A QUANTIZED MODEL FOR COMPUTER FORENSIC INVESTIGATION

[1]ABHISHEK DIVAKAR, [2]VISHAL KUMAR, [3]VIJAY K. CHAURASIYA

[1,2]Student, IIIT – Allahabad, [3]Assistant Prof., IIIT – Allahabad
Email: adowl2001@gmail.com, vishit3107@gmail.com, vijayk@iiita.ac.in

Abstract: This paper presents a model for computer forensic investigation process which follows a quantized pattern and rigid practices. The proposed model, a "Quantized Model for Computer Forensic Investigation (QMCFI)", is capable of bringing uniformity and standardization in computer forensic investigation across the globe. Computer forensic investigations are known to fail due to absence of standards and unreli-able digital evidences. A major fraction of digital evidences presented in courts is deemed inadmissible because of that. Proposed model breaks the investigation in small independent processes which are based on a process work-flow fashion and this eradicates the various failing factors of forensic process. This paper also provides a different vantage point towards the traditional definition of digital evidence and with this authenticates not only result but also the process. This paper goes into depth of process to provide reader with an insight in investigation process. Also guidelines for documentation process which should be followed to procure reliable evidence are also given in proposed model. All in all this paper is intended to act as a handbook for computer forensic investigators.

Index Terms: Computer Forensics, Digital Evidence, Digital Investigation.

I. INTRODUCTION

Computers now became an essential part of anything and everything we do including crimes. Investigators have also taken a forward step towards computers and digital devices reciprocating criminals. These criminals are often caught and prosecuted but in a large fraction of cases their guilt could not be established due to ineffectiveness of digital evidences. This ineffectiveness can be a result of many factors like inaptness of investigators, evidence corruption, malpractices etc. Regardless of the reason, a standard methodology is needed which can be applicable in a broad spectrum of scenarios and produce more reliable digital evidence. This paper presentsa Quantized Model for Computer Forensic Investigation or QMCFI in short. This model is designed to produce reliable and undeniable digital evidence. For that purpose this model incorporates a quantized approach towards computer forensic investigation which breaks down the

investigation process into small independent processes and providesnecessary flexibility increasing reliability at the same time. This approach seeks and eradicates the reasons which turn evidenceinadmissible in court of law. This model also suggestsa slightly different definition of Digital evidence which will prove to be a turning point in digital forensic technology. Computer forensic process has remained consistent for too long against ever changing crimes and criminals. It is the high time for it to evolve too.

A. Digital evidence:

"Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial." This is the definition of Digital Evidence that is still being used in computer forensics and it had served us wonderfully until now. But now, with increasing complexity of cases, more often than not digital evidences are being denied and declared inadmissiblein courts because of two reasons: The ease by which digital evidences can be tainted and tampered. And the absence of a standard methodology which can authenticate not only evidence but also investigation process. Two most desired qualities of digital evidence are integrity and authenticity. Integrity refers to the property of evidence of being in original state as it was before seizure. Digital evidences are never in human readable form so the printouts of computer documents were deemed admissible in court. These printouts are also considered as a part of digital evidence. Authenticity not only refers to the property of evidence being what it claims to be, but also of these printouts to be from the origin they claim to be. To strengthen the evidence and diminish the chances of inadmissibility, current model, QMCFI suggest that not only the artifacts and printouts constitutes the digital evidence but all the supporting documents which can add to integrity and authenticity of digital evidence are part of digital evidence. The evidences created by this model and ideology will be effectively undeniable in any court of law.

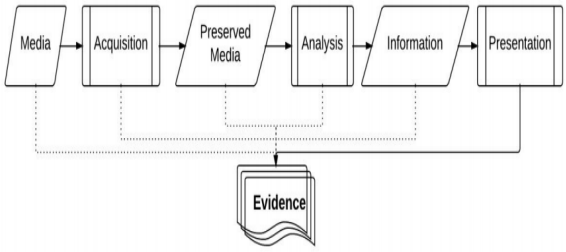


Fig.1 -Composition of Digital Evidence

II. RELATED WORK

Computer forensic is a relatively new field which is originated from computer science and not much work have been done in this field. Computer Forensics came into light when Palmer published "A road map for digital forensics research". Afterwards numerous models for digital forensic investigation were proposed e.g. DFRWS model, US Department of Justice Model, Abstract model, A hierarchical-objective-based framework for digital investigation process, FORZA and The two dimensional evidence reliability amplification process model. All these models lack one thing or another. And only few watched itlight of legal obligations. Fewof them Mandia , Carrier and Spaford and Beebe-Clark mentioned preparation and almost none said what happens after extraction. FORZA was the only one which talked about legal issues and even the latest model followed by DOJ[3]and NIST do not cover the whole process anddepend completely on investigator's expertiseto provide reliable evidence. Definition of digital evidence is also notevolved since 2004.

