Examination of data extraction and parsing in the course of criminal investigation by using "Phone Artefacts"

Prof. Dinesh Gawande[1],Antara Raut[2], Bhagyashri Ninave[3], Ashwini Hiranwar[4], Devashri Gaikwad[5]

[1]*Assistant Professor , Computer Science Engineering, DBACER, Nagpur, Maharashtra, India*
[2,3,4] *Students, Computer Science Engineering, DBACER, Nagpur, Maharashtra, India.*

ABSTRACT

We present Mobile Forensic (Android) Artifact finding. This is use for Mobile Forensic Investigation purpose. It is designed for collection, deciphering and analyzing data stored in all the ranges of handheld devices (Android). It enables the user to analyze data and intelligence from mobile handset (Android Mobile device). It retrieves Phonebook, SMS (read, sent, to be sent), Call History, Installed Application, File System, SIM Data and all possible data available in Mobile. 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. It is a software based solution for, complete with the necessary hardware for forensic investigations of mobile devices. It provides an intuitive and user friendly interface to analyze a wide range of mobile phones secure manner. The information gathered from the examined device is instantly available for review, ensuring its legal standing and credibility in a court of law.

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

1. INTRODUCTION

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. 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.

Technology is advancing at such a rapid rate that the suggestions in this guide are best examined in the context of current technology and practices. Each case is unique and the judgment of the examiner should be given deference in the implementation of the procedures suggested in this guide. Circumstances of individual cases and Federal, State, and local laws/rules may also require actions other than those described in this guide.

2. RELATED WORK

The introductory section has defined and described the characteristics of digital forensic. This section is concerned with the identification of evidence that may be found on a mobile phone. The opportunity to collect evidence from mobile phone is no different than any other digital forensic collection activity and it must comply with standardised criteria for acceptance.

CASE EXAMPLE: POCKET-DIAL M FOR MURDER

Ronald Williams killed his wife Mariama, apparently in a fit of rage after learning that she had an affair. Unbeknownst to Williams, his cell phone pocket-dialed his wife's cell phone during the crime and the call went to voicemail. The recording on his wife's voicemail captured him stating that he was going to kill her, followed by her screams and their 2-year-old daughter pleading with Williams to stop (Krueger ,2011).

2.1 REPORT GENERATION

Some forensic tools such as:

ASR Data's SMART Guidance Software's En Case Technology Pathways .Pro Discover Paraben's Psuite and Access Data's Forensic Tool Kit. The reports generated by these tools are normally collections of bookmarked. Evidence that you have noted during your investigation.

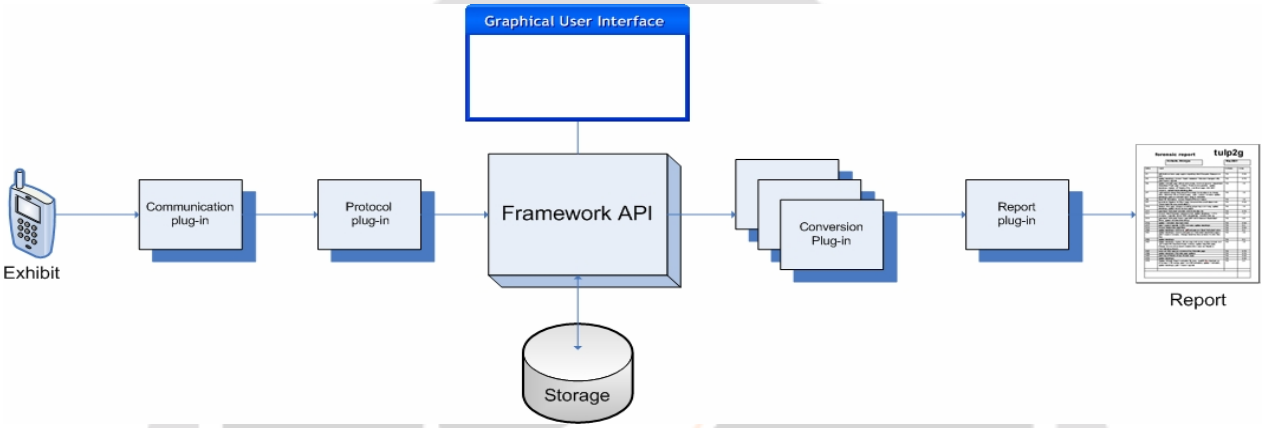


Fig: Method of report generation

2.2 Methodology for Digital Forensic Examination:-

a. Preparation
The original data obtained in the form of traces and logs are stored on a backup device like read only media. A hash of all the trace data is preserved. A copy of the data will be analyzed and the original network traffic data which is not alter by hacker

b. Detection
The presence and nature of the attack are determined from various parameters. A quick validation is done to assess and confirm the suspected attack.

c.Generation
Data are acquired and used to collect the traffic data. The amount of data logged will be enormous requiring huge memory space and the system must be able to handle different log data formats appropriately.

d.Examine
The traces obtained from various nodes which are integrated and fused to form one large data set on which analysis can be performed. There will be some issues like redundant information and overlapping time zones which need appropriation.

e.Analysis
The indicators are classified and correlated to deduce important observations using the existing attack patterns. The attack patterns are put together, reconstructed and replayed to understand the intention and methodology of the attacker.

f. Investigation
The goal is to determine the path from a victim network or system through any intermediate systems and communication pathways, back to the point of attack origination. The packet captures and statistics obtained are used for attribution of the attack.

g.Presentation
The observations are presented in an understandable language for legal personnel while providing explanation of the various procedures used to arrive at the conclusion. The conclusions are also presented using visualization so that they can be easily grasped.

