Desktop Application for Android Forensics

Xtracto

By

Ibrahim Hassan

Umar Mahmood

Hashaam Khalid

Shoaib Razzaq

Supervised by:

AP Waleed bin Shahid (Dept. of IS)

Submitted to the faculty of the Department of Computer Software Engineering,

Military College of Signals, National University of Sciences and Technology, Islamabad,

in partial fulfillment for the requirements of B.E Degree in Software Engineering.

June 2022

In the name of Allah, the Most Beneficent, the Most Merciful

CERTIFICATE OF CORRECTNESS AND APPROVAL

This is to officially state that the thesis work contained in this report

"Xtracto - Desktop Application for Android Forensics"

is carried out by

Ibrahim Hassan, Umar Mahmood, Shoaib Razzaq and Hashaam Khalid

under my supervision and that in my judgement, it is fully ample, in scope and excellence, for the degree of Bachelor of Software Engineering in Military College of Signals, National University of Sciences and Technology (NUST), Islamabad.

Approved by

AP Waleed Bin Shahid

Dept. of IS

Supervisor

Date: _____

DECLARATION OF ORIGINALITY

We hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification in either this institute or anywhere else.

ACKNOWLEDGEMENTS

Allah Subhan'Wa'Tala is the sole guidance in all domains.

Our parents, colleagues and most of all supervisor, AP Waleed bin Shahid.

The group members, who through all adversities worked steadfastly.

Plagiarism Certificate (Turnitin Report)

This thesis has 12% similarity index. Turnitin report endorsed by Supervisor is attached.

_____

Ibrahim Hassan

00000243564

_____

Umar Mahmood

00000261701

_____

Hashaam Khalid

00000281397

_____

Shoaib Razzaq

00000278774

_____

Signature of Supervisor

ABSTRACT

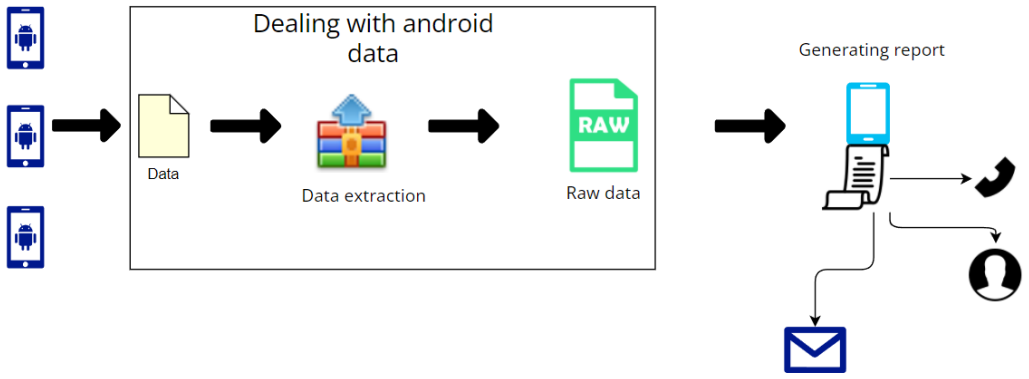
Xtracto is a desktop application for Android Forensics. It provides its users the functionality to extract and report data from an Android device found at the crime scene after connecting it with a windows PC. It covers various data forms and file formats. It has an interactive user interface which displays all the details and information extracted from the device. When data is extracted from an Android, it's in raw form which is difficult to decipher for a user. Xtracto takes this data and transforms it into an easy to understand and concise report for the user. It converts raw data to human readable form. Both the data files and the report are stored in an output folder on the forensic workstation (the PC). Users can also view and analyze previously extracted data from past cases and can view those former reports.

Table of Contents

CHAPTER 1: INTRODUCTION

1.1 Overview

With the dawn of the digital age, the means of communication and the information storage has changed drastically. Same can be said about the data acquisition technologies and methods used for different devices. With the advent of newer technologies, digital forensics, especially mobile forensics have gained traction in the technological domain. We live in an age where crucial information is stored in a device the size of the palm of our hand. Our daily life communication is done using mobile phones, most of them having Android OS. With every subsequent newer version of Android, data acquisition is becoming harder than ever before. Acquiring data, presenting it in a human-readable form, training forensic investigators to make efficient use of the tools available, deciding the best tools for a particular case, worrying about evidence tampering and keeping track of the newer versions of Android is a tedious and cumbersome process. Xtracto frees you of all these concerns by providing a full package of proprietary level services in an open-source tool.



The diagram above describes the general workflow of data extraction and reporting in Xtracto. Raw data is extracted, converted to human-readable report and data is stored in the forensic workstation.

1.2 Problem Statement

Pakistan has not kept up with the everchanging and evolving world in the field of digital forensics and does not have its own indigenous Android forensic tool. All the commercial tools are imported and expensive and with increasing crime and modernization of communication, mobile phones have become the primary source of communication for various people. Thus, a lot of useful and potentially critical information can be recovered from the android phone/s found at crime scenes. To put it simply, the major issues Pakistan is facing in this regard are:-

1. There is no indigenous forensic tool in Pakistan.
2. The commercial tools are expensive
3. Need better training of forensic investigators to make more efficient use of the tools at hand

1.3 Proposed Solution

The major goal of Xtracto is to aid the law enforcement authorities in the process of forensic investigation of digital evidence found at the crime scenes and provide them with an easy-to-use tool for data extraction from an android device, to make the cumbersome process of data extraction smooth and streamlined and to present it in a clear and concise report to the user. Xtract provides a cheap and readily available solution by providing the full package in an open-source tool.

1.4 Working Principle

The project mainly works on the principles of digital forensics amalgamated with data acquisition techniques. The project is divided into different modules and every module is inter-woven with the next module. The list of modules is as under:

- Data extraction
- Data reporting

- Integration
- GUI presentation

1.4.1 Data extraction

An integral part of the project is the extraction of data from the Android. The data comprises of images, videos, documents, audio files, messages, call logs, contacts, device info like IMEI, sensor info etc. and installed apps. This module is of pivotal important in our project.

1.4.2 Data reporting:

This phase involves converting the raw data to an easy to understand, human-readable report which is stored in a directory of the forensic workstation (PC to which the Android device is connected). The report is saved in .pdf format.

1.4.3 Integration:

The different modules are integrated in one stand-alone entity. This stand-alone entity is our application which is essential for a compact solution.

1.4.4 GUI presentation:

The visual demonstration of the project is done through the aid of GUI (graphical user interface).

1.5 Objectives

1.5.1 General Objectives:

"To build a desktop application that will be used to extract data from an Android device and present it in a clear readable form to the user containing only the important information extracted from the device using forensic techniques of Data Acquisition and Data reporting."

1.5.2 Academic Objectives:

- Development of a forensic android tool for data extraction and report generation.
- To implement the techniques of Android forensics and data acquisition
- To implement knowledge of creating a user interface.
- To implement the different coding techniques and skills that we learned thus far.
- To increase productivity by working in a team
- To design a project that contributes to the welfare of society

1.6 Scope:

Xtracto will have a country-wide scope as a digital forensic tool for law enforcement agencies. It is a cost-efficient forensic tool that will be available to all law enforcement agencies to make crime investigation streamlined and more efficient. Xtracto is a user-friendly, open-source tool that gives concise reports of potential evidence extracted from the Android devices in no time

1.7 Deliverables

Tasks	Deliverables
Literature Review	Literature Survey and Feasibility Analysis
Requirements Specification	Software Requirements Specification document (SRS)
Detailed Design	Software Design Specification document (SDS)

1.8 Overview of Document

1.8.1 Purpose:

This document covers detailed review of all major steps involved in Software Development Life Cycle (SDLC), Each chapter covers a single step of SDLC and goes from Software Requirement Specification, Software Design Specification to Software Test Plan & Strategy. These all-involved steps acted as guide to the development team and now shall provide insight to the reader that how prototype idea was formulated and then how hardware integration took place, how software was designed and finally tested.

1.8.2 Headings:

- Headings are prioritized in a numbered fashion, the highest priority heading having a single digit and subsequent headings having more numbers, per their level.
- All the main headings are titled as follows: single digit number followed by a dot and the name of the section.
- All second level subheadings for every sub section have the same number as their respective main heading, followed by one dot and subsequent sub heading number followed by name of the sub section.
- Further subheadings, i.e. level three and below, follow the same rules as above for numbering and naming.

1.8.3 Figures:

All figures in this document have captions and are numbered. All Software Design related diagrams are based on latest UML standards.

1.8.4 References:

All references in this document are provided where necessary, however where not present, the meaning is self-explanatory. All ambiguous terms have been clarified in the glossary at the end of this document.

1.8.5 Links to web pages:

All links have been provided with underlined font, the title of the web page or e-book is written at the top of the link and the title may be searched on google to pinpoint to the exact address.

