept: A schematic diagram [12]

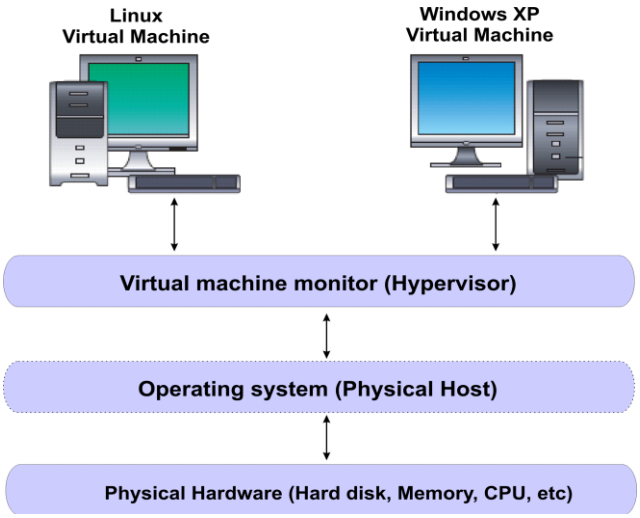

Figure 2: A Generic System Configuration for Virtualization [16]

The generic view of virtualization, as indicated in figure 2, gives a better understanding of the concept. Physical hardware (hard disk, memory, CPU etc.) are beneath the chain of abstraction bearing conventional operating systems (optional), a virtual machine monitor (VMM) or hypervisor and a virtual machine in that order. Conventional computing system setups are altered with the introduction of hypervisors that manage instances of other operating systems. This they achieve by enabling the creation of independent partitions for software services, and trapping and routing of hardware requests among hardware partitions [22] and [21]. This of course is where the problems are situated.

First are critical questions about integrity. How can it be preserved regardless of virtualization capabilities? Is the stored data changed in any way? Is it possible to reconstruct the original state of an image or the evidence it harbours with proofs of non-alteration? In the absence of trustworthy answers from which a decision basis can be derived, the whole investigative process may have limited value since corresponding evidence is likely not to see the light of admissibility [23]. Secondly, given the volatility of digital evidence, and the intricacies of ensuring evidential integrity, it has become more imperative that evidence resident and (or) linked to virtual machines be carefully and skilfully approached and preserved. As always, we may ask why? Because fully-fledged computing environments are now being carried on portable storage devices with the ability to wipe out program activity traces after being utilised. As simple as it is; the act of turning 'off' or 'on' of a virtual machine or its host machine is capable of doing the worst damage to integrity. It is conceivable to overwrite incriminating records after the illicit deeds have been done, many thanks to counter-forensics [24]. Then comes the likelihood of inappropriate application of tools and procedures; propelled by inadequate understanding of architectural layout and operations of a target system [11]. Integrity takes all the blows, and belated response to these could yield undesirable phenomena characterised by wrong or unjust acquittals, or false prosecutions [25].

3 IM(PROVING) INTEGRITY: RELATED WORKS

Several authors and researchers have made suggestion on how integrity could be best maintained. Specifically, there has been wide acceptance of the use and application of checksums for preserving integrity of digital data and (or) evidence. It justifies investigators' ability to verify disk, image or file integrity using cryptographic hash functions [26]. This popular sign-on to the use of hash functions has been sustained by Vaughan-Nichols while evaluating applicable security algorithms adoptable for implementing evidence integrity. His result showed that a combination of Digital Signatures and Secure Hash Algorithm (SHA) proved best for shielding data from alteration or contamination [27]. Digital signatures with SHA-512 prevailed over rival options like Message Digest 5 (MD5), Cyclic Redundancy Check (CRC). The upsides include faster computation, least vulnerability, scalability, higher resistance to collision and higher accuracy towards integrity [27]. This means safeguarding integrity has been acknowledged by several researchers. No doubt, the power of hash functions, independently or jointly with other schemes, for protection of any digital evidence from contamination remains incontestable.

One adoptable technique towards guaranteeing integrity with relation to volatile evidence in the Windows platform included the utilization of the in-built memory dump utility (Microsoft Windows Hibernation), the creation of a bit image, and subsequent analysis of such acquired bit-image using CERT's *LiveView* image analysis utility in a virtual machine [25]. This process of image mounting and booting allowed for the efficient acquisition of an interactive user-level access and perspective of the operating environment with modifications to the underlying image or contents therein. Only read-only access is acquired [28].