III. PROPOSED METHODOLOGY

The methodology proposed in this paper focus on quantizing the forensic investigation process into small independent sub-processes. Quantizing the forensic process provide several advantages over preceding models. Quantizing the process means that all the steps of all phases can be performed by separate investigators and investigation will have small processes. Also for this to happen documentations becomes an essential part. Every process in proposed model is well documented and this eliminates the possibility of any malpractices in investigation process. This also diminishesthe loss in progress that happen due to change in investigators mid-process. As we said before, aimof this model is to bring standardization in computer forensic investigations and, by that, increase reliability of evidences by increasing integrity and authenticity. The proposed model also suggests a different specification for digital evidences and the increased documentation in model endow to this improved specification of digital evidences.

[Documentation]Investigations are not necessarily meant to be carried out by one entity alone. Investigators can often be changedand generally various phases of investigation are carried out by different peoples. So it is strongly advised to commit everything to reports and leave nothing to remember. This way a new investigator can easily come up to speed on case and documentation will also prove very helpful in final phase while presenting the evidence. Documentation should be started as soon as investigation is started. Each step hasdifferent outcomes and should be documented likewise. For this purpose we suggest documentation for each step immediately afterwards. Blank forms for this purpose should be available readily.

A. Phase I – Acquisition

Every forensic investigation is triggered by an event and computer forensics is no exception. Before starting it is essential to make surethat proper authorization is attained to perform assigned tasks, chain of custody is defined comprehensively and proper paperwork is in place.A large fraction of evidences isdenied in court because theinvestigators collected them withoutauthorization orthey just forgot to file proper paperwork. Also the level of investigation must be established before putting in resources, be it civil, criminal or organizational. Jumping in without considering these factors will most probably result in a failed investigation.Acquisition or evidence acquisition refers to identification and preservation of relevant digital artifacts which can later be used as evidence. To begin with acquisition phase, first task will be to secure the site. To stop any activity that cantamper with the potential evidences e.g. stop any network or physical activity at the site. For this easiest way is to turn off the network devices such as router, switch, hub, wireless access points etc. It is also needed in some cases to turn off the monitoring devices like CCTV, as it happens;this duty also falls on the shoulders of Forensic investigators.

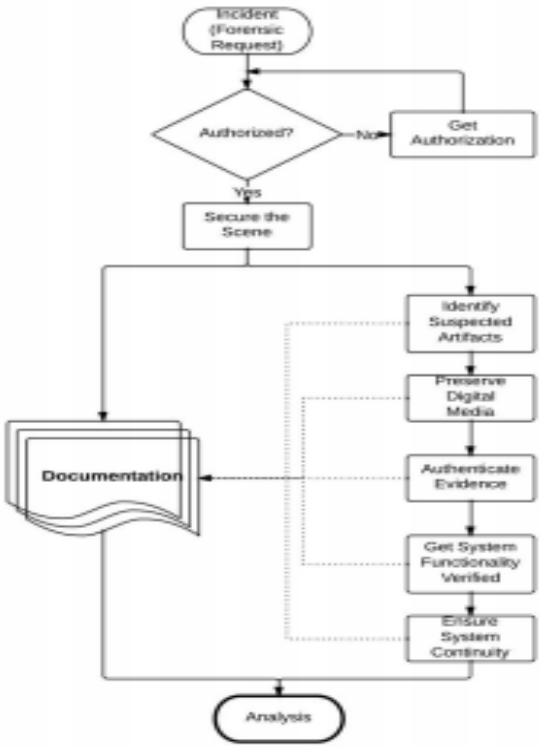


Fig. 2. –The Acquisition Phase

1. IDENTIFICATION

At this point we have a secured site which is effectively isolated. Next task is to identify systems

