

# Tools and Techniques for Data Acquisition using available evidences in Mobile Forensics: A Survey

Prof. Dinesh Gawande<sup>1</sup>, Antara Raut<sup>2</sup>, Ashwini Hiranwar<sup>3</sup>, Devashri Gaikwad<sup>4</sup>  
Bhagyashri Ninave<sup>5</sup>

<sup>1</sup> Assistant Professor , Computer Science Engineering, DBACER, Nagpur, Maharashtra, India  
<sup>2,3,4</sup> Students, Computer Science Engineering, DBACER, Nagpur, Maharashtra, India.

## ABSTRACT

*In this paper we are trying to study various mobile forensic tools which are in use to reveal phone Mobile Forensic Artifact is a forensic software framework for extraction and decoding of data stored in electronic devices. In object-oriented systems a framework is defined "as asset" of classes that embodies an abstract design for solutions to a number of related problems for mobile Forensic tool framework the solutions are so called plug-ns for data extraction and data decoding and the problems are all related to forensic extraction and decoding of data stored in electronic devices .Mobile Forensic Artifact is a forensic software framework for extraction and decoding of data stored in electronic devices. In object-oriented systems a framework is defined "as asset" of classes that embodies an abstract design for solutions to a number of related problems for mobile Forensic tool framework the solutions are so called plug-ns for data extraction and data decoding and the problems are all related to forensic extraction and decoding of data stored in electronic devices.*

**Keyword :** - Key Digital Forensics, Mobile Forensics, Mobile Artefacts, Electronics Evidences, Data Analysis.

## 1. INTRODUCTION

Cybercrime , also called as computer crime, is any illegal activity that involves a computer or network connected device such as mobile phone. Mainly cybercrime is done in two categories, firstly crime in which computing device is the target and second is the crime in which computing device is used as weapon. Because of the fast pace of change of mobile device technologies and operating systems, there are times when a newer mobile device which is Unsupported or only partially supported by commercial mobile forensic tools for data extraction and parsing must be examined in the course of a criminal investigation, with the end goal being the extraction of digital evidence for use in court. In these cases, novel examination techniques must be developed and used, while still adhering to acceptable digital forensics process. It is an investigation and analysis technique to gather and preserve evidence from a particular computing/ mobile device in a way that is suitable for presentation in a court of law. The goal is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on that device and who was responsible for it.

## 2. RELATED WORK:

There are various tools which is used for extracting data in digital forensic. We discuss some of them below:

### 2.1 MOBILedit Forensic tool:

MOBILedit Forensic Express performs mobile phone content extractions and is used by professionals in law enforcement, military as well as the corporate and private sectors. By connecting a phone via USB cable, Wi-Fi or Bluetooth you can perform individual examinations of the majority of mobile devices available and generate reports in multiple formats (PDF, HTML, Excel, etc.) for a variety of needs. This tool can retrieve

messages, call logs, pictures, contacts, apps, calendar events, emails, passwords, media, file system, deleted data and much more. Specific data you want to extract from the device can be selected.



### 2.1.1 Connecting Phones

Connecting Android phones  
We use android phones here.

Connecting iPhones  
Connecting Blackberry phones  
Connecting Windows phones  
Connecting feature phones

### 2.12 Load report configuration:

To speed up the configuration of your report, you may use the configuration of a previous report as a template. The report configuration file is always automatically saved inside the report folder. To load it, simply click "Load report configuration" on the report type selection page, navigate to the report with the desired configuration, and select report\_configuration.cfg in its folder.

### 2.13 Features:

Physical data acquisition.  
Advanced application analysis.  
Retrieve deleted data.  
Beautiful reports.  
Password and pin breakers

### 2.14 Appearances:

MOBILedit has been designed for the most intuitive control possible. Most of components are based on contemporary usage standards. There is no extensive learning necessary to achieve complete control of the program. MOBILedit plugin based design potentially offers control of all current and future mobile phones and phone features.

### 2.15 Applications:

MOBILedit is designed with architecture similar to that of operating systems. The result is that you can add new applications and drivers, and in the same way that Windows or Linux resolves the complexity of computer hardware, MOBILedit reconciles the differences between mobile phones. MOBILedit supports adding applications to enhance its functionality for future phones and new features. For example, if a phone supports

MMS, one can add an MMS application to MOBILedit one can add the ability to edit, upload, or download pictures, control a camera and view movies.