Other authors have emphasized that a valid and well-documented chain of custody encompassing evidential details about 'what, who, where, when and how' is essential towards affirming integrity and acceptance of digital evidence in court; this concept was put forward in the Digital Evidence Management Framework (DEMF). The DEMF proposal saw the integration of several technologies such as biometrics, timestamps from a Secured (Trusted) Third Party (Timestamp Authority) [13], Global Positioning System *(*GPS) coordinated web services/Radio-frequency Identification (*RFID*) devices as specified in the World Wide Web Consortium's (W3C's) Draft Specification 2011 [29], and asymmetric technique hash functions [14].

However, it has been argued that aside from preserving the integrity of digital evidence, it is also pertinent to define confidence on any purported integrity. This idea was expressed in a model called Forensic Evidence Management System (FEMS) [30] that adopted Biba's Integrity model [31] as an evidence integrity preservation technique, and Casey's Certainty scale [32] as the evidence integrity assurance technique with Finite State Automata (FSA) as handling the reasoning behaviour [30].

4 VIRTUAL MACHINE EVIDENCE RELIABILITY MODEL (VMERM)

Evidently new evidence integrity issues have surfaced with the emergence of virtual machines. The validity, totality and reliability of evidence within such environments raise questions in the face of powerful, unavoidable virtual machine attributes like isolation and encapsulation. Thus, it is suggested that the integrity of the environment precedes and is as important as the integrity of the evidence contents. To model a solution, ideas need to be taken from the concept of collision resistance for determining the strength of hash functions, the level and number of abstraction in virtual machine architecture and the number of attributes of evidence contents. Previous models have dwelt much on integrity of evidence within traditional (physical) operating environments, which does not offer appropriate solutions to our context. Hence, the novelty of this work relies on the trend and emergent diversion to virtual machines with little attention to their potential forensic implications.

Virtualisation has revealed segmented levels of abstraction which should be leveraged for success. We thus propose a Virtual Machine Evidence Reliability Model (VMERM) that emphasizes the levels of assurance that can be attributed to the integrity of virtual environment evidence. This scheme leans on the concept of an 'evidence cycle' [14], which defines an

iterative procedure for attaining absolute evidence from virtual machines.

As noted earlier, virtual machines typically retain resultant traces in their host hypervisors, and the hypervisors do same in their host machines. We submit that evidence treated as absolute should involve such established links (traces) between virtual machines, their core hypervisors and host machines (operating systems and physical hardware). These informative links reveal independent abstractions which when integrated defines an 'evidence cycle' yielding a chain of proof that requires integrity preservation emphasis.

4.1 Model Concept and Components

To model assurance levels, a reliability rating factor as noted earlier is presented which outlines integrity planes with respect to the strength of the hash function, evidence cycle and number of evidence attributes [14]. This is further consolidated by the adoption of Clark-Wilson's principles of well-formed transactions and separation of duties. The principle of well-formed transaction emphasizes that, "in a transaction, a user is unable to manipulate data arbitrarily, unless in constrained ways that preserve or ensure the integrity of the data"; while that of separation of duties underscores that, "nobody should perform a task from beginning to end; nevertheless that task should be divided among the two or more people to prevent fraud by one person acting alone" [33]. In the bid to uphold these values, our model adopts the techniques of strengthened hash function, trusted timestamp and digital signatures as plausible, constrained ways of preserving data integrity. It also introduces the theory of trio entities (User/Investigating Party, Trusted Third Party, and Validation Party), all with disparate duties that jointly ensure integrity.

4.1.1 Strength of Hash Function

The strength of the hash function as adopted in this integrity model follows benchmarks recommended by NIST [34]. The National Institute of Standards and Technology (NIST) recommendations emphasize the concept of collision resistance; a measure of the extent of work needed to find a collision for a cryptographic hash function with "elevated" likelihood, which is emphasized by the computational infeasibility of obtaining two incongruent inputs (evidence) $x, x', and\ x \neq x',\ with\ h(x) = h(x')$ [35]. This is projected as half the length of the hash value, *L*, generated by the corresponding hash function, which is *L/2* bits [36]. SHA-256 for instance produces a full length hash of 256 bits, yielding an estimated collision resistance of 128 bits. This implies the more sophisticated the strength of the hash function, the higher the integrity level, and the more trustworthy and satisfactory the evidence [14]. Table 1 summarises our exemplar approved hash values, while Table 2 presents defining security strengths.