3. WORK DONE

CASE STUDY ON MOBILedit FORENSIC :

We take one case study on MOBILedit forensic tool. It is solve by using this tool.

- From : abc police station
- Crime no. 124/17u/s
- Complainant name -xyz
- Accused name - pqr
- Date and place of the crime -25/07/2017 at DEF place
- Case history(data):
  subject: Blackmailing case and physical and mental torture through messages and calls.
- Exhibit details:
  (1) mobile (make :lava :-**imei no.- 35478##########,**
  (35479##########)

  (2) SIM card no.-775#####3

Above case was solved by using MOBILedit forensic tool

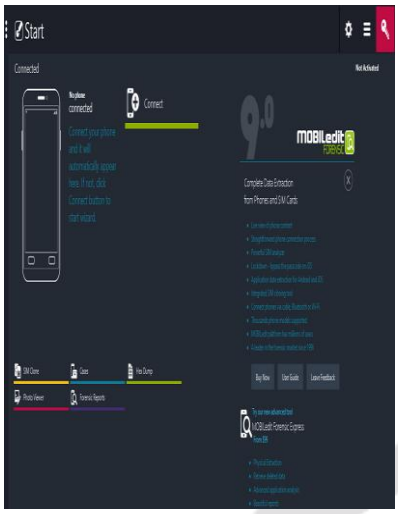


Fig: To connect mobile phone to the application

Fig: Choose connection option

Now above case study is solve by using Oxygen forensic tool

Fig : Connect the phone to the application

Fig: Detection of device connected via data cable

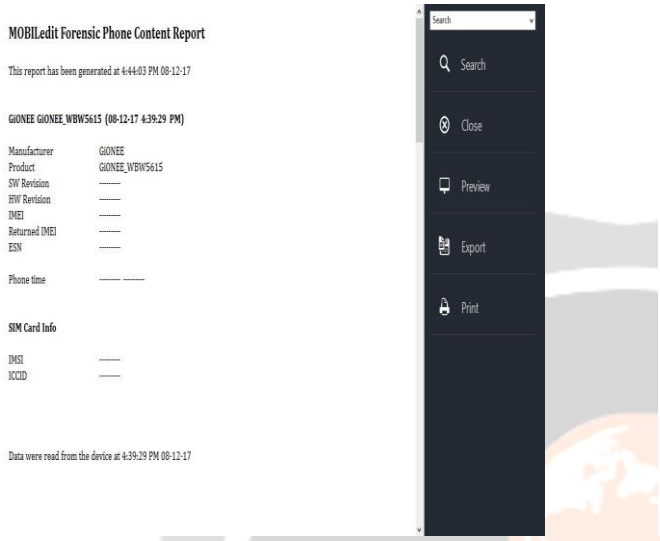
4. RESULT

This section provides guidance in preparing the report that will be submitted to the investigator, prosecutor, and others. These are general suggestions; departmental policy may dictate report writing specifics, such as its order and contents. The report may include:

- Identity of the reporting agency and case identifier or submission number.
- Case investigator and identity of the submitter.
- Date of receipt and date of report.
- Descriptive list of items submitted for examination, including serial number, make, and model and identity and signature of the examiner.

- Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files.

- Results/conclusions of the generated report.



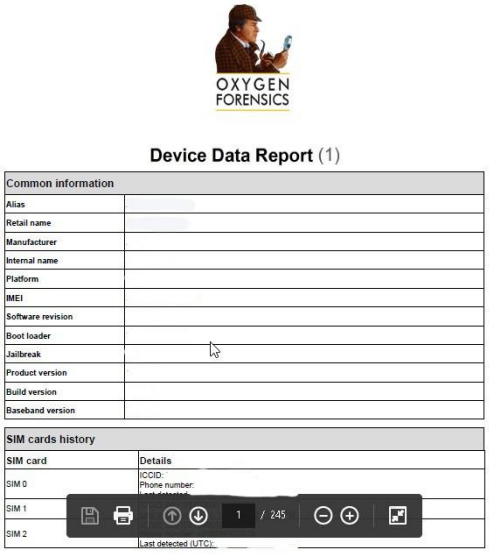


Fig : Report generated from MOBILedit tool is Fig: Report generated from Oxygen tool is

5. CONCLUSIONS

As we can see in this paper, more and more tools are available or developed to facilitate the digital forensic investigators to acquire the digital evidence from the devices. Some of the tools are very powerful to extract the information from and reduce the duration of evidence analysis. Besides the advancement in the digital forensic investigation tools, the methodologies or techniques developed to obtain the information also become more advanced.

6. REFERENCES

[1] https://en.wikipedia.org/wiki/Digital_forensics

[2]https://en.wikipedia.org/wiki/Mobile_device_forensics

[3] https://www.slideshare.net/RobertoEllis/digital-forensics-6106275

[4]http://resources.infosecinstitute.com/computer-crime-investigation-using-forensic-tools-and-technology/#gref

[5]https://booksite.elsevier.com/9780123742681/Chapter_20_Final.pdf.

[6]http://www.dataforensics.org/wifi-forensics/pdf

[7] https://www.ncjrs.gov/pdffiles1/nij/199408.pdf