Evaluating the Harmonized Digital Forensic Investigation Process Based on Call Detail Records

KHAWERIS KHAULA*, IMRAN TOUQIR*, MUHAMMAD FAISAL AMJAD*, AND MUHAMMAD RIAZ MUGHAL**

* Military College of Signals, National University of Sciences & Technology, Rawalpindi, Pakistan.

** Mirpur University of Sciences & Technology, Mirpur, Azad Jammu & Kashmir, Pakistan.

Authors E-Mail: (khaulakhawer.msis14@students.mcs.edu.pk, imrantqr@mcs.edu.pk, faisal@mcs.edu.pk, riazdat@must.edu.pk)

ABSTRACT

Digital forensics gained significant importance over the past decade, due to the increase in the number of information security incidents over this time period. Further that our society is becoming more dependent on information technology. Digital forensics is the process of employing scientific principles and processes to analyze electronically stored information and determine the sequence of events which lead to an incident. Mobile forensics recovers digital evidences from a mobile device under forensically sound conditions based on accredited methods. The biggest challenges faced by the discipline are the ever-changing technology of mobile devices and the lack of a customary digital forensic investigation models. HDFI (Harmonized Digital Forensic Investigation) Process Model is currently premature; however, it is expected to qualify for ISO/IEC-27043 (International Standard Organization/ International Electrotechnical Commission). This demands thorough testing of this model, by taking different types of the digital evidences plus various types of digital forensic investigations into account. CDRs (Call Detail Records) are very significant digital evidence that can contribute a towards a successful investigation and in achieving concrete results. In this paper, HDFI Model has been evaluated using CDRs. The aim is to validate the said model in mobile forensic investigations using CDRs, as the basic digital evidence. An anonymous real-life case scenario is taken for the testing purpose and the CDRs analysis is successfully accommodated in the model. It is established that the model is reasonable enough to ensure the admissibility of the digital evidence in the court.

Key Words: **Mobile Forensics, Digital Forensic Investigation, Harmonized Digital Forensic Investigation Process Model, Harmonized Digital Forensic Investigation, Call Detail Records.**

1. INTRODUCTION

As the world becomes digitally associated, mobile devices have become the leading form of transmission around the globe, as a result, cyber-crime actions across mobile devices, are also growing rapidly [1-3].

The smart devices can save, transmit and process large amounts of confidential data [4]. The improved performance of portable devices can assist in the battle against crimes.

Investigative process models have not been adequately verified and tested in mobile forensics. In order that process model fulfills the standards of the digital forensic area, substantial testing is needed to validate [5]. Ademu and Imafidon [6] emphasized the significance of peer-reviewing, testing and validation of an investigation process model, in a scientific manner.

The HDFI Model is the primary endeavor to standardize the digital forensic investigation process. The HDFI process model is on its way to become an ISO via IEC-27043 [7]. Therefore, it is required to be tested in various aspects and dimensions [8]. The evaluation of HDFI model has great significance to ensure that the model conforms to the standard requirements of the digital forensic community.

In this paper the HDFI model is evaluated by taking CDRs as the prime digital evidence to decide whether the process model is appropriate for mobile forensic investigations. The testing is carried out to evaluate the effectiveness of the HDFI model in a scenario. The paper discusses the strengths and constrains of the said model, during investigation.

The paper layout is as such that the introduction has already been covered in section-I. Rest of the paper has been organized as such that section-II through light on the mobile forensics, CDRs and the HDFIP model. Section-III gives the methodology followed by case study. Section IV elaborates model evaluation. Performance evaluation has been presented in section-V followed by section-VI that concludes the paper.

2. RELATED WORK

Mobile Forensics: Mobile device forensics is an evolving branch of digital forensics that concerns to the recovery of digital evidence from a mobile device under forensically sound circumstances, using accepted methods [7]. The NIST (National Institute of Standards and Technology) guide

covered various important aspects of mobile device features, associated technologies and their relation to forensic procedures. Data acquisition of mobile devices is tricky and requires specific standards that are sound as per Forensic Standards [9]. The different processes involved in the forensic investigation include acquisition, preservation, analysis, examination and reporting of digital evidence.

