Multilevel Visualization Using Enhanced Social Network Analysis with Smartphone Data

Panagiotis Andriotis, University of Bristol, Bristol, UK
Zacharias Tzermias, Institute of Computer Science, Foundation for Research and Technology Hellas, Heraklion, Greece
Anthi Mparmpaki, Institute of Computer Science, Foundation for Research and Technology Hellas, Heraklion, Greece
Sotiris Ioannidis, Institute of Computer Science, Foundation for Research and Technology Hellas, Heraklion, Greece
George Oikonomou, University of Bristol, Bristol, UK

ABSTRACT

While technology matures and becomes more productive, mobile devices can be affordable and, consequently, fully integrated in people’s lives. After their unexpected bloom and acceptance, Online Social Networks are now sources of valuable information. The authors therefore use them for tasks varying from direct marketing to forensic analysis. The authors have already seen Social Network Forensics techniques focused on particular networks implementing methods that collect data from user accounts. During the forensic analysis it is common to aggregate information from different sources but, usually, this procedure causes correlation problems. Here, the authors present their method to correlate data gathered from various social networks in combination with smartphones creating a new form of social map of the user under investigation. In addition, the authors introduce a multi level graph that utilises the correlated information from the smartphone and the social networks and demonstrates in three dimensions the relevance of each contact with the suspect.

Keywords: 3D Graph, Data Correlation, Evidence Visualization, Smartphone Forensics, Social Network Analysis, Social Network Forensics

1. INTRODUCTION

Online Social Networks (O.S.N.) became an integral part of our social life. Facebook active users outreached one billion on December 2012 (“Key facts”, 2013) while Twitter is catching up, with its total number of users reaching 500 million on April 2012 (“Twitter to surpass”, 2012). People in developed and developing countries use smartphones to communicate and they prefer to stay online and in touch with their social circles using the embedded

DOI: 10.4018/ijdcf.2013100103

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
applications on their phones. Unfortunately, miscreants could not stay uninvolved. Incidents like cyber-bullying, insults, identity thefts and phishing are currently present both on Facebook and Twitter (“A Facebook crime”, 2012; “Reports of Facebook”, 2012) and generally social network crime and fraud tend to increase. As a consequence, forensic investigations include the examination of social footprints in their endeavor to find crime evidence.

The variety of O.S.N. complicates the evidence gathering procedure because analysts must use different tools for distinct social networks when they gather the data. If social footprints are discovered on more than one network, they should be correlated to make a complete profile of the suspect. The correlation process can be a tedious task because a large volume of information must be combined together. Moreover, malicious users may choose to employ different social networks to conceal their social footprints, posing a challenge to forensic analysts to deal with a great amount of data in such investigations.

Facebook (“Downloading your info, 2013”) and Twitter (“Twitter blog”, 2012) provide the opportunity to download a user’s data and, in addition, third-party applications (“Download and view”, 2013; “Facebook report”, 2013; http://www.fridayed.com) have been developed to perform the same task. Furthermore, there are few commercial tools that can help an analyst to download a forensic image from a social network profile (http://www.oxygen-forensic.com/en/).

In this paper, we propose a social forensic framework capable of combining social footprints from diverse networks, found locally on the suspects’ computers (such as mailboxes, Skype chat logs, O.S.N.) and on their smartphones. We then store them under an abstract data representation. Provided with their credentials, a crawling component gathers any data available from the social network and communicates under a predefined API with the tool core, to store gathered evidence on a semantically correct manner on a graph database. Graph properties of each network are also preserved in order to correlate data from different sources effectively. In particular, Facebook friends, Skype contacts and Twitter followers point out that two or more entities of each network are related with each other with a type of relationship and phone contacts describe a more strong bond among them. Finally, the visualization of correlated data results to a broader perspective of the suspect’s actions and contacts and helps analysts identify malevolent activity efficiently.

The contributions of this work can be summarized as follows:

- We present a framework capable of combining data from diverse social networks under an abstract graph representation using open source tools.
- We perform data correlation tactics with artifacts found on smartphones.
- We concatenate the social media activity and the personal communication through the phone to distinguish contacts and provide them under a common visualization paradigm.
- To the best of our knowledge there exist a research gap in the area of phone forensics linking them with social network analysis and our work presents a framework that connects the two fields.
- We demonstrate a novel method to display graphs adding layers of connectivity in 3D space allowing the graph to present the most significant contacts to the user.

The paper is organized as follows: In Section 2 we discuss relevant work on Social Network Analysis and Forensics. The architecture of our tool and its implementation as proof of concept is shown in Section 3. Section 4 demonstrates the effectiveness of the proposed method on a case study. In Section 5 we talk about the results and we evaluate the tool. Finally, Section 6 includes the conclusion and our plans for further work.
An Overview of Penetration Testing
www.igi-global.com/article/an-overview-of-penetration-testing/123388?camid=4v1a