1.8.6 Basic Text

All other basic text appears in regular, size 12. Every paragraph explains one type of idea.

1.8.7 Intended Audience and Reading Suggestions

The intended audience for this Document includes the project supervisor, "***Xtracto***" syndicate, BE CSE 24, UG project evaluation team, and other stakeholders at CSE Department, MCS.

For better understanding, the document is divided into chapters

- In chapter 1 an Introduction to Document and System is provided.
- Chapter 2 covers the literature review
- Chapter 3 covers the requirement specifications part and covers Functional, Non- Functional Parts Requirements, resources required, and constraints involved
- Chapter 4 contains the Design Specifications which provide an in-depth view of how the system is developed and how the functionalities are distributed.
- Chapter 5 covers the conclusion
- Finally, in chapter 6, recommendations towards future work are made.

This document is intended for:

1.8.7.1 Developers: (Project Group)

To be sure that they are developing the right project that fulfills the requirements provided in this document.

1.8.7.2 Testers: (Project Group, Supervisor)

To have an exact list of the features and functions that must respond according to requirements.

1.8.7.3 Users:

To get familiar with the idea of the project and how to use/respond in failure situations and suggest other features that would make it even more functional.

1.8.7.4 Project Supervisor: (AP Waleed bin Shahid)

This document will be used by the project supervisor to check and guide the group about the understanding and implementation of the requirements properly and completely during the development lifecycle.

1.8.7.5 Project Evaluators: (CSE Dept. MCS)

To know the scope of the project and evaluate the project throughout the development for grading.

1.9 Relevant Sustainable Development Goals (SDGs)

With “Xtracto” we strive to tackle these two SDG’s in particular: -

- **Industry, innovation, and infrastructure (PRIMARY)**

As mentioned before, Pakistan’s progress in the field of digital forensics is less than ideal to say the least. There is not a single forensic tool which is made by any Pakistani developer or organization. “Xtracto” will pave the way for such tools and encourage others to make similar products so that Pakistan and its law enforcement agencies can slowly catch up to the rest of the world in this regard. With “Xtracto” the forensic tool industry will finally have the vision to see what it really needs and it will start work on developing a holistic suite of products to provide it.

- **Peace, Justice and strong institutions (SECONDRY)**

The main demographic of “Xtracto” are the law enforcement agencies. Using “Xtracto”, investigation teams can better review digital evidence such as android phones found on the crime scene and with the proper analysis of the report generated by “Xtracto”, they can find the culprits thus making sure such people don’t roam about and disturbing the peace of our society and then the law can justly deal with them. This will hopefully reduce the number of unsolved cases and make the investigation process much smoother and faster.

1.10 Structure of Thesis

Chapter 2 contains the literature review

Chapter 3 contains the system requirement specification.

Chapter 4 highlights the Software Architecture and Data Design.

Chapter 5 contains the conclusion of the project.

Chapter 6 highlights the future work needed to be done for the commercialization of this project.

CHAPTER 2: LITERATURE REVIEW

Our team did thorough research on existing products similar to ours and contemplated on how to make it unique and better. We looked at the current situation in our country and its market for such an application. Literature review is an important step for development of an idea to a new product, a detailed study regarding all similar projects is compulsory. Our research is divided into the following points.

- Industrial Background
- Existing solutions and their drawbacks

2.1 Industrial background

Day by day, the rate of crime is on a steady increase in Pakistan. In this current digital era that we live in, the main method of communication between criminals is their personal devices whether it be their mobile phones or some other device. In Pakistan, there are no forensic tools that would help the law enforcement do their job efficiently in the face of a forensic crime investigation. The law here still relies on old methods of investigation.

Which is why Pakistan is in dire need of tools such as “Xtracto”. Digital Forensic tools can help make the investigation process much more time efficient. Especially in investigation or criminal cases, time is of the essence. Every second counts and those seconds could be reduced by a forensic tool which will help in acquiring important data faster.

Digital forensic tools are a means of protection against crimes such as breach of privacy, Blackmailing, Sexual harassment, Money Laundering etc.

The most important technical development in digital forensics is the development of computer forensics tools. Forensic tools have made the job easier for all investigation teams, the data acquiring, inferring and analyzing that used to take days can now be done in minutes or hours. It is an essential tool to have at your disposal for any team in any law enforcement agency. Most of

the different digital forensic tools that are now in market also make sure to keep the original file intact and preserved so that after data is recovered, extracted or acquired from the devices, a comparison can be made with original data to check and verify that there is no tampering or contamination.

This is how the investigation process will go:-

The examination method includes the classification of various violations. After the crime is characterized, examination begins on the Android device, the specialists start their work on that piece of the gadget that is found, so during the examination of the Android device there is high chance of catching the guilty party or suspect. First, they will extract and acquire all possible data from the Android device found on the crime scene. After that, they will have to get rid of all irrelevant data and only focus on the data that will aid them in their case against the culprit. The need to have the remaining data in a readable, concise report so that it can be analyzed with ease and after that they will present the data to their experts so that they can further analyze and infer information regarding the culprit which will help them in the future. After that, all that is left is to catch the culprit. With the use of forensic tools, this can be done in no time.

In Pakistan, there is not a single tool whether it be free or paid for extracting data from a mobile especially not deleted data. Because of this, essential evidence which could prove to be groundbreaking for a case remains uncovered and criminals escape the hand of law.

2.2 Existing solutions and their drawbacks

Following are some well-known forensic tools: -

- **Autopsy: -**

  Autopsy is a digital forensics application for both Desktop and Linux based systems. It is a graphical interface component of a much larger Sleuth Kit and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate about the activities on a device [1].

  The major drawback of Autopsy is that it has a steep learning curve, especially for new users and is harder to use compared to other graphical tools.

- **X-Ways Forensics: -**

  X-Ways Forensics is as a commercial suite of proprietary software available in the market used for digital forensics. It is an integrated computer forensic software which contains WinHex Disk Imager [2]. It provides complete results and is user friendly.

  The only drawback of X-Ways is its expensive price, being a commercial tool.

- **ADB:**

  ADB (Android Debug Bridge) is an open-source and perhaps, the most basic forensic tool available for android devices. It does not have a user interface but can perform complete logical extraction including device gallery, documents and even call logs and contacts using content providers

- **Andriller:**

  Andriller is a python based graphical tool that extracts data logically from an android device. It can also unlock the Android if it knows the hash of the password.

- **XAMN:**

  XAMN is the leading proprietary tool in digital forensics. It has a graphical, user-friendly interface. It can bypass the security of the device, get access to it and extract information. It can even extract deleted data, location information and has a facial recognition feature. The only drawback is that it's expensive compared to all the other tools in the market

- **AccesData FTK**

  AccessData FTK is the major provider of forensics tool training and certification internationally. Over 130,000 governing bodies and law firms use FTK around the world. It can perform analysis on laptops, personal computers, network communications and mobiles. Filtering and searching on it is faster than any other tool available [3].

- **Encase: -**

  Created by guidance software, Encase is one of the most used forensic tools in the world. 90% of the consumer goods companies around the world, 93% of the banks, 100% of the federal agencies, 75% of the power distributors and 80% of the Universities in the U.S. use Encase [4].

- **Digital Forensic Framework (DFF): -**

  This is an Open-Source forensics platform which is developed on a customized Application Programming Interface. Mostly used by the law enforcement agencies, educational institutions and private companies around the world. It is available in three options as DFF which is free, DFF Pro: 1,000€ for one-year support and DFF Live: 1,300€ for one-year support. DFF free will not get any professional support, report editor, automation engine, user activities reporting, hash scanner and skype analysis when compared with DFF Pro and DFF Live [5].

DRAWBACKS

The major problem with all these products though is that: -

- Most of them are not free of costb, none of them are local.
- Even those that are free such as Autopsy are extremely difficult to operate.
- They are all foreign tools.

“Xtracto” being a Pakistani tool will be much cheaper and more convenient for the law enforcement agencies of Pakistan to use. The learning curve for “Xtracto” will be steeper than that of the products above.

CHAPTER 3: SYSTEM REQUIREMENT SPECIFICATION

This section describes the development of Xtracto; the frontend, backend, technologies used for each and system requirements. It also explains the general working of the application; how it starts, extracts data, and generates a report.

3.1 Product Perspective

The main idea behind the project is to make the investigation process in a crime scene more effective, efficient and quick while preserving the cost efficiency of the product at the same time. Open-source tools provide partial and inconclusive results. Moreover, they don't provide reporting and much of the data extracted is inconclusive and can't be used as evidence. Commercial tools address all these issues but are very expensive. The main aim of this project is to create an indigenous forensics tool that is effective, efficient, cheap and provides conclusive evidence along with reporting.