Martin [10] termed that the mobile device forensics world is a complex one. Dissimilar to the PC world's predetermined amount of considerable operating system sellers, there are incalculable makers of cell phones. To convolute things further, every cell phone producer might have his own exclusive innovation and groups. New cell phones are announced at the rankling pace, that continuously effects the research dimensions.

Call Detail Records: CDRsare a network operator's business records that documents communication activity and location of a particular cell phone over time within its own network [11]. The CDRs are maintained by the service provider/operator. MSC (Mobile Switching Center) generates CDRs every time a user makes a call or send a text message. Besides billing information for consumers CDRs facilitate many other network activities as well [12].

The format of the CDRs varies widely among different network operators but all contains the essential information that may interest to the forensic investigators including calling and called numbers, call duration, time of call initiation, and the call type (Voice, SMS (Subscriber Identification Module) or data) [7].

The procedure for obtaining CDRs from the respective network operator varies in different countries and should be in accordance to the respective state laws and policies. However, network operators are reluctant to make their records public.

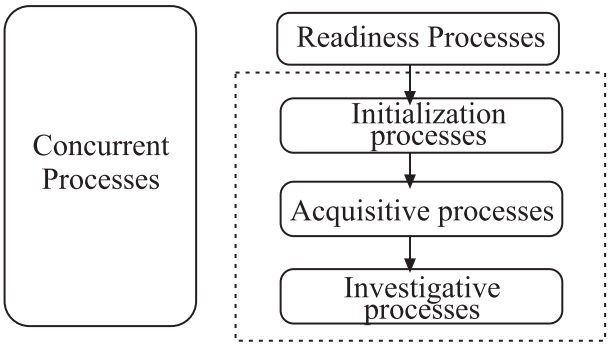

FIG. 1. CLASSES OF HDFIP MODEL [13]

CDRs have the essential data to perform a historical cell site analysis that includes cell, tower/sector location in respect of cell phone. Today, conventional respondent area evidence might be supplemented with authentic CSA (Cell Site Analysis) evidence in situations where one or more than one mobile phone can be joined with litigants, co-conspirators, associates, casualties, or eyewitnesses now and again and places important to the charged offenses. Narrowing the geographic area of mobile devices to one of a cell tower segments at a time is helpful in building up the nearness of distinguished mobile devices in respect to crime scenes and other pertinent areas alongside development patterns of the mobile phones [7].

HDFIP Model and Current State of Research: Valjarevic and Venter [2] proposed the HDFI process model. The proposed model is broad enough to be utilized for diverse digital forensics examinations and distinctive sorts of digital evidence. Additionally, the model is an up-gradation/ enhancement of the past models.

HDFI process model is generic and is on its way to become a standard; ISO/IEC-27043 [13], as shown in Fig. 1.

The model is being tested in various aspects since then. Mumba and Venter [12] tested the HDFI model in postmortem digital investigations. Stacey and Venter [6] perform testing of HDFI process model using an Android mobile phone to authenticate the workability of the HDFI process model with mobile phones.

The HDFI process model consists of five classes Plus the model includes some parallel actions in the model, based on ethics, that the investigator should follow throughout a digital forensic investigation, concurrently with other investigation phases to make sure full acceptability of the digital evidence in formal proceedings (e.g. in court) [11]. These concurrent processes are the activities that harness the integrity of results and contribute immensely to the entire investigation.

3. METHODOLOGY AND CASE STUDY

A criminal proceeding case under investigation is such that the mobile device linked with that in some fashion was not accessible. We can consider a robbery case or some terrorist activity. In such cases, there is seldom any chance of digital evidence acquisition “on the scene”. This makes CDRs the prime digital evidence. We are considering such a situation where a crime has occurred, and the forensic investigators are trying to discover some clues to identify the suspect through the CDRs analysis. The investigators sought the CDRs from

network operators for the nearest cell towers (of the incident location) and against the time at which the incident took place. The investigators mark the calls made during the period. The CDRs pertaining to the suspects (caller) are obtained from the cell network operators for the digital investigation as per mutually agreed contract between both parties. It facilitates monitoring of the connections or contacts of the suspects and reveal their movement patterns.

