Digital Forensic Investigation of Social Media, Acquisition and Analysis of Digital Evidence

Reza Montasari, Birmingham City University, Birmingham, UK
Richard Hill, The University of Huddersfield, Huddersfield, UK
Victoria Carpenter, York St John University, York, UK
Farshad Montaseri, Islamic Azad University of Khark, Khark, Iran

ABSTRACT

Various social networking sites (SNSs), widely referred to as social media, provide services such as email, blogging, instant messaging and photo sharing for social and commercial interactions. SNSs are facilitating new forms of social interaction, dialogue, exchange and collaboration. They allow millions of users and organisations worldwide to exchange ideas, post updates and comments or participate in activities and events, while sharing their wider interests. At the same time, such a phenomenon has led to an upsurge in significant criminal activities by perpetrators who are becoming increasingly sophisticated in their attempts to deploy technology to circumvent detection. Digital forensic Examiners (DFEs) often face serious challenges in relation to data acquisition. Therefore, this article aims to analyse the significance of SNSs in DFIs and challenges that DFEs often encounter when acquiring evidence from SNSs. Furthermore, this article describes the steps of the digital forensic investigation process that must be taken to acquire digital evidence that is both authentic and forensically sound.

KEYWORDS

Digital Evidence, Digital Investigation, Evidence Acquisition, Evidence Analysis, Facebook, Instagram, LinkedIn, MySpace, Social Media, Twitter

INTRODUCTION

Various social networking sites (SNSs), widely referred to as social media, provide services such as email, blogging, instant messaging and photo sharing for social and commercial interactions (Taylor et al., 2014; Cavico et al., 2013). SNSs such as Facebook, Instagram, LinkedIn, Myspace and Twitter are facilitating new forms of social interaction, dialogue, exchange and collaboration. They allow millions of users and organisations worldwide to connect via exchanging ideas, posting updates and commenting or participating in activities and events, while sharing their wider interests (ITU, 2010; Purcell, 2010; Dennis, 2010). Other purposes of using SNS include, but not limited to, general chatting, broadcasting breaking news, arranging a date, following election results, coordinating disaster

DOI: 10.4018/IJoSE.2019010105

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
response, humour and serious research (ITU, 2010). As a result of the provision of such services, there has been a rapid growth in the application of SNSs, in particular those of Facebook and Twitter, by organisations as part of their marketing campaigns (Kozinets et al., 2010; Fagerstrom and Ghinea, 2010). At the same time, such a phenomenon has led to an upsurge in significant criminal activities by perpetrators who are becoming increasingly sophisticated in their attempts to deploy technology to circumvent detection. Although the use of SNSs leaves behind various types of artefacts that are of paramount importance to a digital investigation, nevertheless it often poses serious challenges in relation to data acquisition. To this end, in the following sections, we shall analyse the significance of SNSs in DFIs and challenges that DFEs often encounter when acquiring DE from SNSs.

BACKGROUND

Digital evidence is increasing in both size and significance in criminal and civil trials (Casey, 2011; Kerr, 2010; Brown, 2009; Kessler, 2010; Cohen, 2010; Ball, 2008; Manes et al., 2007). It is latent in the same way as a fingerprint or DNA sample (ACPO, 2012). However, digital evidence is more complex and volatile as it can be accidently or improperly modified, damaged or destroyed during the investigative process (Giova, 2011; Holder et al., 2009; Mukasey et al., 2008; Bem et al., 2008; Ashcroft et al., 2004). The extent of the value of the digital evidence is based not only on the extent to which a tool is trusted (Wojcik et al., 2006; Ciardhuáin, 2004), but also on the competence and experience of the investigator carrying out the digital investigation (ISO/IEC 27037, 2012; ACPO, 2012).

Courts are now increasingly allowing the use of digital evidence obtained from SNSs. Forensic investigation of social media might be needed for various reasons such as collecting evidence for use in criminal proceedings or in organisations’ disciplinary panels for employees that have infringed on company policy (Sipior et al., 2013; Hutchings, 2012). Quoting the head of the UK College Policing, Moore (2014) states, “Complaints originating from social media make up ‘at least half’ of calls passed on to front-line officers”. Referring to the interviews given by other police officers, Moore (2014) continues to state that a significant amount of the calls that the front-line police officer had been asked to respond to were now associated with social media, including death threats, bullying and harassment (Moore, 2014).

In relation to acquiring digital evidence from SNSs, there does not currently appear to be an official guideline specifically designed for digital forensic investigation of SNSs (Taylor et al., 2014). However, the UK’s Association of Chief Police Officers’ (ACPO) Good Practice Guide for “Computer-Based Evidence” (developed by National High-Tech Crime Unit with its main focus being on the field of law enforcement) (Montasari, 2016a) can be a practical starting point for organisations intending to conduct forensic investigation of SNS misuse (Taylor et al., 2014). The ACPO has been updated several times with the latest one being Version 5 in October 2011 (as of April 2018). In the latest version of this guide, the ‘computer-based evidence’ was replaced with ‘digital-based evidence’ to reflect the development of investigating cyber security incidents in a broader context. Since ACPO Good Practice Guide does not form a legal requirement within the UK jurisdiction, its application by DFIs is voluntary. Furthermore, the Comprehensive Digital Forensic Investigation Process Model (the CDFIPM) for Digital Forensics Practice presented in Montasari (2016a), that primarily focuses on digital devices, can also be used to conduct digital investigation both in SNSs and cloud settings.

DIGITAL FORENSIC INVESTIGATION PROCESS

Crime / Misuse Detection and Reporting

Crime / Misuse Detection is the first step in any type of digital investigation regardless of the source from which potential evidence is to be collected (e.g. standalone digital devices, cloud or SNS, etc.)
Related Content

Comparison of Linguistic Summaries and Fuzzy Functional Dependencies Related to Data Mining
www.igi-global.com/chapter/comparison-of-linguistic-summaries-and-fuzzy-functional-dependencies-related-to-data-mining/124580?camid=4v1a

How Big Data Transforms Manufacturing Industry: A Review Paper
www.igi-global.com/article/how-big-data-transforms-manufacturing-industry/219323?camid=4v1a
How Continuous Improvement Can Support Logistics: A Reflection of Best Practices
www.igi-global.com/article/how-continuous-improvement-can-support-logistics/196601?camid=4v1a

Comparative Study on Multi-Objective Genetic Algorithms for Seismic Response Controls of Structures
www.igi-global.com/chapter/comparative-study-on-multi-objective-genetic-algorithms-for-seismic-response-controls-of-structures/124578?camid=4v1a