3.2 Product Functions

The main features of our product will be the following:

1. The application will give nine extraction options depending on the type of data the user wants to extract.
2. The application will provide an option to formulate a report of the extracted data

3.3 User Classes and Characteristics

3.3.1 Summary of User Classes

The following section describes the types of users

- **Data Extraction Application:** The product will be used for data extraction where it will be used by investigation agencies to find leads pertaining a case.

3.4 Operating Environment

3.4.1 Hardware

Windows PC as a forensic workstation: The PC will be connected to the Android device via a data cable to extract data

Android Device: The Android will be connected to the PC to extract data.

3.4.2 Software

- Microsoft Windows

3.5 Design and Implementation Constraints

This software does come with its own design and implementation constraints:

- The product will not be compatible with some of the latest Android versions that have new security patches to prevent data extraction.

3.6 User Documentation

The user will be able to use the following as guide for using the software:

- User Manual that contains textual and pictorial help for users in guiding them to use the software correctly and troubleshoot it.

3.7 Assumptions and Dependencies

The product will need calibration for successful operation and new calibration will be required to redo the setup.

3.8 External Interface Requirements

3.8.1 User Interfaces

The front-end user interfaces will have the following main screens available to the user:

- **Launch Screen:** Once the application is started, the first page that is displayed is the launch menu which gives a prompt that the device is connected/not connected correctly and that everything is ok and the application is ready to start.
- **Main Menu:** This is the main menu of the application; it will show different extraction options that have been deployed in the system and are ready to use.

3.8.2 Hardware Interfaces

- A windows PC will be required as a forensic workstation to extract data from the target device
- An Android device will be required from which we are extracting the data

3.8.3 Software Interfaces

- **Python:** We will be using python programming language because its more interactive support to our project.

- **Visual Studio Code/PyCharm:** We will use Visual Studio Code as a platform to run our python scripts and JavaScript programs.
- **Operating System:** Windows for its user-friendliness and compatibility

3.8.4 Communications Interfaces

- **NCAT:** A networking interface used to communicate between the target Android device and the forensic workstation; the PC.

3.9 Screen Objects and Actions

Home screen: Home screen consists of 3 components:

- Navigation bar
- Connection component on right side bar
- Content screen.

Navigation Bar: Navigation bar have all the option that user will need to navigate throughout the program. It has buttons to navigate to different components and screen of the program.

Some options provided on navigation bar are:

- **Home button:** it will take user to home screen from wherever user is.
- **Raw data:** it will take user to screen to view raw data of a previous project or current project.
- Report button will take user to screen to view report.

Connection component: This component has a button to check if device is connected or not. If device is connected it will change the status button to connected and take the user to extraction screen.

If devices are disconnected this will change the status to “not connected” and take the user to home page screen where user can select from previous projects to view.

Content screen: Both Navigation and connection component will remain same for all the screens of the program. Changes will be shown in content screen according to the screen user is on.

- Under not connected status it will contain option to select from the previous projects.
- Under connected status, it will contain the extraction page. And options for extraction.

Report Screen: Report screen will have options for viewing the parts of reports separately. Battery button will show the details of battery extracted from the raw data. Device button will show the device details and system info will show the system info extracted from the raw data.

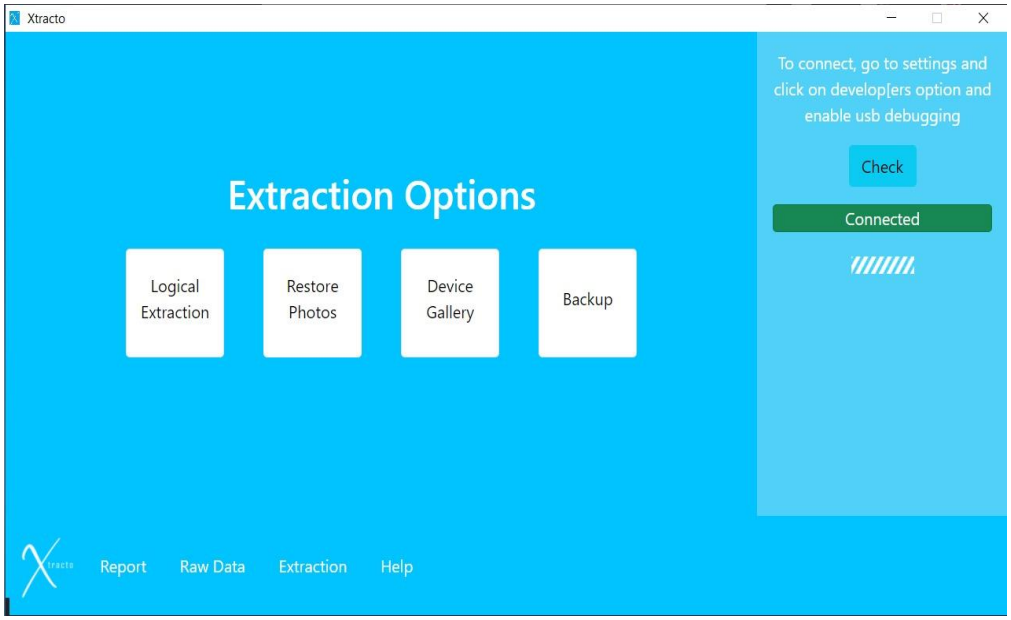
Raw Data screen: It will show all the raw data that was extracted from the android device in a console. Back button will take to the previous page where the user was.

Help screen: It will show the instructions to use the program and how to connect the device. Back button will take to the previous page where the user was.

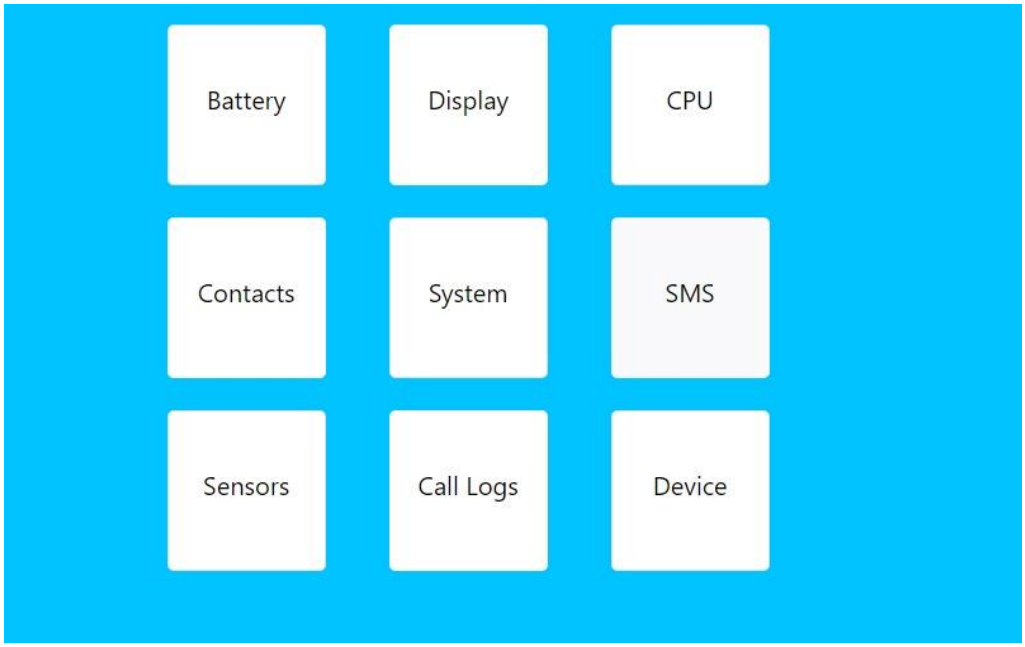
The frontend of the application is developed using ElectronJs. It is a component-based design that sits well with our type of application with multiple different modules.