which might contain information relevant to our investigation. This is easier said than done. Identification is the most crucial part of any forensic investigation. Investigator may leave out some systems which may contain important information or he might include a lot of systems only to find later, during analysis, contains redundant and irrelevant data. This will impact directly on the amount of effort and cost involved and ultimately the effectiveness of investigation and that of the investigators.To identify systems most effective path will be to interview system-users. Unless you are in a hostile environment where system-users tend to be non-co-operative, investigators can get a lot of useful information by users like passwords for systems, encryption, user roles and nature of data on systems. As an investigator you should not have any presumptions about case and should act accordingly.Now, investigator should briefly analyze all the devices on the location. This may sound unreasonable and very tiresome but criminals generally flourish on the ignorance and negligence of investigators. Smart criminals tendto hide evidence, sometimes in obvious places. So as a precautionary measure no systems should be left on presumptions that it might not contain useful data.The most important thing to remember is no to do anything that might tamper the evidence like shutting down, booting, saving etc. Some criminals also Booby-trap their systems to delete evidence on specific triggers. These precautions dependon the type and severity of investigation. Generally the best way to identify relevant systems is to open them and search for keywords, files in obvious places and installed software. For this investigators need various software which can break passwords like ERD Commander, Hiren's BootCD etc. and some tools like backtrack forensics which can boot a system externally and can collect evidence. Some Hardware tools also prove useful like write blockers through which HDDs of systems can be checked without tampering a single bit. Once relevant systems have been identified we can continue with preserving them. CD/DVDs and thumb drives and other storage devices also need to be analyzed and identified as they too may contain incrimination data.[Documents]

 Chain of custody Document. A copy of which will stay with the evidence from beginning to end, continually being updated, and will be a part of final report.
 A document of authorization for Investigation.
 A register of all the devices present at the location, giving each a unique id, and justification behind their inclusion or exclusion as relevant system.
 A document containing all the information which is procured by investigator by other means like interviews, location etc. Photographs of systems should also be attached to this report. A summarized report should also be prepared.

2. PRESERVATION

As name suggests, this phase consists of collecting the identified evidence and preserving them, so that they can be analyzed and presented to prove offense. One way to do it just 'bag and tag' means simply confiscate or seize the HDDs and other storage devices. But for a forensic investigation it is advised not to do any analysis directly to the Device which might accidentally ruin the evidence. So investigators should create aworking copy or analysis copythrough cloning. Also the system being affected by confiscation will affect the business process, so to maintain business continuityinvestigators may replace the existing devicewith a clone. So it's assumed that two clones for each relevantHDD are to be created. For this, investigators use various Forensic Duplicators(not same as HDD Duplicators).These devices have inbuilt Write blocks to facilitate cloning in a forensically sound manner. A hash value will be generated after cloning of each device which will be used to verify integrity later in investigation so it must be documented carefully. This being done it's time to mark all the confiscated artifacts with the unique id and hash, bag them, and get it verified from competent authority that they indeed originated where they said they did.It's better for forensic investigatorsnot to leave any footprints or aftereffects of theirpassing, so they should ensure that the systems are functioning as before the investigation and no loss in productivity is causedin organization. It is also advisedto get this verified by users or other authorities lest someone sue for damage.[Documents]

 A brief report listing all the devices acquired,their unique ID, date and location of acquisition, type, model no., serial no, hash value, corresponding clones, hashes, their model no., serial no. etc. This document must be verified by investigator and designated authority.
 A detailed reportcontaining all the information about devices acquired by investigators. Including, but not limited to, information about users, nature of work, department, passwords, encryptions etc. This document is to aid in the analysis phase and need to be attached with main report.
 A No-objection certificate stating that all devices are working as expected after acquisition. This should be signedby location representative.

B. Phase II – Analysis

This phase is where actual forensic happens. In this phase we identify and extract the information required from the media acquired in last phase. Please be aware that we work only on the media and reports provided by the acquisition phase and in most of the cases it is not possible to go back to the scene tcollect additional evidence. Again investigator need not be the same as the one who performed Acquisition, that's why all forensic investigators need to be thorough in their reports.