In addition to applications, drivers can also be added, which cover the differences between mobile phones at a low-level. Therefore, any mobile phone can be supported. The driver interface is open, COMPELSON Labs offers the source codes of their drivers.

## 2.2 Oxygen Forensic tool:

Oxygen Forensic Detective is forensic software for data acquisition from mobile devices, their backups and images, memory cards, SIM cards, drones and cloud storages. The program has played a significant role in criminal and other investigations all over the world and is used by Law Enforcement units, Police Departments, army, customs and tax services and other government authorities. With Oxygen Forensic .Detective you can acquire and analyze:

- Common device information
- Contacts
- Missed/Outgoing/Incoming calls
- Organizer data (meetings, appointments, memos, tasks, notes, etc.)
- SMS, MMS, Messages, E-mails with attachments
- Photos, videos, audio files and voice records
- Geo coordinates stored in various sources
- Wi-Fi connections history
- Device logs
- Passwords to the device owner accounts and WiFi hot spots
- Deleted data (contacts, messages, calls, photos, etc.)
- Applications data from Android, BB 10, Apple iOS, Windows Phone 8 devices

### 2.2.1 CONNECTING MOBILE DEVICES

How To Connect Android Devices:-

#### Hardware and software you need for connection:

- Original USB cable
- Oxygen Forensic Detective installed on your PC
- Cable drivers from phone manufacturer
- Flash card compatible with the specific device (used as temporary storage when extracting data)

#### OxyAgent application usage notice

- Oxygen Forensic Detective offers 3 methods of data acquisition: Android backup, physical acquisition and logical extraction. In case of logical extraction
- OxyAgent application is installed in the device. Oxygen Forensic Detective installs and uninstalls OxyAgent automatically, so you don't need to perform any special actions about it.
- OxyAgent is a small forensically designed application that allows you to extract the maximum amount of data from Android devices. It does not change any personal information inside the device.

This is the method that works on any supported Android device. In case other methods fail this method will acquire at least the minimum set of data. OxyAgent has no access to the internal memory folders thus it won't return the internal memory files and won't recover deleted data. It will help to extract only contacts, messages, calls, calendar and files from flash drive. Software communicates with the Android device via ADB in order to

acquire data via logical method. You must make sure that proper drivers are installed for the ADB communication to occur. OxyAgent will be installed on the Android device. You must configure the Android device by enabling USB Debugging Mode before starting the software: Follow these steps:

Check whether the device is not locked with a passcode/pattern lock

- Enable USB DEBUGGING/STAY AWAKE in SETTINGS > APPLICATIONS > DEVELOPMENT menu
- Enable UNKNOWN SOURCES in SETTINGS > APPLICATIONS
- Make sure the memory card of minimum 512 Mb is inserted. OxyAgent will use that space to store temporary files. The temporary files will be removed after the extraction is finished.

### 2.2.3 SIM CARD EXTRACTION

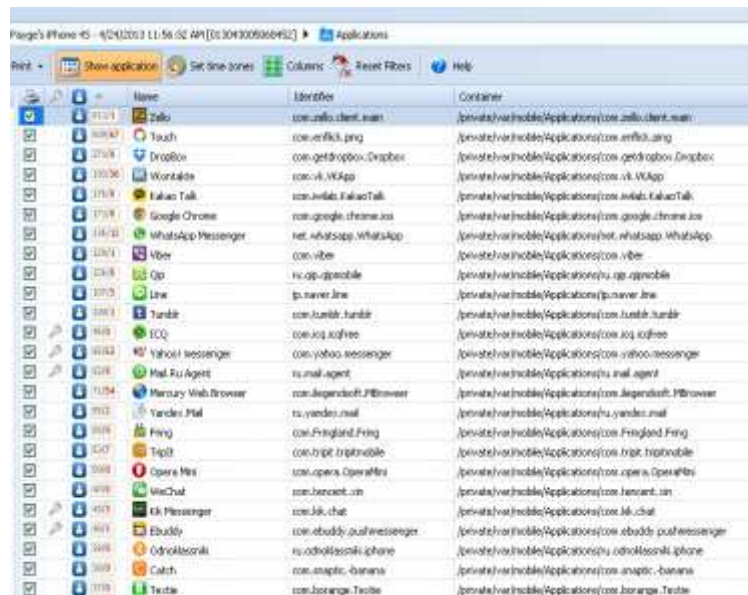
Oxygen Forensic Detective offers the ability to extract data from SIM cards via SIM card reader. Forensic experts can connect one or several SIM card readers that are compatible with Windows OS system. No special settings are required for connection. In case a SIM card is locked with a PIN code it can be entered in the corresponding window in Oxygen Forensic Extractor.