This is the home screen showing that the device is connected, followed by displaying multiple extraction options

3.10 User Interface Images



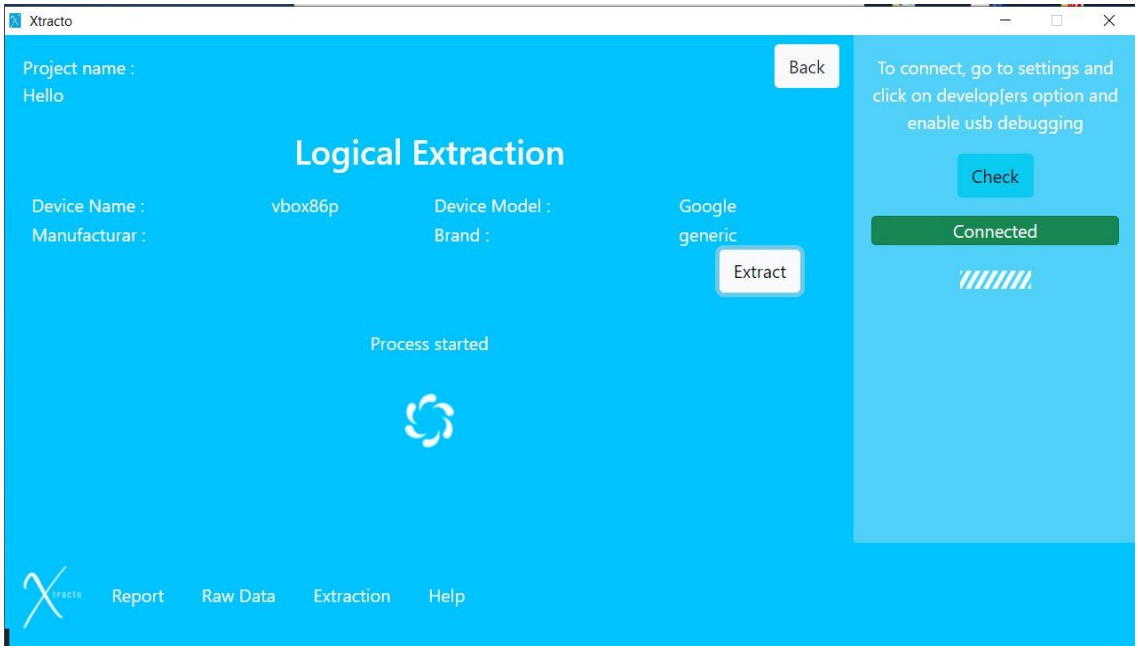
Below are the different kinds of info that can be extracted from the device:



This includes information regarding the battery, display information and CPU specification which are all some basic information, but it also shows the contacts stored on the phone, call logs consist of all calls done by the user in the history of the mobile phone and SMS consists of all messages

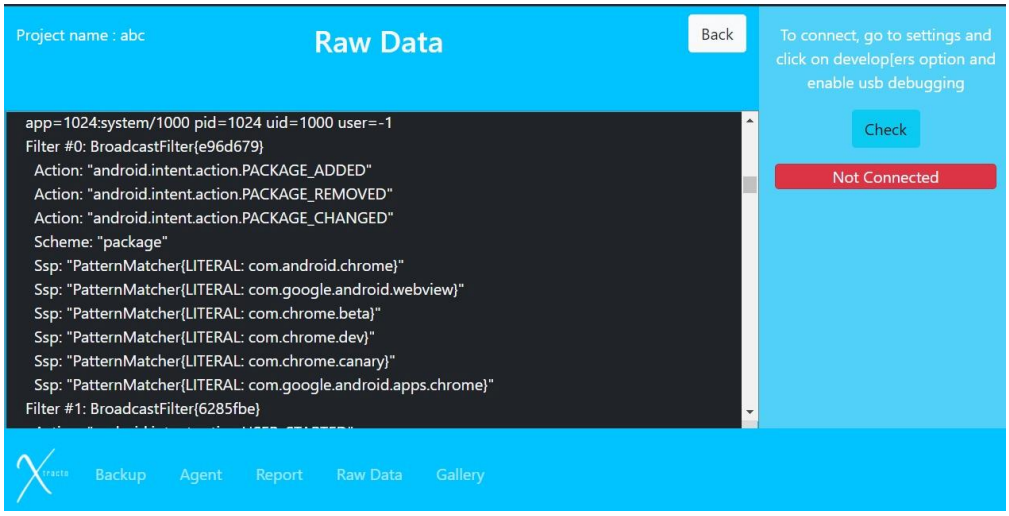
sent and received by the user of the phone. Now, keep in mind all this includes deleted data as well such as deleted logs, messages etc.

When you start extraction, the following screen appears:



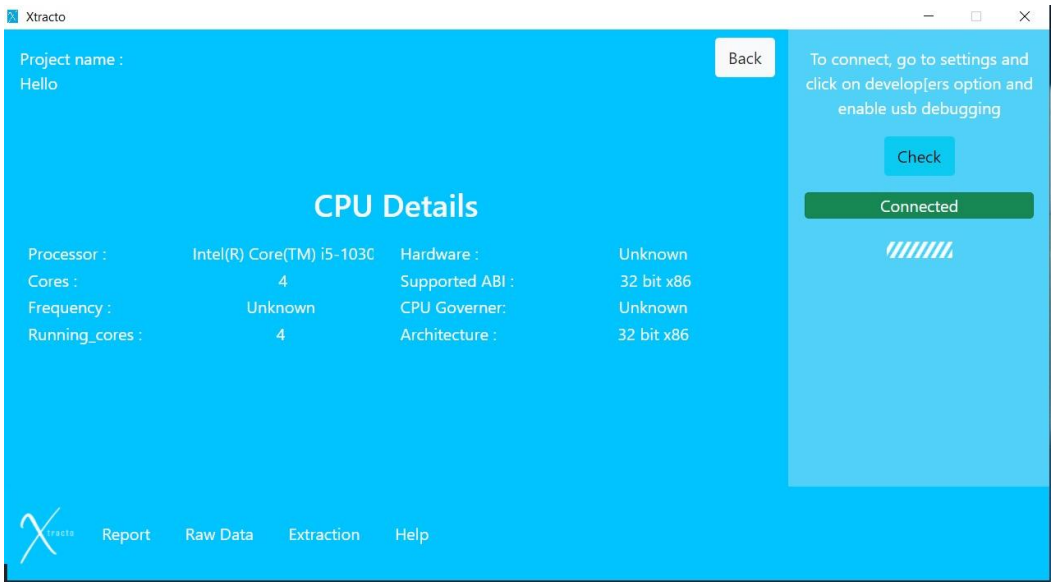
This will take about five minutes. The application is extracting all important data from the Android phone including the deleted data in this step.

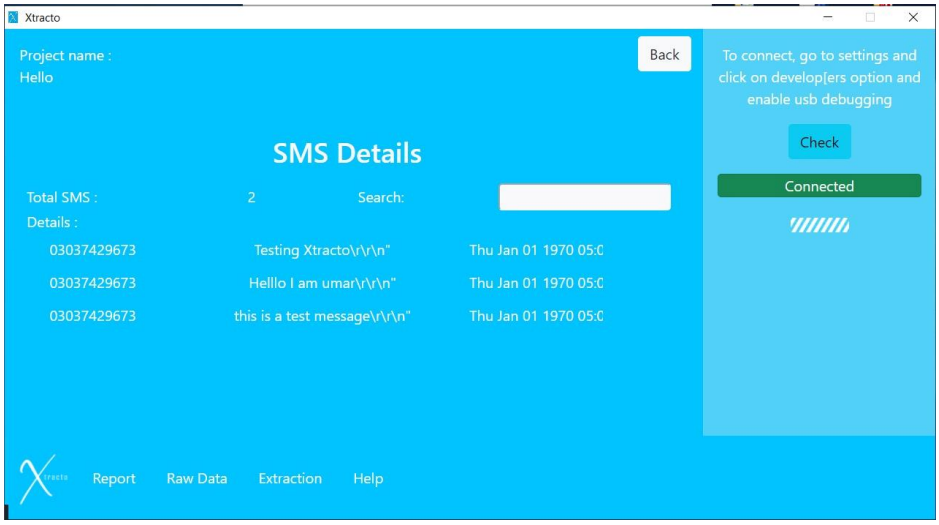
Below is a snapshot of how raw data is shown:



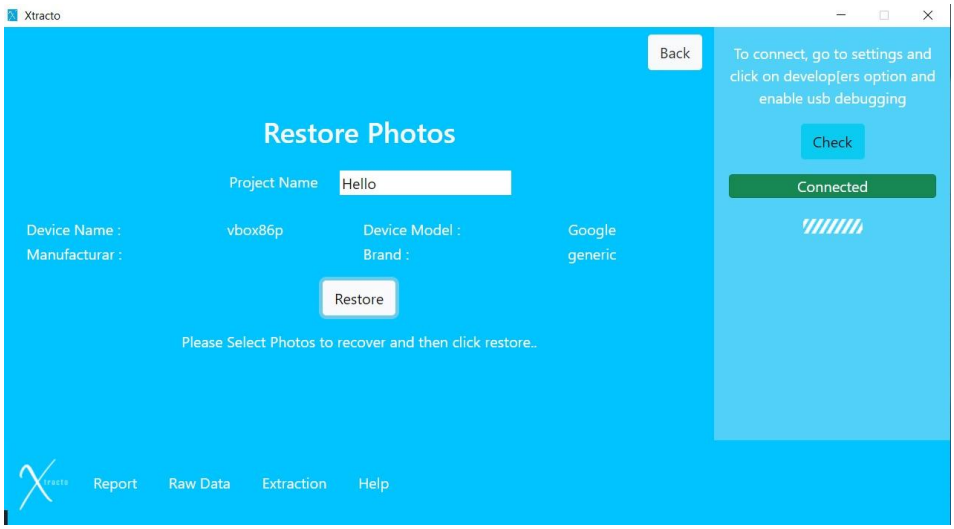
After data is extracted, most of it is useless redundant or irrelevant data to the user. This type of data is incomprehensible and useless for the user of the application. This is where the report generation aspect of the application comes in handy. The application automatically judges which data is going to be useful and only displays that data to the user in the form of a finalized report.

