International Journal of Software Engineering.
ISSN 0974-3162 Volume 11, Number 1 (2020), pp. 1-10

http://www.irphouse.com

A Comparative Study of Software for Data Recovery

Vijeta Bharti[1], Mr. Kiranbhai Dodiya[*], Dr. Shivani Pandya[**]

[1].M.Sc Forensic Science students Parul University Vadodara, India.

**.Ph.D. scholar department of biochemistry & Forensic science Gujarat University Ahmedabad, India.*

*** Head of the Department, Forensic science department, Parul institute of applied science, Parul University Vadodara, India.*

Abstract

Computer forensic has recently gained significant popularity with many local enforcement agencies. it's currently employed in fraud, theft, drug enforcement and almost every other enforcement activity. The research paper includes the categories of attempts to destroy or tamper the files by the culprits and unleashes various recovery techniques, and their significance in numerous situations from those attempts, which destroy files or inflict physical damage to the pc. The paper also presents the character and immediate need of enhancing the present automated forensic tools. The paper gives a fast glance of assorted methods utilized by culprits to destroy the data within the electronic storage media and their corresponding forensic approach done by the pc forensic experts within the perspective of recovery.

Keywords: Data Recovery, UFED Physical Analyzer, UFED Basic, Data Extraction…

1. INTRODUCTION

Information recovery approach retrieving misplaced, deleted unusual orinaccessible data that out of place for numerous reasons inclusive of device problem, terrible music of difficult disk, partition problem, documents loss, password loss and documents repair etc. Records healing now not most effective restores out of place documents however additionally recovers corrupted records. On the basis of diverse lost reason, we are able to adopt precise statistics recovery method. There are software program and hardware reasons that purpose information loss, at the equal time as we will get better facts by way of way of software program and hardware approaches. Being one in every of a kind from

prevention and backup recovers restoration is the remedial degree. The excellent way to make certain the security of your information is prevention and backup regularly. To characteristic and use your facts in keeping with the informative steps, you may reduce the danger of information loss to the bottom. Facts recovery is a technique of finding & convalescing information, wherein there may be a few threat, for now not all conditions can be expected or prearranged. Its method can be there will be some surprising things take place. So, you want lessen the danger in statistics healing to the bottom: backup all the data for your tough disk. Save you the system from being damaged another time. Prevent the system from being broken once more. Don't write whatever to the device on which you want to recover statistics.

Recovery Technique 1

The information recuperation from physically broken hardware entails one in every of a kind strategies. Some damaged can be repaired with the useful resource of changing of elements of tough disk and it's miles usable to a few increase but there may additionally however exist logical damages. To recover the photo from the floor if drives there use the specialized disk picture system, the image is then stored to reliable medium and the saved photograph is assessment for logical damages, which can also help in reconstructing the authentic picture or information. Far flung data healing 2 it's no longer essential to get right of entry to the broken hard pressure physically via way of the professionals however can be recovered via the usage of software program strategies; they may be used remotely with the use of diverse laptop at distinct vicinity through the net. Faraway healing wishes solid connection of bandwidth but remote healing isn't always relevant for those accesses to hardware. Stages of information recuperation three the data recovery has four stages, each phase's stands for special degree and range of statistics restoration competencies. Every section requires one-of-a-kind hdd restore equipment and statistics healing equipment to work with and each phase should made sure for the proper restoration. Section 1: repair the tough drives. Phase 2: picture the drive to new pressure. Phase three: logical recovery of documents, partition, mbr, and mft. Phase four: restore the broken documents that have been retrieved. Software of facts recuperation ufed simple 2

UFED FUNDAMENTALS CELLEBRITE MAKES CELL DEVICE PROOF EXTRACTION TO BE HAD ON TWO SYSTEMS:

The ufed touch, or the ufed 4pc the ufed 4pc is extraction software program that may be hooked up on any laptop platform, handy and securable inside the same manner as every other laptop primarily based software program application. The ufed touch includes standalone proprietary hardware, with the ufed software program installed on the microsoft windows embedded preferred 2009 platform. Users can only get entry to confined capability -shutdown, log on/off- and might't get entry to the windows strolling machine. The ufed touch & ufed 4pc interfaces structure are exactly the equal. Ufed software program is designed to execute handiest read instructions, and to prevent the possibility to regulate it to hassle write commands to cellular gadgets. Whilst the operator

