A Framework for Digital Forensic Investigation using Authentication Technique to maintain Evidence Integrity

Umesh Kumar Singh, PhD
Institute Of Computer Science
Vikram University
Ujjain(M.P)

Neha Gaud
Institute Of Computer Science
Vikram University
Ujjain(M.P)

Chanchala Joshi
Institute Of Computer Science
Vikram University
Ujjain(M.P)

ABSTRACT
Digital evidence is information stored or transmitted in binary form that may be relied in an investigation. Digital evidence is the core for any digital forensic investigation that takes many forms and can be found in several places. It is the evidence on which whole investigation travel and reach to an exact conclusion. Ultimately we can say that any a little bit of alteration with collected data could impact to final result, which would be extremely dangerous to grab an innocent one. In this research work we proposed a framework that covers space to lead an investigation and will keep behind all possible jeopardizes action by achieving evidence integrity associated with evidence classification and to make use of chain of custody in an appropriate position.

Keywords
DigitalEvidence,Evidenceintegrity,EvidenceAuthentication, Digital Investigation Models

1. INTRODUCTION
Crime have no definition, it can be committed by any one, at any time and in any manner. As the technology is abide by the society, crime also proportionally increasing which is the matter of concern. The subject also should be proliferated in society so the coming generation could also keep aware themselves. Digital Forensic Investigation is the phenomenon that solves the digitally committed crime and explores the culprit legally. Evidence play prominent role in whole scenario. Since all exercises are conducted on evidence. If it might tamper in any way obviously it could fall the whole investigation in abhorrence. Digital evidence exist in the binary data that is created, manipulated, and communicated by any device, computer system or transmitted over a communication system that is relevant to the proceeding. Digital evidence is fragile in nature and can be easily destroyed, damaged and might be altered if unfortunately handed over to any surplus entity. In this work we put forward a step to achieve the goal of evidence unifies. The paper is divided into 7 sections. The section 2 deals to related work, section 3 to motivation for work, section 4 is new framework, section 5 recomendations, section 6 to conclusion and 7 acknowledgement respectively.

2. RELATED WORK
The majority of Models have been presented from couples of years around from different investigation institutes, organizations and researchers. Here we have gone through four models to which we have taken as base to recover the idea.

The Groblers "Liforac Model" [1] is a live forensic acquisition processing model that collects the evidence from live acquisition to counter the problems caused by dead acquisitions them into a legally framework. The model is highly suitable to compensate the appeal with legal issues. But the matter of concern here is the evidence is merely collected and consequently pulls for analysis. So in between the collection and analysis phase if it might come in contact of any surplus entity that are capable to cause harm, than in such situation what would be legitimate action to secure, preserve, and provide its integrity. What would be our invert action against such harmful entity to safe guard the data?

The developed model in [2] followed basic concept of Liforac Model [1], but unlike the Liforac Model's technical key pillars [1] they adopted key principles Reconnaissance, Relevancy and Reliability but the working sense is similar. The model also paid full attention on flow of process according with the judiciary norms which also been done in Liforac Model [1]. The additional work adopted by Ieong's [1] model is, they appointed a case leader who does vigilance of whole process. But he is not able to take any stand in case of any tamper action performs against evidence integrity, which was also not admit in Liforac Model and its now matter of concern. Whatever actions gone happen during investigation is indeed to make in regard of judiciary bench whether it have been attacked by any threat or any attempt being tried by them to do so. Because on what basis forensic responder will make assurance to judiciary bench of such kind of hilarious work because there is not a systematic parameters existing in model.

The Hybrid Model [3] adopted the same guidelines that mentioned in [1], and [2] associated with supplementary work of filling gap in between physical and digital evidence but the remainders are same. The work in [3], again confined only to evidence collection, analysis and reporting that become a vulnerable point for intentional entities that always in queue of lurk. So only by just filling the gap in between physical and digital evidence the discussed framework is not capable to safe the evidence, still there is a sick of ignorance about the matter that must be eliminated.