Some general images of the result are given below. The details of device info are displayed on the UI as follows:





Deleted photos can also be restored using an agent. This agent was an APK developed in Android Studio which is controlled by the main desktop application.



For an investigation team, the photos and videos stored in the Android device could prove quite essential for solving the case. “Xtracto” has the feature to recover even the deleted photos from the device. This is done using an Agent which is installed in the device. The Agent works on recovering the deleted bits of the data and reforms them into proper images again. These deleted photos are then displayed to the user.

Figure 1 The agent shows option to restore photos

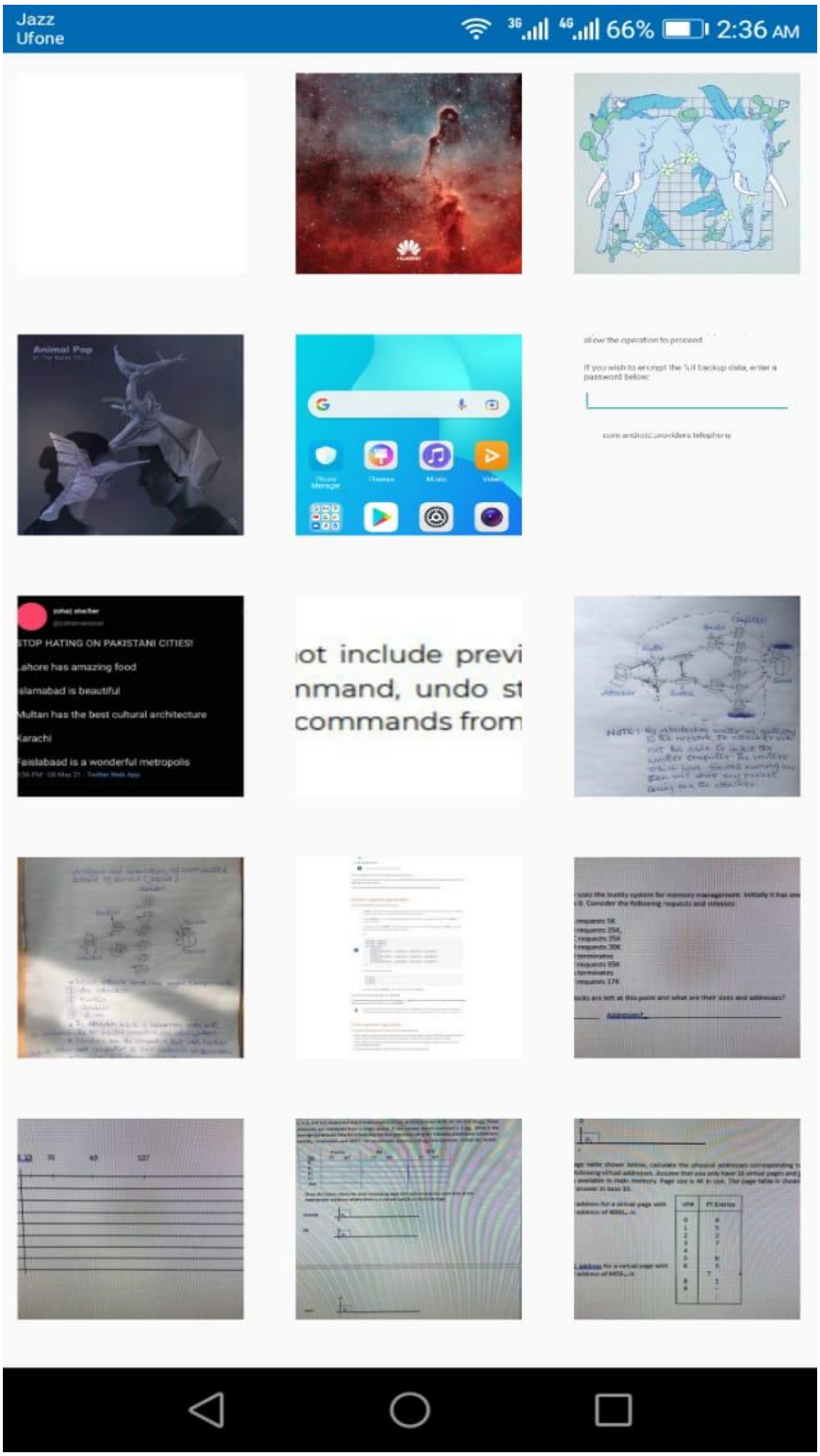
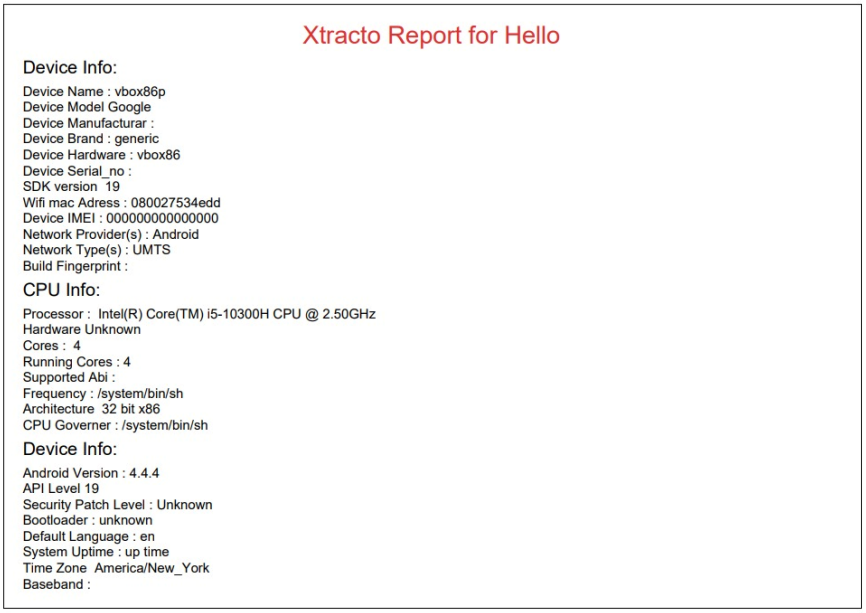


Figure 2 The agent then shows all the images from which the user can select the ones he wants to restore

Now, the question is where this report is stored or saved. This report is saved on the hard drive of the desktop using this application, it is saved in “PDF” format so that it is easy to open and read. Following figure shows the PDF report that the application generates and saves on the PC:



Xtracto Report for Hello

Device Info:

Device Name : vbox86p
Device Model Google
Device Manufacturar :
Device Brand : generic
Device Hardware : vbox86
Device Serial_no :
SDK version 19
Wifi mac Adress : 080027534edd
Device IMEI : 000000000000000
Network Provider(s) : Android
Network Type(s) : UMTS
Build Fingerprint :

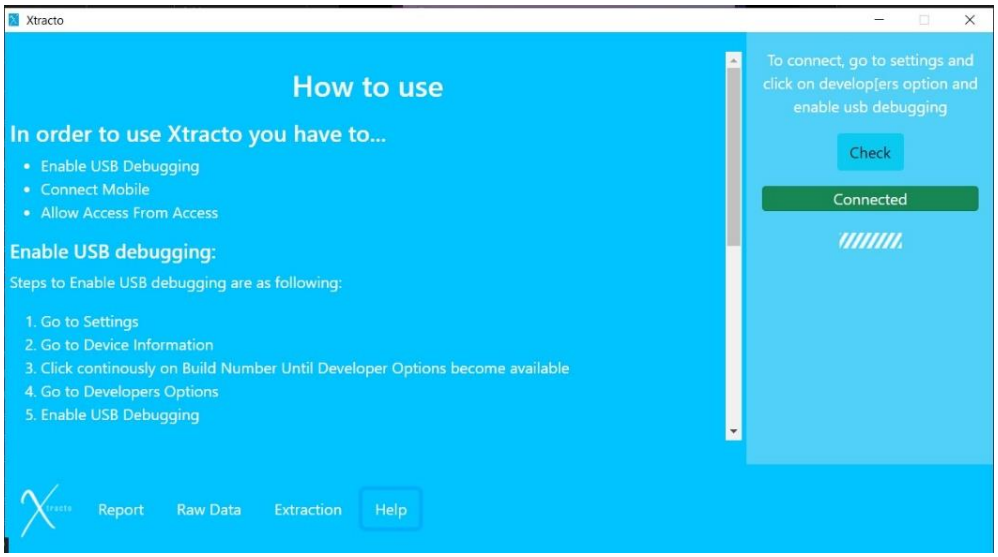
CPU Info:

Processor : Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz
Hardware Unknown
Cores : 4
Running Cores : 4
Supported Abi :
Frequency : /system/bin/sh
Architecture 32 bit x86
CPU Governer : /system/bin/sh

Device Info:

Android Version : 4.4.4
API Level 19
Security Patch Level : Unknown
Bootloader : unknown
Default Language : en
System Uptime : up time
Time Zone America/New_York
Baseband :

Also, we have to make sure that “Xtracto” is a user-friendly application and easy to pick up so that anyone using it could perform its functions without much difficulty, which is why there is a help manual in the application that can easily be accessed. A user manual in ‘Help’ tab is also included to assist users navigate their way on how to use the application



CHAPTER 4: SOFTWARE DESIGN SPECIFICATION

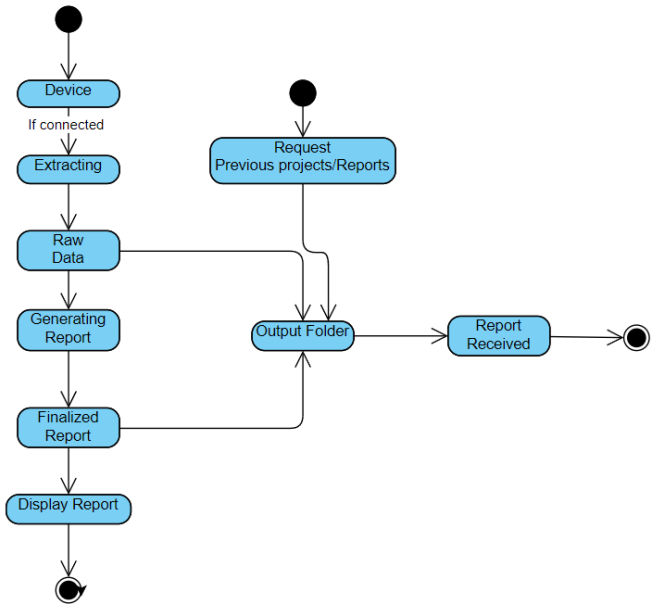
4.1 Architectural Design

This program uses main and sub-program architecture from call and return architecture design.

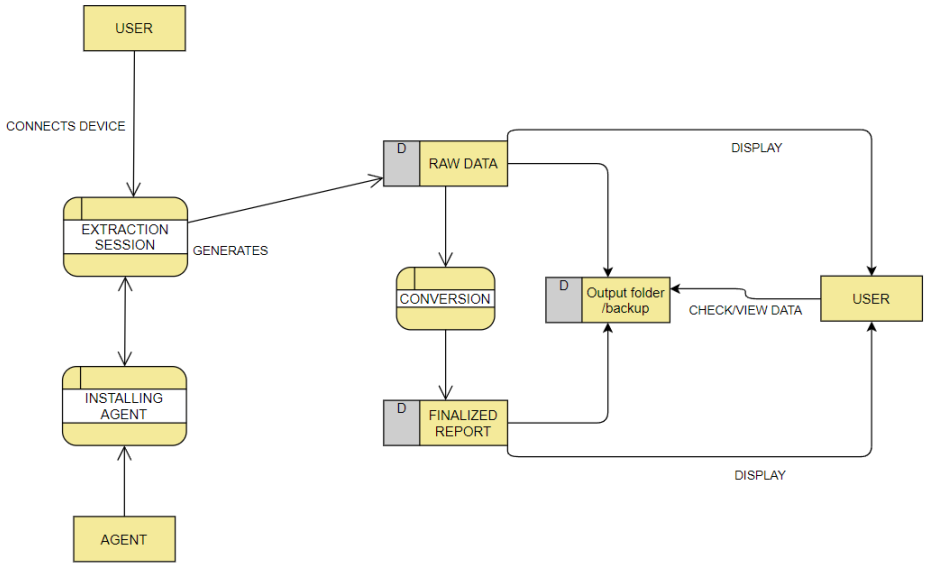
Main program is further divided into subprograms, and they are triggered by the main program. Sub programs include fetching data from the android phone, extracting useful data from the extracted raw data, generating concise report from the data, viewing raw data and viewing previously generated data reports.

Let's look at the architecture of the tool. For better understanding, have a look at these diagrams below. Blocks are subprograms for the main program.

4.1.1 State flow Diagram



4.1.2 Decomposition Description



User connects the android device to the system. If the connection is successful, then data is extracted with the help of an agent. Raw data is collected through this method which is then converted into a report (clearer and necessary data is separated from useless data) which is then stored in an output folder and displayed to the user. The user can view and check up on previous projects whenever he wants.

4.1.3 Design Rationale

Some of the reasons for choosing the Main and subprogram architecture are given below:

1. In Main and subprogram architecture, Program is divided into smaller pieces hieratically so it's easy-to-understand flow of data.
2. It's easy to modify a single subroutine without disturbing functioning of the overall program.
3. Scaling is easy. Adding new subroutines is not difficult and do not alter the flow of the whole

program.

4. It allows us to reuse components.

Layered architecture is another option for the same program, but it will be very complex to maintain and scale the program. Adding new features to the program will become very inefficient. We plan to add more features as we develop the program, so it is not a best fit for us.

4.2 Data Design

4.2.1 Data Description

Our system takes all the data from the android as a raw form that are string of data and send it to home component of the program. This string data is converted to arrays and then processed according to needs. A copy of raw data is also saved in output directory under case name directory in form of string for further use. All the processing is carried out on arrays and then output is used as suited data type.

4.2.2 Data Dictionary

Data used in our program is described with their type below:

- Connection: Boolean (used to tell if device is connected or not)
- Project: string (used to tell if some project is selected, if selected what is its name)
- Raw data: string (fetched from the android in this form)
- Device Name: string (Extracted from raw data)
- Model: string (Extracted from raw data)
- Manufacturer: string (Extracted from raw data)
- Device: string (Extracted from raw data)
- Board: string (Extracted from raw data)

- Hardware: string (Extracted from raw data)
- Brand: string (Extracted from raw data)
- IMEI: int (Extracted from raw data)
- Hardware Serial: int (Extracted from raw data)
- SIM Serial: int (Extracted from raw data)
- SIM Subscriber: int (Extracted from raw data)
- Network Operator: string (Extracted from raw data)
- Network Type: string (Extracted from raw data)
- Wi-Fi Mac Address: string (Extracted from raw data)
- Build Fingerprint: string (Extracted from raw data)
- Public IP address: string (Extracted from raw data)
- Local IP address: string (Extracted from raw data)
- Android Version: int (Extracted from raw data)
- API Level: int (Extracted from raw data)
- Security Patch Level: int (Extracted from raw data)
- Bootloader: string (Extracted from raw data)
- Build Number: int (Extracted from raw data)
- Baseband: string (Extracted from raw data)
- Java VM: string (Extracted from raw data)
- Kernel: string (Extracted from raw data)
- Default Language: string (Extracted from raw data)
- Root Access: string (Extracted from raw data)
- System Uptime: int (Extracted from raw data)
- Processor: string (Extracted from raw data)
- CPU Architecture: string (Extracted from raw data)

- Supported ABIs: string (Extracted from raw data)
- CPU Hardware: string (Extracted from raw data)
- CPU Governor: string (Extracted from raw data)
- Number of Cores: int (Extracted from raw data)
- CPU Frequency: int (Extracted from raw data)
- Running Cores: int (Extracted from raw data)
- Resolution: string (Extracted from raw data)
- Density: int (Extracted from raw data)
- Font Scale: int (Extracted from raw data)
- Physical Size: string (Extracted from raw data)
- Refresh Rate: int (Extracted from raw data)
- HDR: string (Extracted from raw data)
- HDR Capabilities: string (Extracted from raw data)
- Brightness Level & Mode: int (Extracted from raw data)
- Orientation: int (Extracted from raw data)