Table 1: Collision Resistance of Hash Functions

ALGORITHM	**SHA-2**				**SHA-1**
Hash Function / Variant	**SHA-512**	**SHA-384**	**SHA-256**	**SHA-224**	**SHA-1**
Length of Hash Value Generated in bits	512	384	256	224	160
Collision Resistance Strength in bits	256	192	128	112	< 80

Table 2: Strength of Hash Function

ALGORITHM	**SHA-2**				**SHA-1**
Hash Function / Variant	**SHA-512**	**SHA-384**	**SHA-256**	**SHA-224**	**SHA-1**
Collision Resistance Strength in bits	256	192	128	112	< 80
Defined Security Strength	5	4	3	2	1

4.1.2 Number of Evidence Attributes

Evidence Attributes are conclusive properties that consciously describe evidence. Number delineates a summative value that indicates all such attributes making up a single piece of evidence. it should be noted that there is some likelihood that evidence might not retain all possible attributes, enough to qualify it as 'complete' and 'absolute', due to strict situations like resistive forensics; as seen in the case of virtualization. Thus, it is reasonable to suggest that a variation in the number of evidence attributes could precipitate variations in the integrity levels and evidential burden ascribable to such evidence. Hence, it adds weight to presenting digital evidence as encompassing multiple linked attributes rather than a single one. This informed the incorporation of multiple attributes (Hash Value, Geo-location Data, Trusted Timestamp, and Digital Signature) for evidence in the model presented. The model proposes higher priority status to Hash Function introducing a reliability rating factor, Reliability Rating Factor (R_i). R_i takes the value of 1 for any evidence that incorporates hash and any one of the other attributes, 2 for any that incorporates hash and any two of the other attributes, and 3 for any that incorporates hash and all three of the other attributes. By this, the model assumes a minimum level of integrity for the evidence acquired from a virtualised environment.

4.1.3 *Evidence Cycle*

The evidence cycle property asserts that evidence emanating from a virtual machine must possess four integral elements in line with typical virtualisation architecture, where four abstraction layers exist; the virtual machine layer, the hypervisor layer, the host-operating system layer, and the hardware layer. For instance, having evidence that shows the discovery and linkage of either or all of VMware hypervisor signatures; *.vmsd, .vmx, .vmdk, .vmem, .vmsn, .nvram, .vmss, .vmtm, .vmxf, .vswp,* and *.log files* [4], to a known Logged/Account user, Operating System and Hard Drive, gives greater confidence on the potential inference that a higher cycle of proof exists than when such linking evidence is non-existent. Figure 3 shows the process cycle diagram.

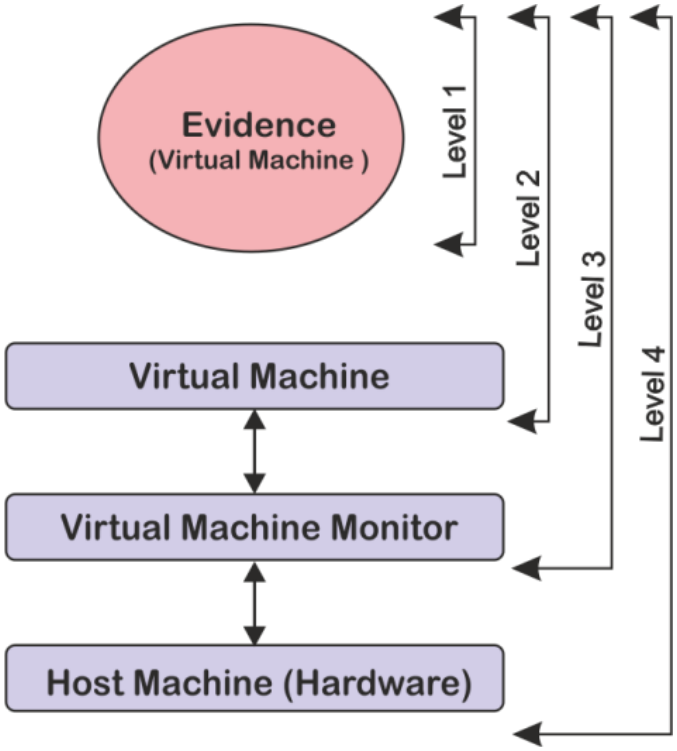

Figure 3: Evidence Process Cycle

4.1.4 *Mathematical Representation*

Given the above, we reaffirm the inter-factor relationship for facilitating evidence accuracy, reliability and completeness as mathematically modelled in [14]; the integrity of virtual environment evidence is dependent on the inter-factor relationship amongst three factors; the strength of hash function, the number of evidence attributes incorporated into the evidence, and the number of evidence cycles covered. Therein, an evidence integrity rating factor is established from which probable inferences can be drawn on the level of reliability ascribable to a given piece of evidence. The mathematical representation is shown:

$$\boldsymbol{I_v = h_i * N_j * C_k} \qquad (1)$$

Where;

h_i represents the *strength of the hash function*, with i = 1 to 5; implying, the comparative bound that relates to any expected strength level of hash function. The strength level, and safety assurance against oppositional tampering is proportional to the value obtained. N_j represents the *number of related attributes* combined into an item of evidence with their corresponding dependability classification. At this point, the more the evidence attributes combined, the more acceptable the evidence for admissibility. And C_k signifies *evidence cycle covered*, maintaining consistency with our idea *"Complete evidence"* encompassing four (4) cycles (with k = 1 to 4, defining cycle transitions achievable by evidence).

We therefore present an integrity enforcement process relative to digital evidence preservation from the virtual environment perspective.

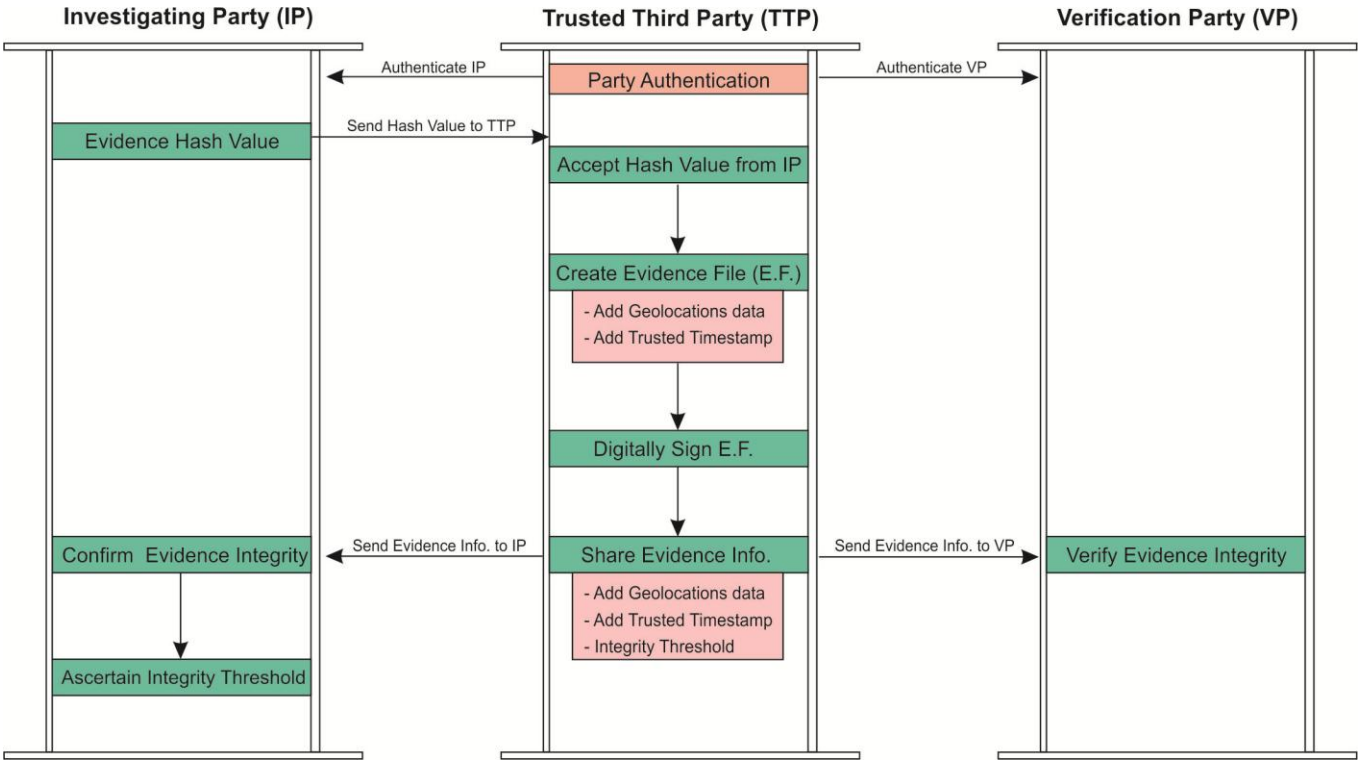

Figure 4: Integrity Enforcement Process

As seen in figure 5, sustaining integrity would involve the adoption and adherence to well-formed procedures that are considered integrity-responsive. By way of emphasizing Clark-Wilson's principles of separation of duties, our integrity enforcement process shows collaboration of three entities; Investigating Party, Trusted Third Party, and Verification Party, whose disparate duties co-jointly reinforce the integrity of any eventual evidence; since the process of managing integrity must not be handled by a single party from start to finish. The Investigating Party is typically the first handler of purported evidence from which a fingerprint is generated and sent to the Trusted Third Party (TTP). The TTP's duties start with initial receipt of an evidence fingerprint from a trusted and authenticated client. The TTP then creates an evidence file whose contents include the collected fingerprint, geo-locations data of the sending party, and a timestamp generated from a trusted, universally-accepted time source. The TTP then digitally signs the new Evidence File (EF) with its private key. The signed document is then released (shared) to all requesting parties holding a public verification/confirmation key. At the receipt and confirmation of a signed evidence file, an investigating party is thus able to determine and disclose an integrity rating factor/factor/threshold covered by the evidence, in line with the initially presented integrity factor/factor/threshold. This could also be verified by the Verification Party. We suggest for any evidence to be considered valid, specific processes must be handled independently by the entity designated with such authorisation, else should be considered invalid. Thus, initial evidence content remains known only to an investigating party which is subject to verification by other parties. The task of consolidating integrity and reliability is managed by an independent trusted third party. This too is verifiable by other parties. The verification party is not able to alter, but may ascertain the correctness or otherwise of any integrity assertion tendered by any other party. With this, important principles of evidence origin authentication, non-repudiation and ultimately, evidence integrity are assured. Thus, with few queries, decisions may be informed.