The Cosic developed 14 stages [4] model whose main goal is to apply a proper management on evidence .Unlike Hybrid model [3], Cosic adopted a single phase sequential phenomenon. The model is again limited to collection and next analysis and later on reconstruction and last is publishing. We see all the discussed model are similar up to some extent but the issue is none of the model taken any action to preserve evidence, which is also our aim to impose evidence integrity and to avoid vulnerable point of model .The subject is serious for both to safeguard evidence from any external influences and also in case if any harm caused so to explain the incident with a legal assurance in front of judiciary bench it is indeed.

3. MOTIVATION

All the reviewed models done/provided an efficient approach in their possible ways because they shown us the path to go through and an opportunity to enhance it. During reviewing the literature we felt infancy after the evidence collection phase of all the investigation. As the evidence is collected, it is switched for next phase of investigation. None of the models taken any stand about how to secure the collected evidence to achieve the evidence integrity, they merely collect it and admitted that phase at any position of the framework. Since the digital data exists in an electronic form embedded onto a magnetic plate that any surplus entity can easily perform intentional tampering with the evidence. So it is needed to develop a protective layer as the evidence is being collected. The second things is all kinds of evidence kept together whether it have been from any assets or computer or might be from network. Obviously examining them simultaneously is quite hectic and complicated task, which results to confusion and also consumption of time.

Our aim is to develop a framework which imposes the evidence integrity with the use of a systematic technique that fits best against any threat.

4. THE NEW FRAMEWOK FOR DIGITAL FORENSIC INESTIGATION

Assuming our virtualization we developed a framework that uses the technique of an authenticated token to provide security level to the model. Figure 1 shows the new proposed model that accomplishes our tasks and below is the discussions respectively.

4.1 Notification

This is the very first phase of the whole investigation where first responder team come into action and get an authenticated permission to proceed further and issue warrant in regard of the case.

4.2 Preservation

At this stage the responsible team reaches to the particular crime location and freezes the whole spot completely. That is because any intentional entity could not be able to perform adversary action with the evidence in order to save the culprit.

4.3 Evidence Collection

Here the Investigation team collects all the related evidence in all manners as much as they can by adapting to all possible ways. Since we are talking about digital crime therefore all the evidence lies in digital form from different sources. In order to make our work more ease we classified the evidences according to their platform. The three categories are:-

4.3.1Internet Based (E1)

It covers all the data related to server, wireless network or we can say that the data gathered from wireless medium, Internet Service Provider incorporated here. Information regarding social networking accounts emails, or from any user friendly applications are captured kept here.

4.3.2 Stand Alone Computer or Devices

Here all the data that exists on any digital assets such as computer, hard disk, pen drive, card reader, and also scanner, printers, modem, power cables etc falls here.

4.3.3 Mobile Device

Since the invention of smart phones and because of its tremendous use we take this device separate. It itself does work similar to any lap book that indulges approximate similar functions.

As all the evidence collected now divide them according to their categories. All the data are saved on investigation machine that is linked to the particular investigation team server. An authentication token sever is sub part of the machine that would generate a seed number that behave as a password, it would be known to only to responsible team member. So nobody out of the team would not make any successful attempt .when any team member open the machine, server will authenticate it by seed number otherwise it will not permit to any other to open the machine.

E = S (E1+E2+E3)

Where, E is the secured evidence.

S is the seed number.

E1, E2 and E3, The categorized evidence.

4.4 Examination

Now all the analysis work will be perform on the collected evidence. The wok is carried out in Laboratory. We do also make use of all the already developed tools as per requirements**.**

4.5 Purification with the Judiciary Norms

After the examination now all the examined data are checked whether they are admissible in the court or not. If not then we have to look for another option to proof it in front of the judiciary bench .Here data is purified and become more unique.

4.6 Reconstruction

In case if we get any misconception to reach to specific decision then we will perform again the replica of whole crime .This stage could also be implemented when we do not get enough evidence to solve the case.

4.7 Dissemination

The whole work is ended up in a systematic manner and the team is ready with all the answers.