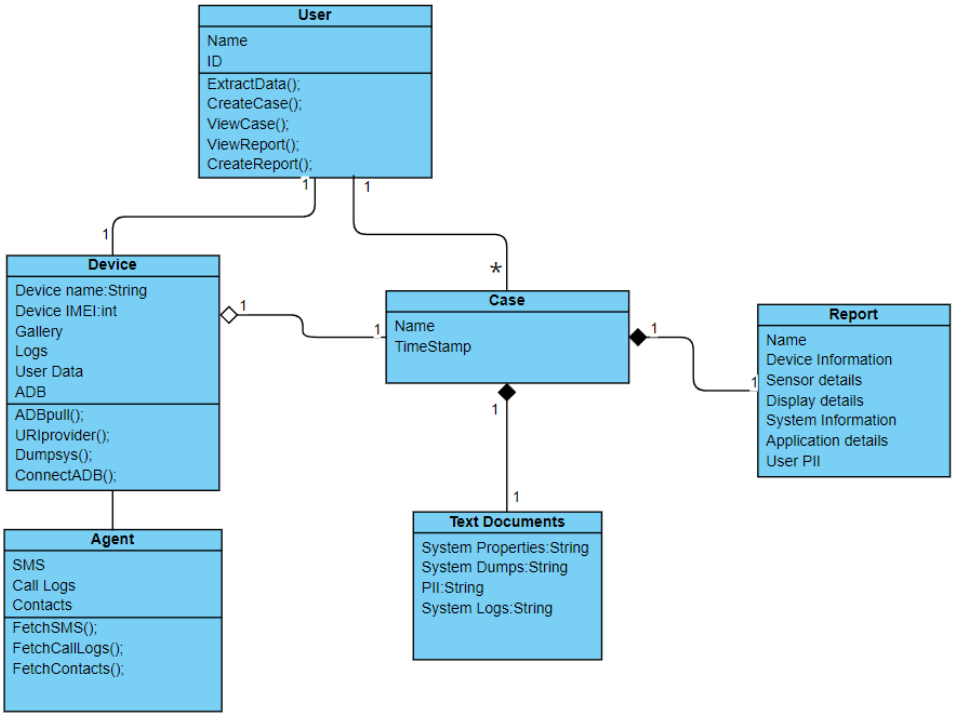
Major functions described in 3.2 and their parameters are given below:

- Extract: project name
- Show report: project name
- Create report: Raw data and project name
- View raw data: project name

4.3 Component Design and Interaction

For optimal functioning of the application, the individual and various components of the system must be working at their best and their interactions should be going smoothly. Let's look at how the components interact with each other.

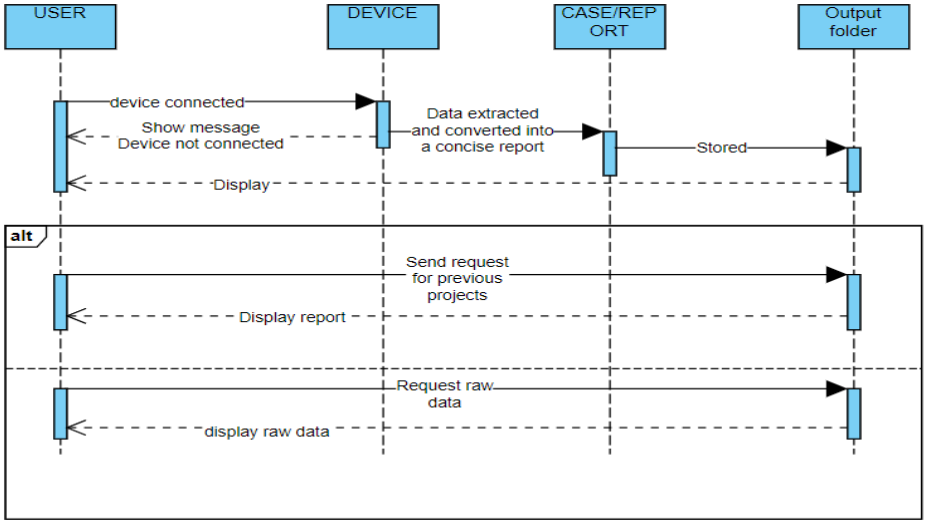
4.3.1 Class Diagram



From the class diagram, we can take a closer look at individual components of the software and how they relate to each other. We can also specifify what kind of relations they have with each other.

4.3.2 Sequence Diagram

We saw the general overview of the relation between different components in the class diagram but lets take a better look at the sequence of events and actions that take place between those components in the sequence diagram.



4.3.3 Use Case

USE CASE NAME	1-Genreate case report
SCENERIO	To generate a clear and concise report of the extracted data from the device
ACTOR	User
PRE-CONDITION	Raw Extracted data should be available.
POSTCONDITION	Report consisting of the necessary and useful data required by the user
DESCRIPTION	The main purpose of the software is to provide the user a report of extracted data from the device while excluding all the useless and irrelevant information.
ACTIVITY FLOW	➢ Connect the Device to your system. ➢ If successfully connected, use the extract option to start the process.

	➢ After the data is extracted, the software automatically generates the report and displays it to the user.

USE CASE NAME	2-View case report
SCENERIO	Old case reports are viewed through the backup.
ACTOR	User
PRE-CONDITION	There are previous projects saved.
POSTCONDITION	User checks and analyses the project. Specific case is selected.
DESCRIPTION	Previously generated reports are available in the backup. User can go through them and check for any information he wants.
ACTIVITY FLOW	➢ Click on Project on the main menu of the software. ➢ Select Project from the drop-down menu. ➢ Details of that project including SMS, logs and contacts etc. are displayed.

USE CASE NAME	3-View raw data
SCENERIO	Raw data instead of the finalized report can be seen.
ACTOR	User
PRE-CONDITION	There are previous projects and data saved.
POSTCONDITION	User checks and analyses the raw data.

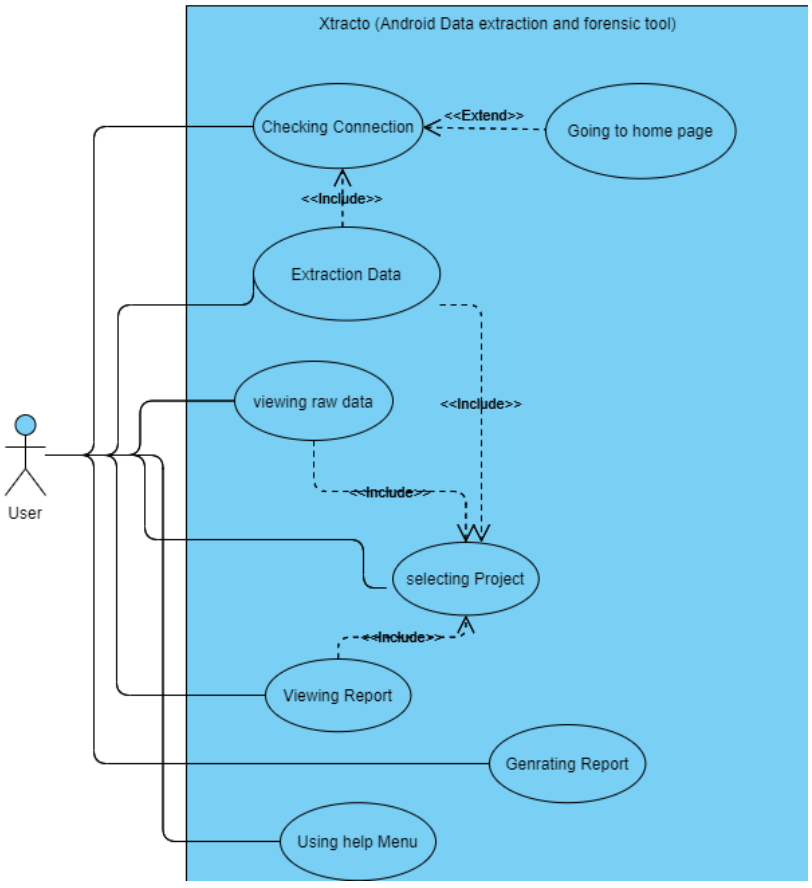
DESCRIPTION	Previously generated reports are available in the backup. User can go through them and check for any information he wants.
ACTIVITY FLOW	➢ Click on the raw data button on the main menu. ➢ Select the Project from which the raw data is to be shown. ➢ Entire Raw data of that device will be displayed on the page.

USE CASE NAME	4-Check Connection
SCENERIO	Check if Android device is connected to application or not.
ACTOR	User
PRE-CONDITION	NIL
POSTCONDITION	User should know status of device. i.e., Connected, Disconnected or unauthorized.
DESCRIPTION	System will check for the connected device and tell the user if it is connected.
ACTIVITY FLOW	➢ Click on Check button on right side bar. ➢ A Success button will say connected if device is present and authorized or disconnected otherwise.

USE CASE NAME	5-View help Menu
SCENERIO	To get instructions of how to use this tool or connect device.
ACTOR	User

PRE-CONDITION	NIL
POSTCONDITION	User should see a help menu to use this tool.
DESCRIPTION	System will provide a brief help on how to use it and how to connect device to the system.
ACTIVITY FLOW	➢ Click on Help button on navigation bar, ➢ A help screen will appear in content component with all the instructions.

4.3.4 Use Case Diagram



4.4 Requirements Matrix

4.4.1 Functional Requirements

REQ-1: Application shall be installed properly.