need to report which platform, model, and extraction kind have been used, no other versions essentially exist amongst ufed touch and ufed 4pc extractions. Ufed operators have to additionally adhere to the same first-rate practices for each touch and 4pc systems that they do for any forensic laptop set up: isolate the forensic device from the internet at the identical time as performing forensic examinations. Don't keep digital proof on any pc that is or can be related to the net at any time. If performing an over the air software application replace, the operator ought to no longer simultaneously have an evidence tool or evidence storage related to the forensic tool. Extract mobile device proof to a garage medium especially designed and organized for that motive: a flash stress, outside tough force, a region on an internal forensic community, or internal strain or partition within the forensic pc. This manner, directors can manipulate who performs extraction based on their level of training, manner responsibilities, or distinctive "proper to apprehend, want to recognize" standards as laid out in their enterprise's guidelines or popular working tactics. Cellebrite encourages all customers who distribute cell evidence collection of their corporations to use ufed permission control. Statistics.

Extraction Type 3

Extraction kind 3

There are extraordinary strategies of mobile tool statistics extraction: logical (present records) and physical (a third extraction type the report gadget extraction, technically falls under the "logical" heading) specific data sorts, if they're supported for the tool, are to be had from each extraction category. In maximum instances, cell telephones are linked to the ufed tool thru a USB cable connection, which communicates with the smartphone to extract its information. The usage of a USB connection presents a tested dependable channel upon which to replicate statistics from evidence to the forensic image. Relying on the situation phone's OS, logical extractions can also as a substitute use USB/Bluetooth protocol APIs or, with older gadgets, serial protocols a good way to extract the facts. Operators should file which connection kind they used for every extraction. Within the uncommon times whilst the extraction fails, the person must in reality start the extraction over. The failure does now not affect the exceptional of integrity of evidentiary statistics due to the fact if handiest affects the transmission of statistics from the gadgets, no longer the statistics on the device. Logical extraction 1 logical extraction of records is executed, for the most part, through a designated API (software programming interface), available from the tool supplier. Just as the API allows business third birthday party apps to speak with the tool OS(operating machine),it also permits forensically sound records extraction. Upon connection, the ufed hundreds the relevant vendor API to the device. The ufed then makes examine best API calls to request statistics from the cellphone. The phone replies to valid API requests to extract distinct content objects such as text messages (SMS), phonebook entries, photographs, and so forth. In july 2011 cellebrite diagnosed the want for a quicker method of extracting records from ios devices. The pre-ufed contact hardware, the ufed traditional or ufed 36, should take many hours to perform those extractions. Cellebrite solved the hassle by means of implementing ios extraction inside its evaluation software program, ufed bodily

analyzer, as of version 2. 1. It's far viable for ios tool extractions to differ between the UFED Touch/UFED 4PC interface and the UFED Physical Analyzer.

That's because the UFED Touch/UFED 4PC obtains the Apple iTunes backup ("Advanced Logical") extractions possible.

Method 1 Like the UFED Touch, relies on the iTunes backup using Apple's backup infrastructure.

Method 2 Extracts backup data if the device is encrypted and the UFED operator does not know the device passcode.

Method 3 is recommended for both encrypted and unencrypted jailbroken devices.

How does the examiner know which method to choose?

The UFED Physical Analyzer interface automatically selects the appropriate extraction method-based on the device's backup configuration, jailbreak status, model, and iOS version-but the operator has the option to use other methods as well, and to combine the data sets. The interface explain which data is available with each extraction method. Users should document which methods they used and why they used it, when possible.

File System Extraction 2

Another logical method extends the examiner's reach to the phone's live partition. Available with the UFED ultimate license, a file system extraction uses different device-specific methods to copy the file system. While these are comparable to the API used in logical methods, they use different sets of built-in protocols, depending on the OS. The mix of protocols often differs from device family.

In some cases, not only with iOS devices as described above but also with Android and Blackberry models, it may be necessary to rely on device backup files to make available files, hidden files, and other data that is not necessarily accessible through the phone's API.

This can include some user deleted and hidden data contained within SQLite databases, including web history, email headers, EXIF data on images, and system data.

UFED Touch Logical 4

The UFED Touch Logical provides users with advanced investigative capabilities: Complete Logical Extraction of data from a wide range of devices such as: Blackberry, iOS, Android, Nokia, Symbian, Windows Phone, Palm and phones manufactured with Chinese chipsets SIM ID cloning which neutralizes the phone from any network activity during analysis and bypasses PIN locked SIM and missing SIM cards frequent updates to ensure compatibility with new phones as they are introduced to the market Analysis, report generation and customization using the UFED Logical Analyzer Field-ready, easy-to-use- no PC required for extraction Fully equipped mobile forensic kit with everything

you need for your investigation.

