

# CDCD-5 an Improved Mobile Forensics Model

Vinit Shah<sup>1</sup>  
PG Scholar, IT Department,  
IET, Devi Ahilya University  
Indore, India  
viniengg@gmail.com

Dr. Pratosh Bansal<sup>2</sup>  
Asth. Professor IT Department,  
IET, Devi Ahilya University  
Indore, India  
pratosh@hotmail.com

**Abstract**—Mobile Technology is an exponential growing technology and making the world digital. Today mobile phones are easily available at cheaper rate for use of common people. Advancement in technology made mobile phone a portable computer. Criminals are using Mobile technology to perform crime. To investigate digital crime around the digital world various digital forensics models have been developed, and to trap such type of criminals forensics experts require a proper tool and proper model to collect evidence from it. Based on core concept of investigation a logically connected model is created. Scope of this paper is to describe a common model for mobile forensics investigation while performing analysis on mobile phone.

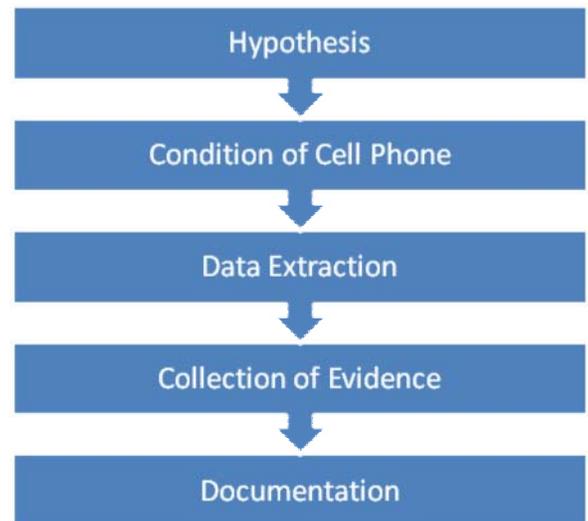
**Keywords**-Mobile forensics, digital forensics, cdc-d-5 model;

## I. INTRODUCTION

Mobile forensics is a branch of digital forensics in which investigator takes evidence from mobile phone. The forensics is a combination of art and science. Technology advancement makes mobile phone a compact size computer [1]. As compared to computer the memory of mobile phone is low and irrespective of this people are using it as personal data storage [2]. The role of mobile forensics tool is extract useful personal information from mobile phone which can be used as evidence in front of judicial authority. There are so many mobile company have their own standard, their own OS, SOCKET. Variety in mobile phone makes it difficult for investigator to investigate it [3]. There are 4-5 new models of mobile phones are launching per week, so it is very difficult to update the tool according to the new model of mobile phone and it makes mobile device forensics investigation is a new and challenging field among the law enforcement agencies and forensics experts [4]. A survey done by FBI (Federal Bureau of Investigation) says that “The use of Mobile phone in a crime is growing rapidly” [5]. To trap such type of criminals various Digital investigation model have been developed by various experts. The developed model is emphasis on core concept of investigation or technical aspect. This paper presents a mobile forensics model for investigation.

## II. PROPOSED MODEL

The Mobile phone forensics is a necessary part of solving crime cases. Each organization has developed its own model. This paper describes the model for mobile forensics investigation. The name of proposed model is **cdc-d-5**, and contains 5 phases as shown in [Fig-1]



**Fig 1. Proposed model.**

## III. DESCRIPTION OF MODEL

### A. Hypothesis:-

Hypothesis is the first and initial phase of any investigation. Hypothesis is a logical approach to solve a crime case. Investigator first understands the full crime scene and according to it prepares the list of evidence. After making the list investigator hypothetically relate the evidence and imagine the crime case. This phase is important because it is the first step of investigation procedure. Hypothesis creation is totally based upon previous experience. It is mandatory

because before starting investigation, investigator knows what evidence must be collected and he/she can choose the appropriate tool which will be according to mobile phone. The creation of hypothesis reduces time and cost and the case can be solved easily. This phase exactly give an idea to the investigator that what data is to be extracted.

**B. Condition of Cell Phone:-**

After hypothesis next phase is validating condition of cell phone to ensure that it is in a working condition or not. This is most important phase from where investigation is really started. In previous phase investigator has prepared list of evidence that are to be collected. In this phase investigator will select the procedure according to the condition (on/off) of cell phone. If the device is found in **ON** condition then collect data from software, and if the device is found **OFF** then don't turn it **ON** it may result change in volatile data.

Depending on mobile phone condition we can classify mobile phone in the following manners [4].

Name of Mobile Phone	Condition	Action
General Phone (Nokia , Samsung, LG)	ON	Do not turn it OFF. It may lock out the feature.
	OFF	Leave the device OFF. Turning ON could alter the device.
Blackberry Devices	ON	Turn the radio OFF.
	OFF	Leave it OFF.

**Table 1- Action taken according to condition of cell phone [4].**

**C. Data Extraction:-**

Data extraction process is the most important phase of investigation. In this phase investigator interact with mobile phones via (Software or Hardware).Technology makes mobile phone similar to computer. Mobile phone is having internal and external memory for data storage. There are so many tools available in market which extracts the data from mobile phone.

Evidence can be extracted from Mobile Phone are as follows:

- SMS Sent, Received.
- Call Logs (Received Call, Missed Call, Dialed No).
- Contact Stored.
- Drafts, Notes, Reminder.
- Internet History.
- Images, Application [3].

**D. Collection of Evidence**

Evidence is a physical proof of crime. Type of evidence depends upon the crime. Different type of crime requires different type of evidence. In this phase investigator use the list of evidence which was created in hypothesis phase. Investigator creates metadata of collected data.