REQ-2: If the system is correctly booted:

- A prompt is displayed that tells you that the system booted up correctly.
- An ‘OK’ button to move on to the next screen.

REQ-3: Application shall boot up properly.

REQ-4: Different options that are available:

- A list of extraction options is shown to choose from.
- Help menu.
- Exit option.
- Home button

REQ-5: The application will extract data from system apps including contacts, messages and gallery (videos, photos).

REQ-6: Application will extract device info including details about sensors, battery and display details.

REQ-7: Application will extract all the system properties including SDK version, Android version, language etc.

REQ-8: The application is able to detect if the device is connected.

REQ-9: The application provides option to enter the target extraction directory.

REQ-10: The application allows the user to choose an extraction method.

REQ-11: The application will enlist the following data on the screen to the user:

PII

- Call logs
- Contacts
- Messages
- Device data
- Accurate Location

Device Details

- Device Name
- Model
- Manufacturer
- Device
- Board
- Hardware
- Brand
- IMEI
- Hardware Serial
- SIM Serial
- SIM Subscriber

- Network Operator
- Network Type
- Wi-Fi Mac Address
- Build Fingerprint
- Public IP address
- Local IP address

System Details

- Android Version
- API Level
- Security Patch Level
- Bootloader
- Build Number
- Baseband
- Java VM
- Kernel
- Default Language
- Root Access
- System Uptime

CPU Details

- Processor

- CPU Architecture
- Supported ABIs
- CPU Hardware
- CPU Governor
- Number of Cores
- CPU Frequency
- Running Cores
- GPU Renderer
- GPU Vendor
- GPU Version

Battery Details

- Health
- Level
- Status
- Power Source
- Technology
- Temperature
- Voltage
- Capacity

Display Details

- Resolution
- Density
- Font Scale
- Physical Size
- Refresh Rate
- HDR
- HDR Capabilities
- Brightness Level & Mode
- Orientation

Memory Details

- RAM
- ROM
- Internal Storage
- External Storage

Sensors Details

- Sensor Name
- Sensor Vendor
- Type
- Power

Apps Details

- User Apps
- Installed Apps
- App Version
- Minimum OS
- Target OS
- Installed Date
- Updated Date

REQ-12: The application will display the extracted data from the Android device on the screen in a concise, human-readable form.

REQ-13: The application will show the option to save the displayed data in a file on the user's PC.

Sr No	Functional Requirements	components
1	Application shall be installed properly.	NIL
2	Application shall boot up properly	NIL
3	Different options that are available: • A list of extraction options is shown to choose from. • Help menu. • Exit option. • Home button	Navigation bar on the bottom of the application menu.
4	The application will extract data from system apps including contacts, messages, and gallery	Extract button on home page. For gallery, the gallery button on the main menu extracts data from the device.
5	Application will extract device info including details about sensors, battery, and display details.	Done from the Logical extraction page.
6	Application will extract all the system properties including SDK version, Android version, language etc.	Logical extraction page.
7	The application can detect if the device is connected.	Connection component on the right-side bar.
8	The application provides option to enter the target extraction directory.	Option available on Home page
9	The application allows the user to choose an extraction method.	Check boxes on home page.

10	The application will enlist the data described in the SRS under the REQ 11.	From the Raw data component.
11	The application will display the extracted data from the Android device on the screen in a concise, human-readable form.	Report component.
12	The application will show the option to save the displayed data in a file on the user's PC.	Report component
13	Choosing Help Menu option shall show Instruction Manual.	Help component on the Navigation bar.

4.4.2 Nonfunctional Requirements

4.4.2.1 Performance Requirements

Response Time

The system shall be working within 1 minute of opening it.

Platform

The system application shall be compatible with Windows.

Efficiency

The system shall be able to extract data at the rate of approximately 4 Mbps.

4.4.2.2 Safety Requirements

The use of this product in the wrong hands can lead to illegal activities and can compromise the victims' privacy. It can also be used to extort people. The investigators must be careful not to let the application be sold to private and suspicious group of people.

4.4.2.3 Security Requirements

Application running on the system shall not need any additional or personal information. There are no connections to other devices or severs so no data will be sent or received or used in any way.

4.4.2.4 Software Quality Attributes

Usability

The graphical user interface of virtual stem is to be designed with usability as the priority. The extraction system will be presented and organized in a manner that is both visually appealing and easy for the user to navigate and use the system.

Accuracy

The system shall provide 95% accuracy to make the project more useful for the forensic investigators.

Legal

The system will follow the customer privacy policy strictly.

Reliability

The system shall be able to work in a normal way after restarting due to an error.

Ease of Use

The investigation professionals will need training of one day to completely understand the system.

Operating Constraint

The system requires a Windows PC to extract data. The application will not be compatible with Linux.

CHAPTER 5: CONCLUSION

In this thesis, we discussed an Android Forensic tool “Xtracto” which would help us in extracting data from an Android phone and make a concise and clear report which it will present to its user. We laid out exactly how our product works and how it implements different techniques to acquire and report data. This product will be much cheaper and easily available than other similar tools and it will be Pakistan’s first such tool. This product’s main demographic is law enforcement agencies which can use this product to better their evidence reviews and smoothen their investigation process. Sometimes important evidence such as mobile devices is wasted but with this product at their disposal, they can make sure the information inside the culprit’s phones doesn’t go to waste.

“Xtracto” is a unique product for our country, relatively easy to use and it fulfills its purpose of being something beneficial for society.”

CHAPTER 6: FUTURE WORK

Future milestones that need to be achieved to commercialize this project are the following.

6.1 Making the product applicable to Apple and other devices:

The main objective of this product was to extract and report data from mobile devices that are found on crime scenes. Sometimes there could be devices other than Android. Eventually, with hard work and adjustments this product could be made applicable to other devices as well. Afterall, as we said we don't want the evidence to be wasted on the crime scenes and to completely ensure that this tool should be able to extract data from devices of all manufacturers (or at least the most well-known ones).

6.2 Security bypass: -

As of right now, there no means of cracking the pin/password or any form of security on the device. So technically, for "Xtracto" to work we must first crack the security through other mean and then operate the tool on the device. However, with time, security breaching can be incorporated in the tool which would make the job much easier.

6.3 Face Recognition: -

The feature to match our suspects picture from those in the android device could prove quite beneficial for the investigation team as it gives confirmation on the user of the device can certainly be added to "Xtracto" to further emphasize its importance as a tool for law enforcement agencies and investigation teams.

6.4 Location history and Keyword search: -

Location history is that feature on your Android phone which keeps track of all the places you visited throughout the day, every day. Soon, “Xtracto” would be able to extract this information from any android device regardless of its version.

Currently, “Xtracto” cannot search specific keywords from all the documents in the device which could be an inconvenience especially if the investigation team is looking for something specific, but this could certainly be fixed with enough time.

References

[1] "Autopsy," [Online]. Available: https://www.autopsy.com/.

[2] "Xways," [Online]. Available: http://www.x-ways.net/forensics/.

[3] "Accessdata," [Online]. Available: https://accessdata.com/.

[4] "Ensace," [Online]. Available: https://www.ensace-gmbh.de/en/.

[5] "Security News Paper," [Online]. Available: https://www.securitynewspaper.com/2020/11/17/list-of-all-smart-phone-forensics-tools-2020-edition-part-i/.

[6] D. Biswas, C. Wang and A. Stevanovic, "An automatic traffic density estimation using Single Shot Detection (SSD) and MobileNet-SSD," 2018.

[7] "Autopsy," [Online]. Available: https://www.autopsy.com/.

Report

ORIGINALITY REPORT

12%	10%	4%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.researchgate.net Internet Source	3%
2	www.coursehero.com Internet Source	2%
3	play.google.com Internet Source	2%
4	Submitted to Higher Education Commission Pakistan Student Paper	1%
5	archive.org Internet Source	1%
6	Submitted to Oxford Brookes University Student Paper	1%
7	Submitted to University of Warwick Student Paper	1%
8	Submitted to University of Suffolk Student Paper	<1%
9	sourceforge.net Internet Source	<1%

10	www.ukessays.com Internet Source	<1%
11	etd.aau.edu.et Internet Source	<1%
12	Submitted to University of New York in Tirana Student Paper	<1%
13	users.marshall.edu Internet Source	<1%
14	docplayer.net Internet Source	<1%
15	www.out-law.com Internet Source	<1%
16	Abdul Rehman Javed, Waqas Ahmed, Mamoun Alazab, Zunera Jalil, Kashif Kifayat, Thippa Reddy Gadekallu. "A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions", IEEE Access, 2022 Publication	<1%
17	www.ideals.illinois.edu Internet Source	<1%
18	www.destinationrail.eu Internet Source	<1%
19	Submitted to Universiti Malaysia Sarawak Student Paper	<1%