Targeted Data Extraction 4

Cellebrite's UFED Touch Logical, is a mobile forensic solution for the fast, logical extraction of data from a wide range of devices including: legacy and feature phones, smartphones, tablets and portable GPS devices. With its intuitive GUI and easy-to-use touch screen, the UFED Touch Logical solution immediately delivers forensically sound evidentiary data.

The solution includes:

UFED Logical Analyzer: A comprehensive analysis and reporting application

UFED Phone Detective: Instant mobile identification

UFED Reader: Enables the sharing of information with any authorized personnel, without limitation

The UFED Touch Logical is mission-ready for use in the field or lab and available in standard or ruggedized versions**.**

Forensic data extraction

The UFED Touch Logical has the ability to extract a vast amount of mobile data from the SIM and phone memory in a fast and simple process:

Apps data

Passwords

IM (instant messaging)

Phonebook contacts

SMS

MMS

Email

Calendar

Pictures

Audio/Music

Videos

Ringtones

Call logs

Phone details (IMEI/ESN)

ICCID and IMSI

SIM location information (TMIS, MCC, MNC, LAC)

GENERAL FEATURES OF UFED PHYSICAL ANALYZER SOFTWARE FOR DATA RECOVERY

It should provide users with all physical, file system and advanced logical extraction capabilities for different devices and different Operating Systems as well as allow extraction of cloud data source tokens accessed by the mobile phone with or without consent.

It should support more than 27,980 device profiles and 7590 different mobile application versions.

It should support management, upgrades and control from a centralized software.

The extraction software should be touch screen enabled, allowing easy use on tablets.

It should be operated with a USB software license dongle.

It should come with a compact and lightweight case with all necessary cables for the supported phones/OS.

It should support Data carving from unallocated space which enables to recover a greater amount of deleted data from unallocated space in the device's flash memory.

It should support the decoding of the iCloud backup and production set obtained from Apple devices.

It should enable Highlighting of the exact position for each decoded the analyzed data and the Hex.

It should enable using the Python shell to enhance the capabilities for content decoding.

It should be able to run Python scripts via plugins and edit and create new decoding chains.

It should support image carving, a feature used to recover deleted image files and fragments when only remnants are available.

It should support advanced location carving, by decoding more location data from unallocated spaces and unsupported databases.

It should perform on-demand searches for viruses, spyware, trojans and other malicious payloads in files.

It should allow decoding & conversion of BSSID values (wireless network) and cell ID values into physical location with map coordinates. This service should be available with in both online & offline mode.

It should support tagging of events using one or more labels via hotkeys.

It should be able to highlight platform for chat messages such as WhatsApp, Skype, Facebook Messenger, Azar and Telegram.

It should be able to decode powering events.

It should have a built-in SQLite Viewer.

It should have a wizard to visually map data from databases which are not automatically decoded by building queries.

It should be able to save the queries created by the wizard and then run them again when the same application is encountered in other extractions.

It should have a built-in tool for researching databases recovered as part of the investigation using Fuzzy Model.

It should be able to read report file generating using corresponding Cloud extraction solution.

It should be able to integrate with Active Directory for user authentication.

It should be able to match files extracted against Hash Databases and it should have built-in support for Project VIC & CAID hash databases.

It should be able to decode Google Archive Files.

It should be able to decode modified IMEI numbers for Android devices.

It should include the provision of a case id as well as other relevant case-related information as part of the extraction report and allow filtering based on specified data range.

It should enable visualizing of events over time, view distances between events and see the number of events within a defined timespan in a table.

It should enable conversion of single or multiple locations to their corresponding address.

It should support viewing of all locations on a single map.

It should enable viewing of extracted location using offline maps even without an Internet connection.

The offline maps should have an India version.

It should support the ability to highlight information based on predefined list of values.

It should support viewing of text files including file information, content, and Hex.

It should support quick search within decoded data.

It should enable viewing of communications between sources in data and time order.

It should enable quick reference pointer to set to analyzed data item and data file item.

It should support Hexadecimal view of the extracted data enabling advanced search based on multiple parameters, regular expressions and more.

It should enable the translation of foreign-language content from extraction to English. Translation should be possible from at least 5 language. If required, then at least 70+ languages should be available at additional cost.

It should be able to Generate and customize reports in different formats e.g. PDF, HTML, XML, Excel and Word.

It should enable Chat messages to be exported in conversion format, in PDF reports.

It should support Exporting selected emails to EML format.

It should support hash verification to ensure the extraction decoded is the same extraction received from the device.

It should be able to merge multiple extractions in a single unified report for efficient reporting and investigation.

