NEW IMPROVEMENT IN DIGITAL FORENSIC STANDARD OPERATING PROCEDURE (SOP)

Sundresan Perumal[1], and Norita Md Norwawi.[2]

[1]*Universiti Sains Islam Malaysia ,sundresan@hotmail.com*
[2]*Universiti Sains Islam Malaysia, norita@usim.edu.my*

ABSTRACT. In today's digital forensic investigation, there are hundreds of specific and unique application software packages and hardware device that could be used in the investigation .Even with all this yet there are quite number of failure in SOP that being practiced by the current digital forensic investigator .In this research paper an improved SOP is being proposed. This proposed SOP will be flexible rather than being limited to a particular process of an investigation.

Keyword : Digital Forensic, Standard Operating Procedure,CyberSecurity Malaysia

INTRODUCTION

In today's digital forensic investigation, there are hundreds of specific and unique application software packages and hardware devices that could be used in the investigation (Yunus, 2008). Even with all this yet there are quite number of failure in SOP (Standard Operating Procedure) that being practiced by the current digital forensic investigator. There should be a biggest concern for every digital forensic investigator for the fragile evidence as this is always slipping out from digital forensic SOP (Sundresan Perumal &Norita Md Norwawi, 2010).

There are several research have focused on digital forensic investigation procedure .As the most basic four procedure that being identified are identification of digital forensic evidence , preservation of digital forensic evidence, analysis of digital forensic evidence and last is presentation of digital forensic evidence (McKemmish,2002).Refer figure 1.0 basic four procedure in digital forensic investigation.

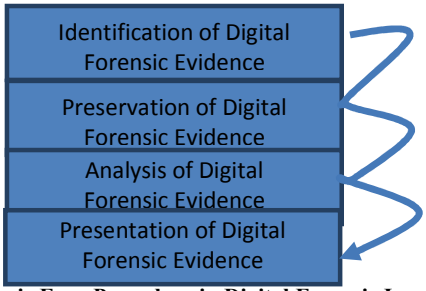


Figure 1.0 Show Basic Four Procedure in Digital Forensic Investigation.

EXISTING PROBLEM IN CURRENT DIGITAL FORENSIC STANDARD OPERATING PROCEDURE (SOP)

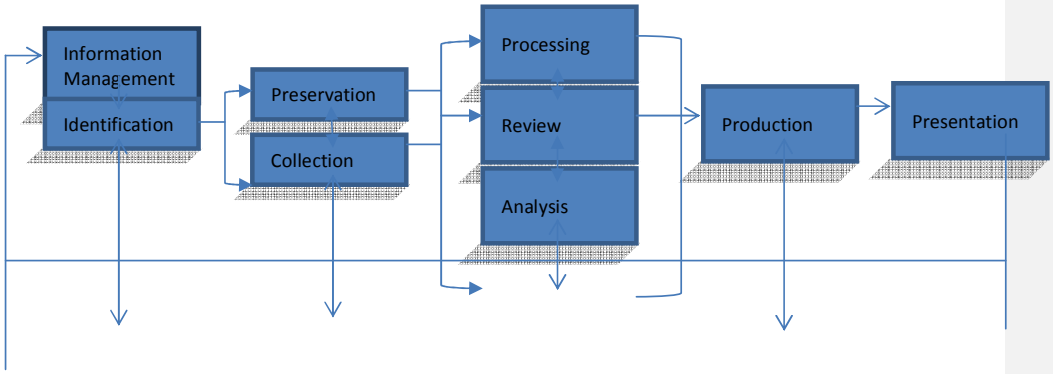
Executing evidence collection in digital forensic investigation are completely different compare to other type of evidence collection such as blood, tool mark and fibers (Brill & Pollitt, 2006). Standards operating procedures is the most important aspect for a digital forensic investigator to work. The reliability of the investigation starts from a strong SOP.

Creating a permanent set of SOP is something that is infeasible (Pollitt, 2008). The type of crime is growing very advanced, new tool and method for solving digital forensic problem are there, so with this in mind, a regular change is required in the existing SOP or else the SOP will be outdated and useless.

Different country will have different SOP to operate as there is always legal environment barrier that need to be followed.There was a time where digital forensic investigator requested for universally accepted SOP but was not been accepted since the procedure and protocol were not same in all over the country (Palmer, 2001).

The first electronic discovery reference model (EDRM) which is widely accepted as SOP framework created by George Socha and Thomas Gelbman (Socha and Gelbman, 2008). Refer figure 2.0, Electronic Discovery Reference Model showing stages from left to right.

