Configuration Manual

MSc Research Project
MSc in Cybersecurity

Bhavesh Dalvi
Student ID: x23206080

School of Computing
National College of Ireland

Supervisor: Dr. Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Bhavesh Rajesh Dalvi

Student ID: x23206080

Programme: MSc. In Cybersecurity **Year:** 2024-25

Module: MSc Research Project

Lecturer: Dr. Imran Khan

Submission Due Date: 29.01.2025

Project Title: Cracking the code: Digital Forensic Analysis of social media applications on virtual android devices

Word Count: 1270 **Page Count:** 5

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: BRDalvi

Date: 28.01.2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Bhavesh Dalvi
x23206080

This document provides the detail steps that were taken as a part of performing the experiment in this research project. This relates to the section 4 titled ‘Design Specifications’ of the main report. As a part of the experiment setup, we utilized three industry recognized and legally accepted forensic tools or software namely Android Studio, FTKImager and Autopsy along with the three social media applications of Instagram, X, WhatsApp. The below sections detail the steps and configurations made on each of the tool/ software to configure the test environment and derive the expected results:

1 Configuring the virtual android devices – Android Studio

- As a part of this research, we utilized the Android Studio software for creation of customised virtual android devices on which the social media applications would be installed and tested
- We installed the Android Studio (v2024.2) software from the official product website
- The software was downloaded and installed on our laptop
- We initiated the process of creating the virtual devices by selecting a new project
- We opened the SDKTools under SDKManager in the settings tab to ensure that the Android Emulator, Android SDK Platform-tools and the Intel x86 Emulator Accelerator are pre-installed. If not, we need to install them
- Then we initiated the process of virtual android device creation, for which we clicked on the Device Manager tab and then clicked on ‘Create New Device’
- This popped up the tab containing the list of available devices and an option to create your own device
- We selected the Google Pixel 6 device running on Android 9 and 14 for Instagram and Twitter applications respectively and Google Pixel 5 device running on Android 14 for WhatsApp application
- We made certain customizations in the storage and camera settings of these devices
- Then we installed the ADB installer file (.exe) within the Android SDK Platform-tools folder in the directories of Android studio on the local laptop. This was done to configure the ADB tools in the Android Studio software
- We then used the adb root command to root all the virtual devices using the command line terminal of the Android Studio software
- Once the devices were configured and booted, we installed the social media applications of Instagram (v278.0.0.22.117), X (v10.55.0) and WhatsApp (v2.24.20.81) from the ApkPure website on these virtual devices using the drag and drop method
- Once the applications were installed and running, the test data was configured for analysis purposes. This has been already discussed in the main report under section 4
- This concludes the use of the Android studio software

2 Data Acquisition and Processing – ADB Commands and FTKImager

- As a part of this research, we utilized the ADB tool/command and FTKImager (v4.7.3.81) tool to extract and process the social media data from the virtual android devices
- We used the adb pull command in the terminal of the Android Studio software to extract the social media related data from the internal and external storage of the virtual device onto the local storage of the laptop
- Post data extraction, we utilize the FTKImager tool to backup and create forensic images of the data to maintain its integrity and availability
- In the FTKImager tool, we click on create new image file
- Then we select the data that has been extracted for the respective applications one by one to create an image file
- The necessary details are inputted like file name, file destination etc
- The FTKImager tool then starts the process of transforming the raw extracted data into an image file (.ad1 extension)
- Once the image file is generated, the tool computes and verifies the hash value of the data to ensure that it is not tampered with in anyway and the integrity is maintained
- Once the image file is generated and hash is verified, the FTKImager tool is used to mount the image file on the logical drive
- This is done for two reasons, one to create more backups to maintain data availability and the second reason being that the Autopsy tool works with certain specified file types only for the analysis purpose. This image mounting feature creates the image file into the accepted extension
- To mount the image file, select the image file that was just created and select the option of mounting on to the logical drive and specify the drive partition name
- This mounts the image file onto the logical drive which will then be analysed using the Autopsy tool to look for digital artifacts
- This concludes the use of the ADB commands and FTKImager tool

3 Analysis – Autopsy Software/Tool

- As a part of this research, the Autopsy tool (v4.21.0) was used for analysing the extracted data and recovering potential digital evidence/artifacts
- The autopsy tool is an open-source tool that was downloaded from the official website and installed on the laptop
- On opening the autopsy tool, we select the option to ‘Create a new case’
- The basic case and configuration details were inputted
- The autopsy tools allow us to select different types of data files to be analysed. We select the mounted logical drive as our data source
- We load the internal and external storage data for each application one by one in different autopsy cases
- Once the data source is selected and the file name and destination folder settings are configured, the tool starts analysing the data
- This takes a considerable amount of time depending upon the size and type of data source

- Once the data is analysed, by the autopsy tool it generates the directory of files and folders that contain the data of different types, extensions, sizes etc
- This data is then analysed manually, and the digital evidence/artifacts are noted
- This concludes the use of the Autopsy tool/ software

The screenshots of the entire configuration and the generated results is recorded and presented in another file named as Artefacts-ICT. The file is submitted with the main report and configuration manual. Kindly refer to the file to check the screenshots for better visualization of the steps.