At this point it is important to emphasize that all duties assigned the various parties need to be strictly adhered to for the framework to be valid. Any change or transfer of duties outside that which is already laid is considered not in line with the framework's objective, and might be considered an irregularity that could jeopardise the integrity of the evidence in question. The cogency of this model appraoch to integrity is also tied to the basic assumptions that; no integrity level is assumed before model adoption,while minimum level is assumed after model adoption. It is also assumed that the User/Investigator retains an adeqaute understanding of the features and functions of the hypervisor and its file system. By this, A reliability rating factor R_i is introduced to better conceptualise integrity levels. This is shown in table 3.

Table 3: Reliability Rating Factor

Reliability Rating Factor (R_i)	Description
i = 1	Hash Value + Any 1 of [Timestamp, Geolocations Data, Digital Certificate]
i = 2	Hash Value + Any 2 of [Timestamp, Geolocations Data, Digital Certificate]
i = 3	Hash Value + All 3 of [Timestamp, Geolocations Data, Digital Certificate]

In this particular concept, the model assumes at least a minimum level of integrity for the evidence acquired within a virtualised environment. This minimum factor/threshold translates to R_i=1, where at least one hashing and one other attribute are assured. R_i can thus take a combination of either of two attributes, three attributes or four attributes; all depending on the investigator's ability to produce the required attributes. This implies the investigator's ability to generated acceptable hash value, valid timestamp, digital certificate, and geo-location data relative to the evidence. The more evidence attributes achieved, the higher the reliability rating attributed.

Our concept towards integrity gains root from existing techniques and frameworks, starting from traditional computing environments to contemporary virtual computing platforms. New evidence integrity enhancement attributes like geolocation data and digital signatures are introduced, along with an integrity rating factor/threshold that calibrates levels of veracity of and evidence stemming from a virtual machine environment. These conjointly offer enhancements to evidential integrity as related to virtual platforms and in comparison to existing models. With elevated assurance, value is added to evidence since proofs can be made about intractability to alterations, non-repudiation of origin and time, and strong auditability.

5 CONCLUSION AND FUTURE WORK

This discourse brings to light the problems of managing evidential integrity of digital evidence emerging from virtual machine environments. It is not enough that decisions be inferred from digital evidence, but such decisions must be made on solid and trustworthy evidence for justice to be served. The only prerequisite for this is that such evidence must be proven to be integrity-enabled. Given the difficulties of attaining this quality, especially within virtual environments, we propose a Virtual Machine Evidence Reliability Model (VMERM) that introduces novelty in the aspect of guaranteeing evidential assurance in a virtual machine environment.

