Chapter 16
Mobile Phone Forensic Analysis

Kevin Curran
University of Ulster, UK

Andrew Robinson
University of Ulster, UK

Stephen Peacocke
University of Ulster, UK

Sean Cassidy
University of Ulster, UK

ABSTRACT

During the past decade, technological advances in mobile phones and the development of smart phones have led to increased use and dependence on the mobile phone. The explosion of its use has led to problems such as fraud, criminal use and identity theft, which have led to the need for mobile phone forensic analysis. In this regard, the authors discuss mobile phone forensic analysis, what it means, who avails of it and the software tools used.

1. INTRODUCTION

Forensic Science is the use of forensic techniques and values to provide evidence to legal or related investigations (Jansen, 2008). Issues such as deoxyribonucleic acid (DNA) typing or the identification of drugs are obvious topics within this field. These involve the use of specialised scientific apparatus. Mobile phone forensic analysis is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. Digital forensics has grown rapidly due in part to the increase in mobile devices (Harrill, 2007). The phone no longer simply connects us vocally with another, instead it stores our activities, dates, private numbers, experiences – written, visual or audio-visual; and it allows access to the internet where we send private and public messages. We no longer laugh, cry and love face to face; instead, all is recorded on our 'Smartphone'. As we transfer our experiences from the active, interpersonal world, to the digital; nothing remains private. Whispered conversations, clandestine notes, and mental images are transferred and recorded by phone instead. Although it may defy the ICT novice,

DOI: 10.4018/978-1-4666-1758-2.ch016

deletion has never really meant deletion. Forensic investigators commonly start with phone numbers dialled, answered, received or missed; stored phone numbers of people whom the mobile phone user may know and text messages sent, received or deleted (Punja, 2008). Mobile phone capabilities increase in performance, storage capacity and multimedia functionality turning phones into data reservoirs that can hold a broad range of personal information. From an investigative perspective, digital evidence recovered from a cell phone can provide a wealth of information about the user, and each technical advance in capabilities offers greater opportunity for recovery of additional information (Jansen, 2008). Mobile phone forensics is a challenge as there is yet no de facto mobile phone operating system.

There are two important points to remember when about to analyse a mobile phone. If the device is found switched on, DO NOT switch it off and if the device is found switched off, DO NOT switch it on. Pay as you go mobile phones are seen as 'disposable' in the criminal world. They are a means of communication that is not traceable, because there is no signed contract with the network provider for the authorities to trace. However if the phone is seized from the criminal then a number of forensic tests can be carried out and will reveal the entire call history and messaging history of the criminals in question. Another place where mobile phone forensic analysis plays a very large role is in domestic disputes. For example in the case of an abusive person who has been ordered by the court to stay away from their spouse but returns to the family home to harass the other. Here the police can have a cell site analysis carried out and determine where the abusive partner's mobile phone was at the time of the alleged incident. Mobile phone forensics can also play a vital role in road traffic collisions. The mobile phone can be taken and call records and logs checked to see if the accused was using the phone when the accident occurred.

Access to recovered information from mobile devices must be kept stable and unchanged, if it is to stand up in court. The integrity of the recovered data must therefore be kept intact. This is a vulnerable process, but as the years pass, advancements have been made to literally copy the information as fixed images, and thus unchanged, and unchangeable. Data saved on phones is stored as flash electronically erasable programmable (EEPROM) read-only memory (ROM)).

Mobile phone forensic analysis involves either manual or automatic extraction of data to be carried out by the mobile phone forensic examiners. Automatic extraction is used when the device is compatible with one or more pieces of forensic software and manual extraction is necessary when no compatible software is present. Automatic reading of a SIM Card is used when the mobile phone is supported by one or more pieces of forensic software. A manual verification is then required to confirm the extracted data is complete and correct. Manual reading of SIM card is used when the mobile phone is not supported by any forensic software, or the support offered is limited to such a degree that very little data is capable of being extracted. This method of analysis requires a forensics examiner to manually traverse a handset and digitally record each of the screens. This will include the recording of audio and videos in a format playable by the OIC. All images taken will be produced as a paper based report. Forensic analysis of a mobile device using either manual or automatic techniques can produce some or all of the following data: Make and model of the mobile handset; Mobile Station International Subscriber Directory Number (MSISDN); Integrated circuit card ID (ICCID) - The SIM cards serial number service provider name (SPN); Abbreviated dialling numbers; Last numbers received; Last numbers dialled; Missed calls; Short messages (SMS); Calendar entries; Photographs stored in handset; Video stored in handset; Smart media/compact flash; MMS Messages; Sim card link integrated circuit card ID (ICCID); International mobile