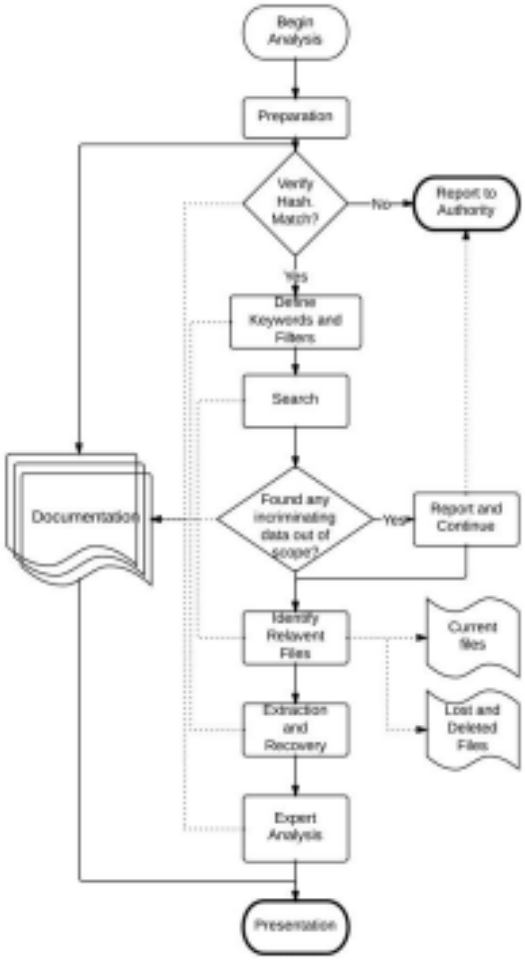


Fig. 3 –The Analysis Process

1. PREPARATION FORENSIC LAB:

To perform aforensic analysis we need a lab which is capable of handling data and devices in a forensically sound manner and have all the required tools: software and hardware to perform the task. The systems performing the analysis should not be connected to any network. In cases when a network is needed a local network could be set up which must be isolated from outside network. These systems contain sensitive information and should be protected accordingly, physically and logically. INTEGRITY CHECK: Before starting with the analysis, investigator need to verify the integrity of the media provided with the reports of acquisition. Investigator must calculate hash of media and match them against the reports of acquisition. If the hash isfound to be inconsistent with the acquisition report then investigator needs to stop and report to the authorities. Logic behind this is if you perform a forensic analysis on such device it is most likely not going to be admissible in any court because our initial artifact was tainted. DEFINE SCOPE: Define scope of the analysis based on the nature of crime and warrant issued. Any evidencethat is found outside the scope is inadmissible in courts unless investigator just stumbled on it by chance and wasn't looking for it. Even in such cases it is expected to get a warrant for second offense and make a separate case. So, if such evidences are encountered then investigators should report to authorities and continue with current investigation.DEFINE RELEVANT EVIDENCE: Before starting the investigation investigator must know what he is looking for. It is too unprofessional and cost ineffective to search for everything. Relevant evidence can be defined by investigator's own experience and consultation with subject specialists or experts. An Investigator can also be a expert himself lest he have proper qualifications to testify in court as expert in that matter. For example in a health related scenario a forensic investigators probably will be unfamiliar with the information relevant to the case. In this case they can consult experts, i.e. doctors, for probable type and nature of evidence.[Documents]

- Report of Integrity check i.e. hash matching must be documented.
- Documentcontaining information about scope, warrant, expected information and relevancy should also be produced.

2. IDENTIFICATION DEFINE KEYWORDS AND FILTER:

Define the search keywords and filters based on scope and expert advice. Most of the forensic analysis softwaretools like EnCase facilitate a grep keyword search. Forensic investigators must be apt in writing grep queries for searches. Also some tools like FTK comes with various preprogrammed keyword sets for general cases such as child pornography, emails, web addresses etc. Investigators must be very careful while defining and selecting keywords and filters so that they satisfy the scope of the investigation. Minimizing the keywords to search while covering the whole scope will result in a cost and time effective process. SEARCH: Search the given artifacts with defined keywords and apply filters. Then investigators have to look at the search resultsandidentify audit trails. Results will include current files, which generally are in perfect health, and lost and deleted files, some parts of which might be lost and are only recognized by analyzing headers in free spaces in Storage devices. Deleted and lost files are grouped by type as they don't have file system entries to specify location and are searched by their headers. Searching also includes manual searches in which investigator have to manually open each file and decide whether it is relevant or not using his expertise. IDENTIFY RELEVANT FILES: Result of search should now be checked manually by investigator and relevant files should be marked for retrieval. This should be done on basis of prior consultation with the subject expert. Again if information outside the scope is caught in the search, it is very important to report to the authorities and do notlet that hinder the current investigation. Audit trails found should be followed accordingly but no

trail is worth following if it's not going to be accepted in court.[Documents]

 A document containing detail of whole process, used keywords, filters, found relevant files and reasons of exclusion.

3. EXTRACTION

In extraction we recover the files identified in the last phase. These files, if healthy, are easy to extract but if they are deleted or lost then it becomes a tedious task and investigator will have to use data carving tools to extract files based on their headers. These files should then be provided to expert in desired for be it in electronic or printed form. Files which are password protected present additional challenge. There are numerous tools to reveal passwords. These files should be analyzed after breaking password and documented as such.[Documents]

 List of documents extracted should be documented to avoid any malpractices.