It is recommended that existing and newer forensic applications be updated to include virtual platform signatures and file systems; to enable easy and efficient virtual forensic investigations. The framework presented assumes a conceptual base since fully-fledged industrial demonstration has not yet been carried out; however, this forms the basis for future work especially with application to real life scenarios. Conceivably, an automated system could be implemented to combine the processes outlined in the framework to enhance accuracy and timeliness. Future work would also see the incorporation of SHA-3 (Secure Hash Algorithm 3) also referred to as Keccak as potentially way of improving the strength of hash function; subsequently improving evidence integrity, given its pronouncement as the potential credible ready-to-use replacement for SHA-2 in the event of compromise The framework presented could also be reviewed in the light of its applicability to other virtual machine vendor applications. The benefits of adopting this framework are anticipated to prevail over known constraints, thus the likelihood of assuming a de facto position.

6 REFERENCES

[1] IBM, "Accelerating an information-led transformation with IBM System z," IBM Systems and Technology Group, New York, White Paper 2010.

[2] Mike Duren and Chet Hosmer, "Can Digital Evidence Endure the Test of Time?," in *Digital Forensics Research Workshop*, New York, 2002.

[3] Fotis Tsifountidis, "Virtualization Security: Virtua Machine Monitoring and Introspection," Surrey, England, 2011.

[4] Brett Shavers, "Virtual Forensics: A Discussion of Virtual Machines Related to Forensic Analysis," 2008.

[5] Diane Barrett and Greg Kipper, *Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments [eBook - PDF]*, electronic ed. Burlington, USA: Elsevier Inc., 2010.

[6] Brian Hay and Kara Nance, "Forensics Examination of Volatile System Data Using Virtual Introspection," Fairbanks, 2009.

[7] A Jump and B Gammage, "Emerging Technology Analysis: Hosted Virtual Desktops," Gartner Inc., White Paper G00164950, 2009.

[8] Ellen Messmer. (2009, October) Gartner: Server virtualization now at 18% of server workload. [Online]. http://www.cio.com/article/505444/

[9] Diane Barrett, "Forensic Challenges in Virtualised Environments," University of Advancing Technology, White Paper 2011.

[10] Christiaan Beek, "Virtual Forensics," Ten ICT Professionals, Paper n.d.

[11] Dave Oswald. (2007, January) Forensic Restitution. [Online]. http:/www.restitution.co.za

[12] Ben Pfaff, Tal Garfinkel, and Mendel Rosenblum, "Virtualization Aware File System: Getting Beyond the

Limitations of Virtual Disks," Department of Computer Science, Stanford University, California, 2006.

[13] Jamin Cosic and Miroslav Baca, "Do We Have Full Control Over Integrity in Digital Evidence Life Cycle?," in *ITI 2010 32nd International Conference on Information Technology Interfaces (ITI).*, Cavtat, 2010, pp. 429-434.

[14] Uchenna Peter A Daniel, Gregory Epiphaniou, and Tim French, "A Novel Evidence Integrity Preservation Framework for Virtualised Environments: A Digital Forensic Approach ," in *Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensics (CyberSec2013)*, Kaula Lampur, 2013, pp. 97-106.

[15] Peter Sommer, "Digital Evidence, Digitak Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers," Information Security Guide 2012.

[16] Bradley Schatz, "Digital Evidence: Representation and Assurance," Queensland University of Technology, Queensland, PhD Thesis 2007.

[17] S Vanstone, P Van Oorschot, and A Menezes, *Handbook of Applied Cryptography*.: CRC Press, 1997.

[18] Chet Hosmer, "Proving the Integrity of Digital Evidence with Time," *International Journal of Digital Evidence*, vol. I, no. 1, pp. 1-7, 2002.

[19] Christopher James Hargreaves, "Assessing the Reliability of Digital Evidence from Live Investigations involving encryption.," UK, 2009.

[20] Derek Bem and Ewa Huebner, "Computer Forensic Analysis in a Virtual Environment," *International Journal of Digital Evidence*, vol. VI, no. 2, pp. 1-13, 2007.