It should be able to support file system extraction of blocked application data by downgrading the APK version temporarily for Android devices running on Android 6 and above.

Downgrading the APK should support shared data extractions, in addition to "no shared" data.

It should have the option to adjust the timestamp according to the time zone and offset setting on the device.

It should support extraction, decoding and media analysis from most popular drones from DJI with latest firmware's. it should also support the DJI Go app.

The software should provide additional security for protecting the reports. It should also allow to password protect the reports.

The software should provide a file format viewer which allows users to view, search and copy readable content from various file types like plist, bplist, etc.

The software should allow decoding of backups for MTK based Android phones.

The software should support physical extraction capability using the emergency download mode.

The software should provide lock bypassing physical extraction support for devices with Coolsand based chipsets.

The software should be able to produce powerful visual reports which should include conversation screenshots, locations on the map and extraction summaries.

The software should provide greater access to supported applications with the use Android emulator. It should allow examiner to simulate exactly how the data appears from a user perspective.

The software should allow examiners to automatically extract and preserver public domain data from lead cloud data sources such as Facebook, Instagram and Twitter.

The software should allow automatic decoding of data from .zip files.

The software should allow examiners to perform a quick selective extraction of selected applications without performing a logical, file system or physical extraction.

It should provide generic pattern/pin/password lock screen removal and bypass method for various models from leading vendors including Samsung, LG, Motorola, Sony, Xiaomi and others. It should support Android v6 and above with Full Disk Encryption and security patch older than August 2018.

It should provide a simple extraction flow with generic extraction for unsupported devices.

METHODOLOGY:

There are three different methods of mobile device data extraction:

Logical (existing data) and Physical (all data) File System Extraction (only deleted data), if they are supported for the device, are available from each extraction category.

Firstly, we select the appropriate model no. of phone in UFED software.

And go to the setting in mobile phone then USB debugging enable. For debugging enable, tap the developer option 7 times.

In cyber cases, mobile phones are connected to the UFED device via a USB cable connection, which communicates with the phone to extract its data.

As per requisition, we select extraction type from UFED: logical, physical and file system.

If required only existing data, then we are use logical extraction method.

Then mobile connect with UFED software with the help of appropriate data cable & go with UFED application, logical extraction as per application extraction and get raw data

RESULTS AND DISCUSSION

The aim of this research work is to propose to introduce most effective tools to analyze. During our practical work we find out that numbers of tools are available in market.

This research has compared the data recovery capabilities of five tools under identical conditions to assess the speed with which the tools complete the data recovery process and the extent of the variations between the tools in terms of the files recovered.

No two tools produced identical results, and no tool recovered all the files in a disk image ("all" is defined at the sum total of the distinct files collectively recovered by the tools). Of course, it is also possible that some files resident on the disk image were not recovered by any tool.

In this paper the techniques discussed plays vital role and each technique has its own advantages and draw backs. We also discussed the importance of recovery and how the data is been recovered. The delete from computer does not mean it is deleted from the hard drive and don't think it cannot be recovered.

FUTURE SCOPE

This work limited to digital devices. There are number of device available in market like pen drive, memory card, hard disk etc. and number of methods are available to investigate memory forensics which can be helpful to find out easy method to examine

digital to cyber forensic investigator.

ACKNOWLEDGMENT

I would like to express my special thanks of gratitude to my Head of Department Dr. Shivani Pandya for their able to guidance and support in completing my dissertation.

I would also like to extend my gratitude to the Mr. Kiran Dodiya Ph.D scholar department of biochemistry & Forensic science Gujarat University Ahmedabad and Mr. Rajesh Kumar for providing me with all facility that was require.

REFERENCES

[1] Ankita Gaikwad, "Restore Bin: Restoration on Android Device.," *International Journal of Computer Science and Information Technology Research* , p. 3, april 2015.

[2] F. Kausar, "NEW RESEARCH DIRECTIONS IN THE AREA OF SMART PHONE FORENSIC ANALYSIS," International Journal of Computer Networks & Communications (IJCNC) Vol.6, , p. 8, July 2014 .

[3] M. A.-H. a. A. AlShidhani, "Smartphone Forensics Analysis: A Case Study," International Journal of Computer and Electrical Engineering, Vol. 5, No., p. 5, 6, December 2013.

[4] R. Lohiya, "Survey on Mobile Forensics," International Journal of Computer Applications (0975 – 8887)Volume 118 – No., p. 6, 16, May 2015.

[5] "https://www.magnetforensics.com/," [Online]. Available: https://www.magnetforensics.com/.