2024 IEEE International Conference on Cyber Security and Resilience (CSR)

A Survey of Digital Forensic Tools for Android and iOS Smart Phones

Sthembile Ntshangase
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
smlambo@csir.co.za

Norman Nelufule
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
nnelufule@csir.co.za

David Mulihase
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
dmulihase@csir.co.za

Mamello Mtshali
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
mmtshali3@csir.co.za

Chantel Mokoena
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
cmokoena@csir.co.za

Palesa Moloi
Information and Cybersecurity Centre
Council for Scientific and Industrial Research (CSIR)
Pretoria, South Africa
pmoloi@csir.co.za

***Abstract*—Mobile theft has been an increasing problem in South African cities and townships. This is also motivated by the black market for cellphone sales, but it has recently emerged that in many instances, the phone is stolen to harvest the credential and defraud and clean the victims' bank account. Such cases are hardly reported as the success rate of prosecution is low. This is due to the lack of capacity, investigative tools, and the financial constraints of the investigative authorities. This paper presents a review of modern mobile forensic investigative tools, both open-source and commercialized. The purpose of this survey article is to present an analysis of tools in terms of their strengths and weaknesses and to simplify the work of investigators by bringing all the latest tools into one article.**

Keywords—Digital Forensic, Mobile Forensic, Cyber-Crime Investigation, Fraud Investigation

I. INTRODUCTION

The world faces high mobile phone theft, with London's

Unlocking a phone usually means bypassing security mechanisms such as a PIN, password, pattern, or biometric verification to obtain access to the device's interface and functionality [4],[5]. Once the mobile device is unlocked, the user can use the phone, including accessing applications, settings, and data saved on the device. In addition to this, investigators can perform both logical and physical extraction from the unlocked mobile device.

In contrast, extracting data from a locked phone involves accessing the device's data without unlocking it, which has some limitations. This necessitates specialized software, procedures, or hardware instruments designed to circumvent security protections and access data straight from the device's storage. This method is frequently used in forensic investigations or by law enforcement organizations to obtain evidence from locked devices without the user's consent.

In this research, we perform a literature review and desktop research survey on existing digital forensic tools to