 List containing names and locations of password protected files.

4. EXPERT ANALYSIS

All the work up till now was to gather information to build the case. But in this phase all that gathered information is provided to Subject matter experts who now relates information, analyze them and build the case. Expert Analysis is not essentially a part of forensic investigation but the team which constitutes experts contains lawyers, specialists and forensic investigators too. All the findings of experts must be documented and verified.[Documents]

 Documents containing findings of various experts signed / verified by them and competent authority.

C. PHASE III – PRESENTATION

This phase is where investigators along with expertsprepare findings to be presented in case, provide testimony and resolve conflicts. In internal forensic investigation it also becomes a job of investigators to find the root cause and suggest countermeasures.

1. PREPARATION

In this phase all the documents and findings and conclusions are indexedarranged and sorted in an effective manner and presented in court. The lawyer is essential to this phase and this is not actually a forensic related task but investigators are a essential part of this process and must be aware that his duties extend to this phase too.

2. PROVIDE EXPERT TESTIMONY

A forensic investigator is also considered an expert. So he can also be called upon by court to testify for validity of investigation and his findings.

3. DISPUTE RESOLUTION

Sometimes question of integrity and authenticity of evidence and findings can also be put into question by court. In such scenarios, it becomes duty of forensic expert prove authenticity of evidence and sometimes replicate some analysis steps.

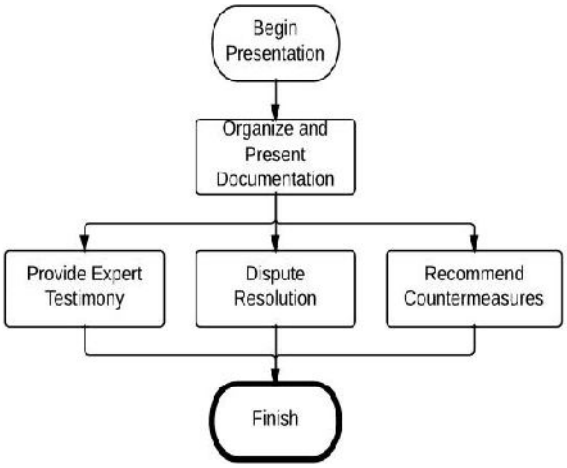


Fig. 4 –The presentation process

4. RECOMMEND COUNTERMEASURES

In internal organizational investigations it is also expected of forensic investigators to find out the root cause of offense and provide recommendations and countermeasures for the same.

CONCLUSION AND FUTURE WORK

Proposed Model, QMCFI, is much more reliable and flexible than previously proposed models. The quantization of computer investigation process increasesthe authenticity of procured evidence by suggesting a standardized process and adding proof of authenticity of the process to the resulting digital evidence. Proposed model simplify the investigation process and prevent the chances of small mistake to be amplified into huge ones. Also, an adjustment hasbeen made to traditional definition of digital evidence to accommodate additional process authenticity. Both the model and definition complementeach other. Still, a single paper is unable to capture all the aspects of computer forensic investigation with desired level of detail. More research on each phase separately is required and continuous revision of investigation techniques is required with evolving technology. Also opinions and research of scholars from related disciplines like legal and law enforcement are required to complete the study.

REFERENCES

[1] Eoghan Casey, “Digital Evidence and Computer Crime, Second Edition”, Elsevier, 2004.

[2] Gary L. Palmer, “A road map for digital forensics research” – report from the first digital forensics research workshop (DFRWS) 2001.

[3] DoJ, “Electronic crime scene investigation: a guide for first respond-ers”, U.S. Department of Justice, 2001.

[4] Mark Reith et. al., “An examination of digital forensic models,” International Journal of Digital Evidence, Fall 2002.

[5] Nicole Lang Beebe and Jan Guynes Clark, "A hierarchical, objec-tives-based framework for the digital investigations process," Digital Investigation 2.2, 2005.

[6] R.S. Ieong, "FORZA–Digital forensics investigation framework that incorporate legal issues." Digital Investigation 3, 2006.

[7] Marjan Khatir et.al. "Two-dimensional evidence reliability amplifi-cation process model for digital forensics," Digital Forensics and In-cident Analysis, 2008.

[8] Kevin Mandia et.al. “Incident response & computer forensics,” 2nd ed., McGraw-Hill/Osborne, Emeryville, 2003, p. 507.

[9] Brian Carrier and Eugene H. Spafford, “Getting physical with the digital investigation process,” International Journal of Digital Evi-dence, Fall 2003.

★★★