The CDRs are obtained from XYZ Company whereby CDRs are limited for experimental analysis. Only the results are described in the paper because of the confidentiality of the CDRs and privacy of the costumers. "Sentinel Visualizer" software is used to map the CDRs for visualization of the data.

4. TESTING THE HDFI PROCESS MODEL

The HDFI process model is applied throughout the investigation process. Law enforcement authorities can obtain the CDRs from the service providers through the appropriate legal documentation. Procedures for getting records from service providers may vary among different countries/ states. Accredited firm/ chamber and ongoing consultation with legal counsel is advisable as self-explanatory in Fig. 2.

The Readiness Processes Class: As the readiness is the organization's ability to optimally perform digital investigations. This optional class does not belong to the investigation procedure itself but needed for preparation and its planning. The existence of agreement between the network operators and the regulating authorities for the acquisition of the CDRs is the readiness desired in this case. We further discuss the 14 phases of the HDFI process model involved in the investigation.

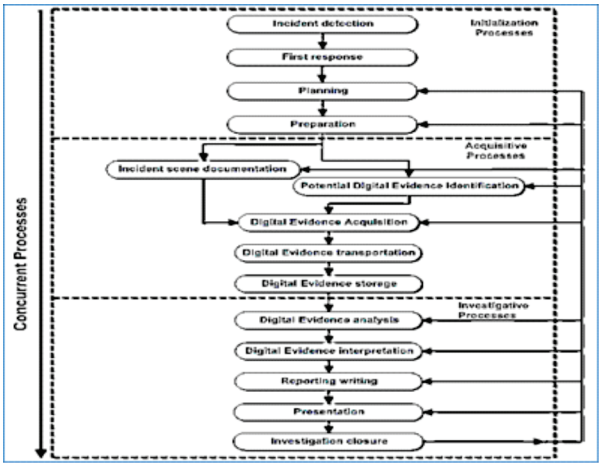

FIG. 2. HARMONIZED DIGITAL FORENSIC INVESTIGATION PROCESS [13]

Incident Detection Process: A criminal activity has been occurred and reported. The forensic investigators did not find any digital evidence from the incident scene. The incident is first detected by some media personnel or a common man that was present at the incident scene. He/She then reported the event to the crime investigator.

First Response Process: The digital investigator of the crime cell is the first respondent of the incident. After getting no digital evidences from the incident scene, the investigator informed the same to the authorities about lack of evidence for investigation, hence maintaining the flow of information that is needed throughout the investigation process.

Planning Process: The investigator seeks the required history of the suspect from the network service provider and remain in close coordination with network operator as case processes further. As the readiness processes have already been followed, we only need to incorporate the readiness class processes in this phase.

Preparation Process: In this phase, all the equipment and data that will assist in the analysis phase are prepared and collected including the CDRs link analysis software "Sentinel Visualizer" for CDR visual analysis. It acts like a forensic workstation for analysis of CDRs and obviously attains the data history of the client from the mobile service provider.

Incident Scene Documentation: All the documentation, after interviewing the first respondent of the case plus the photographing of the evidence at the incident scene, was handed over to the digital forensic investigator.

Potential Digital Evidence Identification Process: The investigator acknowledged and documented the CDRs as the potential evidence.

Digital Evidence Acquisition Process: CDRs are collected from the relevant service provider. The receiving investigator at the lab acquired the custody of CDRs after signing the received and release vouchers. As the investigation proceeds and the need arise, more relevant CDRs are acquired from the service providers. This may be an ongoing activity during investigation. The investigator also documented the whole process while conserving the CDRs chain of custody and

integrity.