[21] Uchenna Peter Daniel, "A Framework for Evidence Integrity Preservation in Virtualized Environment: A Digital Forensic Approach.," London, MSc. Thesis 2012.

[22] Patty Bates, "The Rising Impact of Virtual Machine Hypervisor Technology on Digital Forensics Investigation," *Information Systems Audit and Control Association.*, vol. 6, pp. 47-50, 2009.

[23] Chris Reed, "The Admissibility and Authentication of Computer Evidence - A Confusion of Issues," in *5th BILETA Conference of British and Irish Legal Technology Association*, 2005, pp. 1-9.

[24] Simson Garfinkel, "Anti-Forensics: Techniques, Detection and Countermeasures," in *2nd International. Conference on i-. Warfare and Security*, Califonia, USA, 2007, pp. 77-84.

[25] Sasa Mrdovic, Alvin Huseinovic, and Ernedin Zajko, "Combining Static and Live Digital Forensic Analysis in Virtual Environment," in *XXII International Symposium on Information, Communication and Automation Technologies 2009 (ICAT 2009).*, 2009, pp. 1-6.

[26] B Carrier and E H Spafford, "Getting Physical with the Digital Investigation Process," *Digital Evidence*, vol. 2, no. 2, 2003.

[27] J S Vaughan-Nichols, "Virtualization Sparks Security Concerns," *Computer*, vol. 41, no. 8, pp. 13 - 15, August 2008.

[28] Matt Healey, Cushing Anderson, and John Humphreys, "IDC: Analyze the future," Massachusetts, IBM Virtualization Services 2008.

[29] W3C. (2011, Junw) A W3C Organization Website: Geolocation API Specification. [Online]. http://dev.w3.org/geo/api/spec-source.html

[30] Kweku K Arthur, Martin S Olivier, Hein S Venter, and Jan H.P. Eloff, "Considerations Towards a Cyber Crime Profiling System," in *Third International Conference on Availability, Reliability and Security,2008 (ARES 08)*, 2008, pp. 1388-1393.

[31] C P Pfleeger and S L Pfleeger, *Security in Computing*, 3rd ed.: Prentice Hall, 2003.

[32] E Casey, "Digital Evidence maps - A sign of times," *Digital Investigation, Elsevier*, pp. 1-2, 2007.

[33] Sonya Q Blake. (2000, May) The Clark-Wilson Security Model. Document.

[34] FIPS PUB 180-3 NIST, "Secure Hash Standard (SHS)," Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, Technology Standard 2008.

[35] Dieter Gollmann, "Computer Security," in *Computer Security*. West Sussex: John Wiley and Sons, Ltd, 2011, p. 258.

[36] Quynh Dang. (2011, September) Recommendation for Applications using approved hash algorithms. [Online]. csrc.nist.gov/publications/./800-107/Draft_Revised_SP800-107.pdf

[37] Jasmin Cosic and Miroslav Baca, "(Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp," in *MIPRO, 2010 Proceedings of the 23rd International Convention*, 2010, pp. 1226-1230.

[38] S Saleem, O Popov, and R Dahman, "Evaluation of security methods for ensuring the integrity of digital evidence," in *2011 International Conference on Innovations in Information Technology (IIT)*, 2011, pp. 220 - 225.

[39] Brian D Carrier and Eugene H Spafford. (2004) An Event-Based Digital Forensic Investigation Framework.

[40] J S Vaughan-Nichols, "Virtualization Sparks Security Concerns," *Computer*, vol. 41, no. 8, pp. 13-14, 2008.

[41] Matt Healey, Cushing Anderson, and John Humphreys, "IDC: Analyze the Future," Massachusetts, IBM Virtualization Services 2008.

[42] R Rogers and K Seigfried, "The Future of computer forensics: A needs analysis survey," *Computers and Security*, vol. 23, no. 1, pp. 12-16, February 2004.

[43] Richard Boddington, Valerie Hobbs, and Graham Mann, "Validating digital evidence for legal argument," in *Proceedings of the 6th Australian Digital Forensics Conference, Edith Cowan University.*, Perth Western Australia, 2008, pp. 1-17.

[44] J D Durick. (2011, May) Virtual Machine Files Essential to Forensic Investigations. Document.

[45] C Miller, "Electronic Evidence - Can you prove the transaction took place," *Computer Lawyer*, pp. 21-33, 1992.

[46] E. Casey, "Error, Uncertainty, and Loss in digital evidence," *International Journal for Digital Evidence*, 1998.