A forensic analysis of iOS, Android and Windows Phone 8.1 to extract WhatsApp data

Adam Shortall and Dr. Hannan Azhar
Computing, Digital Forensics and Cyber Security
Canterbury Christ Chruch University, Kent, UK

Abstract

Popular encrypted messaging services such as Skype, Viber and WhatsApp can be used by organised crime groups to streamline their illegal operations [1]. Encryption techniques used by such applications [2] made traces of illegal activities almost undetectable. If large amount of users can communicate with each other without monitoring using such applications, they could be a potential threat to the security. Attempts to forensically examine such applications are necessary to trace any illegal activities by crime groups. This paper reports challenges involve to examine data of the WhatsApp application on popular mobile platforms for forensic investigations. Some research found [3] in the area of forensic analysis of WhatApp on Android devices but few studies go into any depth on iOS and hardly any studies found with regards to Windows Phone and WhatsApp forensics. This paper reports the use of the latest forensic software, including EnCase, UFED and Oxygen Forensic Suite to examine three popular mobile platforms (iOS, Android and Windows phone) to retrieve messaging data, contacts and any media of the WhatsApp application that had been sent to or from the device without performing any live data forensics and minimising alteration of data to comply with ACPO good practice guidelines. The operating systems used were Windows phone 8.1, Android 4.4.4 (KitKat) and IOS 8.3.

Investigation reported in this paper revealed that all three forensic tools gained the same results as each other. IOS and Android both had data extracted with ease and faced no issues. This included any chat data, user's contacts and media sent to and from the device. Windows Phone 8.1 however revealed very little. Although by default the messages are stored on the readily accessible external micro SD card, they are encrypted, as with the other devices. It was found that Windows 8.1 did not allow access to application or system files, where the AES encryption key is stored and this in turn didn't allow messages to be decrypted and contacts to be accessed as they were stored in system and application folders.

For future investigations it would be desirable to use IEF by Magnet Forensics as they claim to be able to ascertain lots of data from smart phones utilising this software. It would also be useful to utilise free software such as Autopsy 3.0 which are powerful tools but are not recognised as industry standards, to see what results they produce.

References:

1. BBC News Europe, 2015. BBC News: Charlie Hebdo attack: Three days of terror. Available at: http://www.bbc.co.uk/news/world-europe-30708237 [Accessed : 29 April 2015].
2. Ibrahim, M., 2014. How to Decrypt WhatsApp crypt7 Database Messages. Available at: http://www.digitalinternals.com/security/decrypt-whatsapp-crypt7-database-messages/307/ [Accessed : 29 April 2015].
3. Sahu, S., 2014. An Analysis of WhatsApp Forensics in Android Smartphones. *International Journal of Engineering Research,* 3(5), pp. 349-350

Keywords: Mobile forensics, Forensic tools, WhatsApp forensics.