Digital Evidence Transportation Process: The digital evidences (CDRs here) were transported to the laboratory in a forensically sound style and hence maintained its integrity. CDRs are transported both electronically (through email) and physically (in the form of CDs).

Digital Evidence Storage Process: The evidence is stored when the analysis was not required to be carried out in real time. However, in this case, the analysis was done immediately according to the sensitivity of the event but at the same time CDRs are protected as per the legal obligations.

Digital Evidence Analysis Process: The CDRs were saved on a hard drive, at lab, that is forensically cleaned and a forensic copy of the acquired CDRs was made. Further analysis was done on the copy to preserve the integrity of the original evidence. The mapping software Sentinel Visualizer was used to analyse the CDRs into some meaningful information. The calling patterns were established, CDRs were examined and analysed to identify the travel behaviour of the suspect through forensic tool.

During the analysis phase, CDRs may be considered insufficient to process further investigation. The CDRs would again be requested from the service providers, acquired through the digital evidence collection phase and then transported and stored for analysis. Hence the need for an opportunity to go back from the analysis phase is observed by the authors for the demand of additional CDRs.

All the parallel activities were properly followed including information flow and the preservation of digital evidence.

Digital Evidence Interpretation Process: The analysed data was interpreted and selected by taking the relevant case into account. The selected information was also sorted in the descending order of importance of the collected data to the investigating case.

Report Writing Process: The comprehensive summary of the entire investigation process is presented in easy language that is understandable for all the involved stakeholders, i.e., the investigators, the affected personnel, legal authorities and the government (as per the nature of the crime). The summary should include all the details such as who did what and how and their respective location as per timeline. The inference of the mapping software is also included in this phase.

Presentation Process: The sorted evidences plus the detailed report are presented to all stakeholders.

Investigation Conclusion Process: After presenting the results, the investigation process will be considered as closed. The evidence and the investigations done on CDRs are found satisfactory to identify the suspect criminal where no other digital evidence was at hand. And if the results of the CDRs analysis are supported through some other evidences, they will provide a solid proof to induct a criminal.

The Concurrent Process: This phase comprises of the parallel actions that are to be carried throughout the investigation process. The actions include acquiring the authorization, preserving the information flow, documentation, and the chain of custody. These actions are successfully performed throughout. 'Interaction with the physical investigation' activity is not applicable here as we do not have the mobile device in hand. The goal of the parallel processes is to attain and preserve integrity, confidentiality and availability while keeping the investigation process as efficient as possible. The acceptability of the digital evidences, in the formal proceedings or the court of law, is also ensured by the concurrent processes [14].

5. FINDINGS AND OBSERVATIONS

It is important to note that the emphasis of testing is to evaluate the effectiveness of the HDFIP model. The analysis of CDRs is a part of the HDFI model's Investigative Class and it further validates the successful accommodation of such testing in the HDFI model.

It is found that there may arise a need for more CDRs during their detailed analysis in the mapping software. The authors, therefore, recommend that the forensic investigators ought to have the facility to go back to the planning phase for more CDRs from analysis phase. The authors found it unnecessary to first conclude an incomplete investigation and then start all over again.

It is also observed during the evaluation that CDRs alone may not be enough to indict a suspect; it must be supported by further investigations or proofs. There exists a possibility that the suspect has used a stolen cell phone and hence, the IMEI (International Mobile Equipment Identity) or SIM can be registered on someone else' name. Cloning of SIM or IMEI spoofing can also be the possible reasons to avoid indicting a

suspect solely on CDRs analysis. However, it must bring into notice that CDRs provide valuable insight towards investigation of crime.

As all the phases of the said model are the inputs to the next phase, so to make the model efficient, parallel actions must be carried out. The concurrent processes are meant to avoid contamination of CDRs and any unauthorized access to them. They also ensure proper information flow and documents to compensate for the fact that different personnel with varying expertise are involved in the investigation.