The program acquires both actual and deleted SIM card messages, contacts and calls. Once acquisition is completed you can view SIM card data together with other extractions in analytical sections, like Timeline or Social Graph.

### 2.1.4 APPLICATIONS

The Applications section shows detailed information about system and user applications installed in Apple iOS, Android, BlackBerry 10 and Windows Phone 8 devices. Currently we support 400+ unique applications and 5100+ app versions.



Name	Identifier	Container
Zello	com.zello.client.main	/private/var/mobile/Applications/com.zello.client.main
Touch	com.veriflick.png	/private/var/mobile/Applications/com.veriflick.png
Dropbox	com.getdropbox.Dropbox	/private/var/mobile/Applications/com.getdropbox.Dropbox
Wontable	com.vi.VKApp	/private/var/mobile/Applications/com.vi.VKApp
KakaoTalk	com.kakao.KakaoTalk	/private/var/mobile/Applications/com.kakao.KakaoTalk
Google Chrome	com.google.chrome.ios	/private/var/mobile/Applications/com.google.chrome.ios
WhatsApp Messenger	net.whatsapp.WhatsApp	/private/var/mobile/Applications/net.whatsapp.WhatsApp
Viber	com.viber	/private/var/mobile/Applications/com.viber
Qip	ru.qip.qipmobile	/private/var/mobile/Applications/ru.qip.qipmobile
Line	jp.naver.line	/private/var/mobile/Applications/jp.naver.line
Tumblr	com.tumblr.tumblr	/private/var/mobile/Applications/com.tumblr.tumblr
QQ	com.qq.kgfree	/private/var/mobile/Applications/com.qq.kgfree
Yahoo! Messenger	com.yahoo.messenger	/private/var/mobile/Applications/com.yahoo.messenger
Mail.Ru Agent	ru.mail.agent	/private/var/mobile/Applications/ru.mail.agent
Mercury Web Browser	com.legendsoft.PBrowser	/private/var/mobile/Applications/com.legendsoft.PBrowser
Yandex Mail	ru.yandex.mail	/private/var/mobile/Applications/ru.yandex.mail
Fring	com.Fringland.Fring	/private/var/mobile/Applications/com.Fringland.Fring
Tipit	com.tipit.tipitmobile	/private/var/mobile/Applications/com.tipit.tipitmobile
Opera Mini	com.opera.OperaMini	/private/var/mobile/Applications/com.opera.OperaMini
VicChat	com.fancient.com	/private/var/mobile/Applications/com.fancient.com
Kik Messenger	com.kik.chat	/private/var/mobile/Applications/com.kik.chat
Ebuddy	com.ebuddy.pushmessenger	/private/var/mobile/Applications/com.ebuddy.pushmessenger
Odnoklassniki	ru.odnoklassniki.iphone	/private/var/mobile/Applications/ru.odnoklassniki.iphone
Catch	com.anaptic.banana	/private/var/mobile/Applications/com.anaptic.banana
Textie	com.boranga.Textie	/private/var/mobile/Applications/com.boranga.Textie

Some applications of oxygen forensic are as follows:

- Social networks.
- Messenger
- Productivity
- Web browsers
- Navigations
- Travels
- Fitness
- Multimedia
- Spyware

### 3. CONCLUSIONS

In this paper we are studied various mobile forensic tools which are in use to reveal phone Mobile Forensic Artifact is a forensic software framework for extraction and decoding of data stored in electronic devices. In this research we show that caution must be taken when evidence is extracted. The conclusions provide a warning for professional practice and increased awareness for potential loss and spoliation of evidence when investigating cases using these tools.

### 4. REFERENCES

- [1] <http://www.oxygen-forensic.com>
- [2] <https://support.mobiledit.com/portal/kb/articles/getting-started>
- [2.1.2] <https://support.mobiledit.com/portal/kb/articles/load-report-configuration>
- [2.1.5] <https://support.mobiledit.com/portal/kb/articles/list-of-apps-for-android>.
- [2] [https://www.oxygen-forensic.com/download/articles/Oxygen\\_Forensic\\_Detective\\_Getting\\_started.pdf](https://www.oxygen-forensic.com/download/articles/Oxygen_Forensic_Detective_Getting_started.pdf)