Name of evidence	Information retrieved
Call No.(received, dialed)	Time of call, Duration of Call, Location of call,
SMS(Sent, Received)	Time of SMS
Contact	Known Person

**Table 2- Information retrieved with Evidence**

This information is retrieved with time and date. Investigator use time and date to create the evidence. After collecting the entire evidence investigator arrange evidence according their own priority.

**E. Documentantion:-**

Documentation is the next and important phase of model. In this phase evidence is arranged in the form of document, and it is presented in front of judicial authority. Document must be clear, concise, factual, and timely. Document is the summary of crime case with evidence which is a proof that crime was done by suspect or not [6].

The flow chart of CDCD-5 model is described here.

(fig-1). In future Mobile phone will be same as computer and required more data to be extracted thus **cdcd-5** model has a considerable great variety of future scope. An investigating expert may add some extra phase in model and can also use it for another digital device investigation.

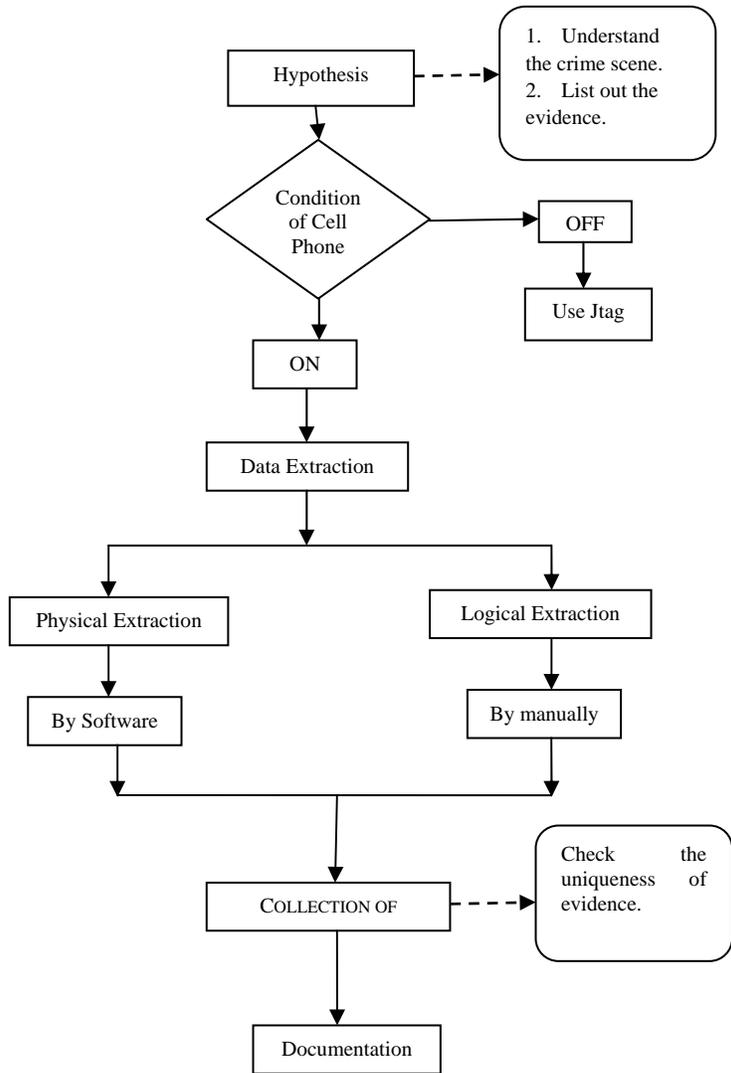


Fig 2: Flow chart of proposed model cdcd-5

#### IV. CONCLUSION

A new Mobile Forensics process model has been developed which emphasis on technical and core concept of investigation process. The **cdcd-5** is a standardizing process for mobile forensics investigation. The proposed model is starts working when an investigator is reported of a crime and ends while the evidences are submitted in to court. Like to solve any other Crime Cases, it is necessary to recover all the useful information from mobile phone and present it as a evidence. To successfully collect evidence from mobile phone investigator may follow the model. Common model of mobile forensics include hypothesis, condition of cell phone, data extraction, collection of evidence, documentation as shown in

#### REFERENCES

[1] Web reference: - [http://www.iceg.net/2008/books/2/34\\_312-323.pdf](http://www.iceg.net/2008/books/2/34_312-323.pdf)  
“Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective” by Rizwan Ahmed Rajiv V. Dharaskar [As Accessed on 20-DEC-11]

[2] Web Reference: - [http://en.wikipedia.org/wiki/Mobile\\_phone#In\\_general](http://en.wikipedia.org/wiki/Mobile_phone#In_general)  
[As Accessed on 27-JAN-12].

[3] Amjad Zareen , Dr Shamim Baig “Mobile Phone Forensics Challenges, Analysis and Tools Classification”  
Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering 2010

[4] Shivankar Raghav, Ashish Kumar Saxena “Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition” Student Conference on Research and Development (SCORED 2009), 16-18 Nov. 2009 Malaysia.

[5] Web reference: - <http://www.forensicfocus.com/downloads/windows-mobile-forensic-process-model.pdf> by Anup Ramabhadran “FORENSIC INVESTIGATION PROCESS MODEL FOR WINDOWS MOBILE DEVICES” [As Accessed on 4-MARCH-12].

[6] Web Reference: - <http://mobileforensics.files.wordpress.com/2010/07/cell-phone-evidence-extraction-process-development-1-1-8.pdf> “CELLULAR PHONE EVIDENCE DATA EXTRACTION AND DOCUMENTATION”