Forensic Data Recovery from Android OS Devices: An Open Source Toolkit

Patrick Dibb and Mohammad Hammoudeh
School of Computing, Mathematics & Digital Technology
Manchester Metropolitan University, Manchester, UK
Patrick.Dibb@mmu.ac.uk and M.Hammoudeh@mmu.ac.uk

Abstract—The recovery of data from mobile phones is a very specialist and evolving field, which can make considerable assistance in the prosecution of criminal cases. Data can include not just call history or text messages but, as mobile phones become more smart, it can also include internet web pages, chat data, social media files and other application data. In this paper we present an open-source toolkit has been developed to improve workflow for forensic analysts and aid Android OS mobile phone forensics. This toolkit has been designed to automatically extract and handle all data extracted from the devices so that vital intelligence can be searched and identified quickly, accurately and efficiently. This paper describes and presents the features of this toolkit.

Keywords—Mobile Forensics; Android OS Forensics

I. INTRODUCTION

With the ever increasing number of smart phones used in people’s lives, it is vital that digital forensic analysts have the correct resources to extract evidence from such devices if they were misused. Mobile devices hold a wealth of information that can include vital evidence for use in criminal cases or legal disputes. It is essential that legal procedures are applied to avoid any possible legal challenge. The data in a mobile device could be easily damaged if not handled correctly.

Currently, there are tens of commercial tools, from a relatively simple data acquisition to more complex forensic extractions. However, these tools are very expensive and have inherent limitations, e.g., designed for computer forensics, limited examination features, extracted data can not be ported directly with circuitry to extract additional evidence. In this work we present an open-source toolkit for devices powered by the rising and one of the most dominant operating systems (OS) for mobile devices, Android.

II. TOOLKIT DESCRIPTION

This toolkit provides an inclusive solution for Android OS devices forensics. It comprises sophisticated methods to collect, preserve, analyse and present information found on an Android device in a manner that meets the common legal regulations.

Once the analyst has logged into the software, he can open an existing case, or create a new case. When a new case is created, it will be assigned a unique case number and will automatically be associated to the case creator. At this point, the data from the device can be extracted, hashed and stored in a secure location. The toolkit has a built in method for data extraction that uses expert and ethical techniques that ensures the integrity and completeness of the extracted data.

The toolkit goes beyond data extraction, it allows analysts to discover linked exhibits that details criminal connections. It provide tools, e.g. advanced search capabilities, that aid in producing clear and concise reports documenting evidence to be used to prove or disprove a case.

The toolkit is capable of displaying and categorising extracted data in an intuitive format. Currently, the toolkit is capable of extracting text messages, call logs, contact numbers, and application data, e.g., Facebook, Twitter, Google Maps and Whatsapp. The software has functions that allows the user to export data into other formats where it can be further manipulated.

III. CONCLUSION AND FUTURE WORK

This paper presented a powerful tool for any mobile phone forensic analyst. It is suitable to extract and analyse Android OS devices. Analysts can use the various features of the toolkit to find intelligence and evidence that detail criminal connections. The various functions used in extracting and analysing the data provide analysts with information that can be used as a legally admissible evidence. This toolkit was tested (black-box/white-box) using Android OS mobile phones. Testing showed that the results obtained were accurate and complete. The toolkit can be downloaded from [1].

The software is only in its first stages and there are multiple avenues that can be followed. First, add further capabilities to display and analyse more application data, e.g. ebay searches. Second, implement forensically sound methods to automatically root an Android OS device. This enable logical data extraction and analysis, because if the device is not rooted then the data such as text messages, call logs and contacts will not be accessible.

REFERENCES