6. CONCLUSIONS

The need of the testing of the HDFI process model (which is expected to be an ISO standard) is discussed in the paper. The paper thus presents the findings of the investigation process after evaluating the said model. The testing of the service provider CDRs is efficiently accommodated by the HDFI process model. The successful evaluation of the CDRs (during investigation) ascertains the efficiency of the HDFI process model. The competence of the model lies in the fact that it makes the investigators and analysts accountable for every action taken by ensuring the concurrent processes throughout the forensic examination.

The paper provides a concrete move towards the standardization of the HDFI model by conducting the successful analysis of important digital evidence. The integrity, confidentiality and availability of the CDRs are effectively maintained throughout the forensic investigation procedure.

The authors mention that the forensic investigators ought to have the facility to go back to the planning phase from analysis phase, as per the need for more CDRs during analysis.

7. FUTURE WORK

Future work is intended to include the testing and investigation of more types of digital evidences (forensic tools, digital devices, vendor/service provider data) and digital investigation environments (live, post-mortem, network, mobile) using the HDFI process model. The testing of the model through CDRs while having the mobile device in hand may also be considered as potential work.

ACKNOWLEDGEMENT

The authors wish to thank the FMS Advanced Systems Group for providing us with the complete trial version of their CDR link analysis software "Sentinel Visualizer" that was needed for the testing of the HDFIP model.

REFERENCES

[1] Raghavan, S., "Digital Forensic Research: Current State of the Art", Computer Science & Information Technology, Volume 1, pp. 91–114, 2013.

[2] Valjarevic, A., and Venter, H.S., "Harmonized Digital Forensic Investigation Process Model", Proceedings of IEEE Conference on Information Security for *South Africa*, Johannesburg, Gauteng, South Africa, 2012.

[3] Goel, A., Tyagi, A., and Agarwal, A., "Smartphone Forensic Investigation Process Model", International Journal of Computer Science & Security, Volume 6, No. 5, pp. 322, 2012.

[4] Owen, P., and Thomas, P., "An Analysis of Digital Forensic Examinations: Mobile Devices Versus Hard Disk Drives Utilizing ACPO and NIST Guidelines", Digital Investigation, Volume 8, No. 2, pp. 135-140, 2011.\

[5] Mumba, E.R., and Venter, H.S., "Mobile Forensics Using the Harmonized Digital Forensic Investigation Process", IEEE Conference Publications, 2014.

[6] Ademu, I., and Imafidon, C., "The Need for Digital Forensic Investigation Framework", International Journal of Engineering Science & Advanced Technology, Volume 2, No. 3, pp. 388-392, 2012.

[7] Jansen, W., Brothers, S., and Ayers, R., "Guidelines on Mobile Device Forensics", National Institute of Standards and Technology, Special Publication, 800, 101, Revision-1, 2014.

[8] Omeleze, S., and Venter, H.S., "Testing the Harmonized Digital Forensic Investigation Process Model Using an Android Mobile Phone", IEEE Conference on Information Security for South Africa, Johannesburg, South Africa, 2013.

[9] Sharma, K., Makino, M., and Shrivastava, G., "A Volume in the Advances in Wireless Technologies and Telecommunication (AWTT)", Book Series, 2020.

[10] Martin, A., "Mobile Device Forensics", SANS Institute, 2009.

[11] O'Malley, T.A., "Using Historical Cell Site Analysis Evidence in Criminal Trials in Obtaining and Admitting Electronic Evidence", United States Attorney's Bulletin, Volume 59, No. 6, pp. 16-34, 2011.

[12] Singh, R., Chourasia, K., and Singh, B., "Cellular Phone Forensics", International Journal of Scientific and Research Publications, Volume 2, No. 8, 2012.

[13] ISO/IEC 27043, "Information Technology, Security Techniques, Incident Investigation Processes and Principles Committee Draft", 2014.

[14] Raymond, E., and Venter, H.S., "Testing and Evaluating the Harmonized Digital Forensic Investigation Process in Postmortem Digital Investigation", Association of Digital Forensics Security and Law Conference on Digital Forensics, Las Vegas, Nevada, USA, 2014.