Figure 2.0 shows Electronic Discovery Reference Model showing stages from left to right (Socha & Gelbman, 2008).



The electronic discovery reference model outline the key objective of the processing stage as below:

- Capture and preserve the evidence.
- Custodians.
- Capture and preserve the metadata.
- Establish the parent child relationship between source data file.
- Automate the identification and eliminate redundant evidence.
- Provide a means to programmatically suppress materials that is not relevant to the review based on criteria such as keyword.
- Unprotect and reveal information within files.
- Accomplish all this goals in a very cost effective manner.

IMPROVED DIGITAL FORENSIC STANDARD OPERATING PROCEDURE (SOP) MODEL.

Figure 3.0 show Improved SOP Model in Digital Forensic Investigation.

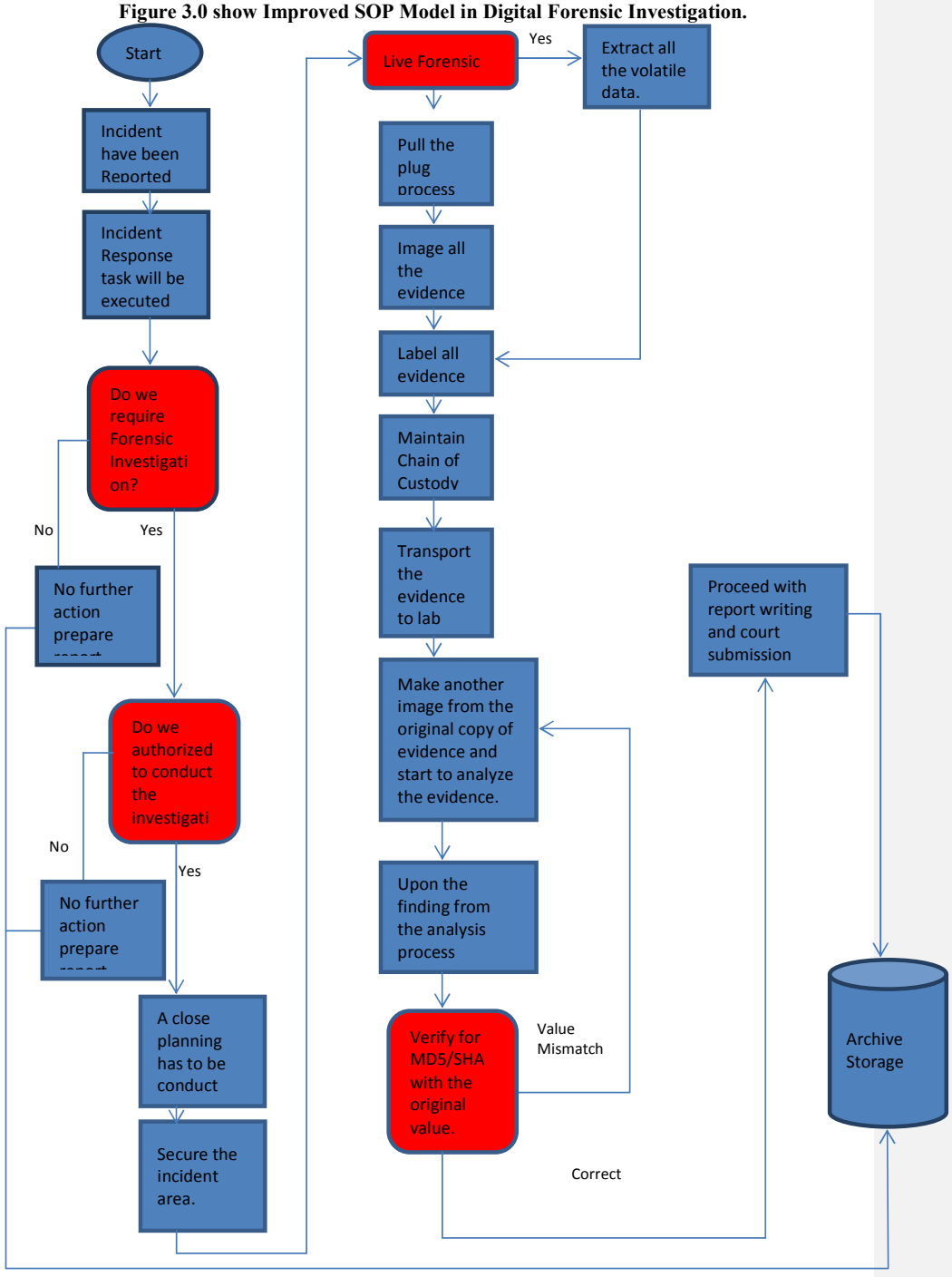


Figure 3.0, show improved SOP model in digital forensic investigation .Based on figure above it is very important for the digital forensic investigator to know the job before he continues.