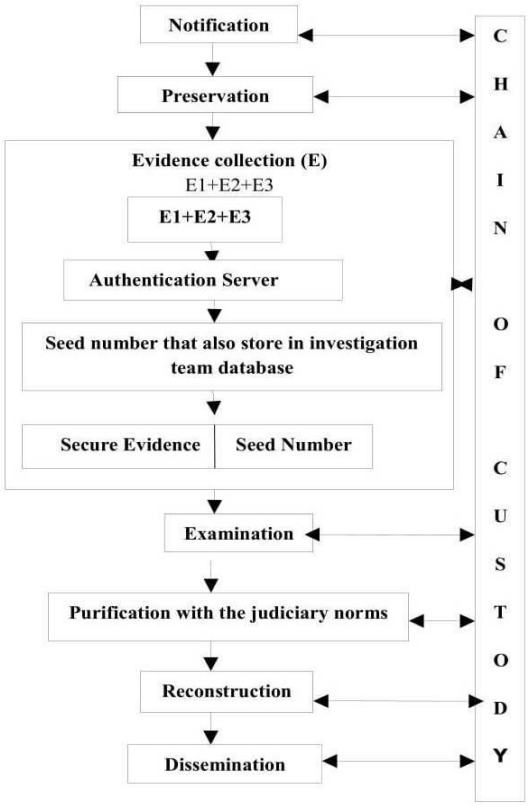

Fig 1 : The new framework

5. RECOMMENDATION

The comparison is made of the proposed framework with the few already existing work. The figure 2 shows the detail comparisons of the existing model with the new framework.

Number of phases	Liforac Model	Forza Model	Chain of custoduy and life cycle model	Hybrid Model	The new Framework
1.Notification	Yes	No	yes	Yes	yes
2.Preservation	Yes	Yes	yes	Yes	yes
3.Evidence collection	Yes	Yes	yes	Yes	yes
Evidence classification	No	No	No	No	yes
3.1 Internet based	No	No	No	No	yes
3.2 Stand alone	No	No	No	No	yes
3.3 Mobil devices	No	No	No	No	yes
Evidence Security	No	No	No	No	yes
4.Examination	Yes	Yes	yes	Yes	yes
5.purification with judiciary norms	Yes	Yes	yes	No	yes
6.Reconstruction	No	No	yes	Yes	yes
7.Dissemination	Yes	Yes	yes	Yes	yes
8 chain of custody	Not from initial stages	Yes	yes	No	yes

Fig 2 : Observation Table

6. CONCLUSION

In this paper we considered a framework where evidence and its security can be achieved by any responsible Investigation agencies. Additionally we reviewed evidence collection and classified it in an appropriate manner to utilize the time. Eventually, all the resultant is checked whether it compensates to the judiciary norms. Inarguably chain of custody is maintained from initial to the last phenomenon. It should be tested and evaluated in real investigation environment, so the respective feedback would define the necessary modification.

7. ACKNOWLEDGEMENT

I extend my sincere acknowledgement to Prof .Dr.Umesh Singh (Institute Of Computer Science,Vikram University, Ujjain) for his most valuable technical assistance and consistent inspiration for preparing this research review paper.

8. REFERENCES

[1] Bobbler.M.M, Solms S.H.von.Modelling Live Forensic Acquisition, Workshop on digital Forensic Incident analysis (WDFIA 2009).

[2] R.Ieong FORZA digital forensics investigation frameworkthat incorporates legal issues,Digital Investigation.

[3] Vlachopoulos.K., Magkos S.E., and chrissikopoulous V.AModels for Hybrid Evidence Investigation

[4] J.cosic,Z.cosic,M.Baca,chain of digital evidence basedmodel of digital forensic investigationprocesses,International Journal of computer Science andInformation Security.

[5] Ciardhuain, s.(2004) An extended model of cyber crimeinvestigation Accessed on 20 october 2011 Available onwww.ijde.org/citeseerxist.psu/viewdoc/download?doi=10.1.1.80...Accessed on 11August 2011.

[6] Baryamureaba, V. Tushabe, F.(2004) The Enhanceddigital investigation process (2004) Available(online);http://www.dfrws.org/2004/bios/day 1/tushabeEIDIP.pdf Accessed on 15 june.

[7] Reith,M.Carr.C.Gunsch,G.(2002)an examination of digitalforensic model.Department of Electrical and ComputerEngineering Air Force institute of tehnology.Wright Patterson.Available(online)http://www.utica.edu accessed on the 7october 2011.