According to the SOP model in figure 3.0 the first foremost itinerary need to be prepared in advanced before proceed to an investigation are *"Grab Bag"* which contain all the suitable tool, storage media and notes. The investigators need to make sure that they are well trained to utilize all the tool which is available (Baryamureeba &Tushabe, 2004). At the second level investigator have to make sure that they have been granted access to conduct the investigation and also to perform hardware seizure at the crime scene, this authorization could be obtain from a suitable manager, typically the person in charge of the incident management process, a senior manager or a police officer(Kohn et.al,2006) .

When the digital forensic investigator obtained the authorization to conduct the investigation the first thing they have to do is to secure the scene. The first task in evidence collection is , do not damage or corrupt the evidence platform particularly the primary evidence at the scene. Decide with an immediate if the suspected system power is up to conduct live forensic. In live forensic there are quite number of information that could be obtained from the memory such as clipboard content, device list, encrypted drives information, list of open network port, list of running process, and some general system information's.

If in a case of live forensic is failed or at the time of approaching the crime scene the suspected computer were power down then traditional digital forensic is going to be applied. Where the investigator required to create an image out of the hard disk drive. It is very important task to label all the evidence that collected at the crime scene. As the task continues, i physically secure both the original evidence and all the evidential copies, maintain a proper chain of custody. Upon all the evidence is being stored and it's time to start analysis process to identify the hidden data or deleted data on the evidence that have been collected .This stage may get highly technical but there are many tool exist to support this work. Once the necessary findings is done then the investigation officer need to verify that the evidence is not being tempered and the officer can proceed with report writing and court submission document preparation.

VALIDATION

The new proposed SOP is already being validated by two establish bodies as one is based in Malaysia that is CyberSecurity Malaysia, who is currently looking into most of the cyber forensic cases and another bodies is known as PeopleTech System, this is a Chennai India based digital forensic investigation lab. There were number of cases being tested by these bodies before endorsing the model to be stable and save to be practice by the digital forensic investigator and also incident response team.

CONCLUSION

In digital forensic analysis it is important for the investigator to understand that all the digital evidence depends on the case context and largely depends on the knowledge, experience, and expertise and thoroughness. Based on the improved SOP model the process flow need to be in cyclic, as digital forensic investigator need to repeat the process till a conclusion could be made.

FUTURE WORK

A**s** at the moment the SOP is only focusing on computer forensic, as in future the SOP model will be integrated into cloud computing forensic as todays modern computer environment have moved past the local data center with a single entry and exit point to a

global network. This technology require a huge forensic attention as in cloud computing it deals with high speed system for managing very large scale data sets. This platform have also raised question on complication for information security.

REFERENCES

Baryamureeba, V.,Tushabe, F.(2004) . *The Enhanced Digital Investigation Process Model.* University Institute of Computer Science, Uganda.

Brill, A.E. and Pollitt, M. (2006). *The Evolution of Computer Forensic Best Practices: An Update on Program Publications.* Journals of Digital Forensic Practice, Vol. 1, pp.3-11.

Casey, E. (2004). Digital Evidence and Computer Crime, 2nd Edition, Elsevier Academic.

Kohn, M., Eloff, J.H.P. & Olivier, M.S. (2006). *Framework for Digital Forensic Investigation.* Information and Computer Security Architectures Research Group (ICSA).

Mckemmish, R. (2002).What is forensic computing? Trend and issue in crime and criminal justice. Retrieved from http://www.aic.gov.au/publication/tandi/ti118.pdf.

Palmer, G. (2001). *A road map for digital forensic research*. Proceeding of the digital forensic workshop. Retrieved from http://www.dfrws.org/2001/dfrws-rm-final.pdf.

Pollitt, M. (2008).*Applying traditional forensic taxonomy to digital forensic*. International Federation for Information Processing International Conference. Digital Forensic : 357-365.

Socha, G & Gelbman , T.(2008). Preservation node. Retrieved from http://www.edrm.net/wiki/index.php/preservation node.

Sundresan, P & Norita, Md. (2010). *Integrated Computer Forensic Investigation Model Based on Malaysian Standard* . International journal electronic security and digital forensic. Volume 3, 108-119.

Yunus, Z. (2008). *The New Frontier For Terrorist, CyberSecurity Malaysia*. STAR In-Tech, Retrieved from http://www.thestar.com.my on 1 July 2008.