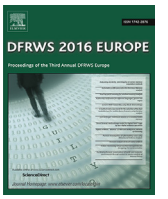
Digital Investigation 16 (2016) S55–S64

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin



DFRWS 2016 Europe — Proceedings of the Third Annual DFRWS Europe

A method and a case study for the selection of the best available tool for mobile device forensics using decision analysis

Shahzad Saleem [a, *], Oliver Popov [b], Ibrahim Baggili [c]

[a] School of Electrical Engineering and Computer Science, National University of Science and Technology, H-12, Islamabad, Pakistan
[b] Department of Computer and Systems Sciences, Stockholm University, Postbox 7003, SE-164 07, Kista, Sweden
[c] Tagliatela College of Engineering, University of New Haven, 300 Boston Post Road, West Haven, CT, 06516, USA

Keywords:
Digital forensics
Mobile device forensics
Mobile device forensics tools
Evaluation
Multi-criteria decision analysis
Digital evidence
Digital investigation
Expected utility
Total ranking
Hypothesis testing

A B S T R A C T

The omnipresence of mobile devices (or small scale digital devices – SSDD) and more importantly the utility of their associated applications for our daily activities, which range from financial transactions to learning, and from entertainment to distributed social presence, create an abundance of digital evidence for each individual. Some of the evidence may be a result of illegal activities that need to be identified, understood and eventually prevented in the future. There are numerous tools for acquiring and analyzing digital evidence extracted from mobile devices. The diversity of SSDDs, types of evidence generated and the number of tools used to uncover them posit a rather complex and challenging problem of selecting the best available tool for the extraction and the subsequent analysis of the evidence gathered from a specific digital device. Failing to select the best tool may easily lead to incomplete and or improper extraction, which eventually may violate the integrity of the digital evidence and diminish its probative value. Moreover, the compromised evidence may result in erroneous analysis, incorrect interpretation, and wrong conclusions which may eventually compromise the right of a fair trial. Hence, a digital forensics investigator has to deal with the complex decision problem from the very start of the investigative process called preparatory phase. The problem could be addressed and possibly solved by using multi criteria decision analysis. The performance of the tool for extracting a specific type of digital evidence, and the relevance of that type of digital evidence to the investigative problem are the two central factors for selecting the best available tool, which we advocate in our work. In this paper we explain the method used and showcase a case study by evaluating two tools using two mobile devices to demonstrate the utility of our proposed approach. The results indicated that XRY (Alt_1) dominates UFED (Alt_2) for most of the cases after balancing the requirements for both performance and relevance.

Introduction

The overarching goal of this work is to help investigators select the best available tool for mobile device forensics. The selection is based on both the performance of the forensics tools and relevance of the digital evidence in solving

* Corresponding author. Tel.: +92 321 5051723.
E-mail addresses: shahzad.saleem@seecs.edu.pk (S. Saleem), popov@dsv.su.se (O. Popov), IBaggili@newhaven.edu (I. Baggili).

http://dx.doi.org/10.1016/j.diin.2016.01.008

or furthering a specific case. The outcome will facilitate proper extraction, valid analysis, correct interpretation, right conclusions and the increased possibility for a fair trial. The selection is based on a formal method called Multi Criteria Decision (MCD) analysis. Performance and relevance are the two factors for MCD analysis in our proposed work.

ICT facts and figures" released by ITU (International Telecommunication Union, 2012; International Telecommunication Union (ITU), 2013) indicate deep penetration and wide acceptance of mobile devices in our society. These devices are versatile in nature and are used for various extensive daily activities. Consequently, a user will leave traces of digital activities (digital footprints) whenever he/she interacts with a mobile device. These digital footprints transform the mobile device to a personal digital behavioral archive. These behavioral archives are typically important to an investigation because they not only reveal digital evidence but behavioral patterns of its user as well. Moreover, around 80% of court cases have digital evidence linked to them (Rogers, 2004; Baggili et al., 2007). In the past years dozens of murder cases have been settled with the help of digital evidence found on the murderer's and or victim's mobile devices (Baggili et al., 2007).

The forensics community has appreciated the importance of mobile devices by acknowledging a separate branch of digital forensic science called "Mobile Device Forensics" (Casey, 2011). Private sector has also responded by developing numerous dedicated tools to perform mobile device forensics.

The problem however, is that the number of forensics tools is quite large and their performance varies for different types of digital evidence. For example one tool will perform better for recovering SMS while the other will perform better for recovering standalone files. Therefore, during the preparatory phase it becomes difficult for an investigator to select the best available tool. Therefore, as a general guideline, experienced digital forensic scientists and examiners typically cross-validate their results by using a variety of tools, which in turn leads to longer investigative time.

Preservation and protection are the two umbrella principles stipulated by the extended abstract process model with 2PasU (Saleem et al., 2014a). Selection of the best tool is one of the requirements of the model during preparatory phase. Failing to select the right tool may easily lead to incomplete and or improper extraction, which eventually may violate the integrity of the digital evidence and diminish its probative value and hence admissibility. Moreover, the compromised evidence may lead to erroneous analysis, incorrect interpretation and wrong conclusions, with an eventual consequence of a compromise in the litigating party's right of a fair trial.

In the past, vendor evaluation results were the only results available for use when selecting appropriate tools for a particular investigative scenario. The National Institute for Standards and Technology (NIST) realized the need for evaluating the forensics tools as an independent third party. Therefore, they published Smartphone Tool Specification (National Institute of Standards and Technology (NIST), 2010a) and Smartphone Tool Test Assertions and Test Plan (National Institute of Standards and Technology (NIST), 2010b). Later on, NIST used these specifications and test plans to evaluate forensics tools. Evaluation reports were published on the NIST website (National Institute of Standards and Technology (NIST), 2013) with free public access.

NIST has evaluated the forensics tools by using different mobile devices. So, the evaluation results cannot be generalized and used to compare different forensics tools. To solve this problem the same mobile devices were used to evaluate different forensics tools and the results were published in Kubi et al. (2011). But the comparison in Kubi et al. (2011) was not formal and automatic. The evaluation process was moved further to formally compare the forensics tools by using quantitative analysis (Saleem et al., 2013).

In Saleem et al. (2013) the tools were formally compared only with respect to their performance. Every type of digital evidence is equally important and relevant in a given scenario was the underlying assumption. However research has illustrated that different types of digital evidence extracted out of a mobile device are not equally relevant to understand and solve the case at hand (Saleem et al., 2014b). The work presented in this paper extends the prior research and proposes a formal method for to select the most appropriate tool for a particular investigative scenario. It is based on multi-criteria decision analysis with performance and relevance as the two critical factors. We further present as a case study two forensics tools that were evaluated with the help of two mobile devices to demonstrate the utility of our proposed formal method.

Performance measurements of nineteen potential sources of digital evidence were already published (Kubi et al., 2011). These measurements provided the base to connect the alternative forensics tools while building the MCD model.

Relevance is the second factor for the MCD model. It is case dependent, e.g. an SMS can be more important than call logs in one case type and vice versa in another. Our work uses seven different types of investigations having an associated digital side, as identified by Maxwell (Anobah, 2013). With that said, the method we present is extensible to inherit other types of crimes and is not limited to the seven types used when writing this paper.

This research actually builds on the idea presented in a short paper (Saleem and Popov, 2014), measures the factor of relevance by conducting a survey and concludes by producing the formal results. Relevance, in the survey, was measured on a linear scale from zero to ten points. It provided a formal association of the relevance factor to each type of digital evidence. This association was the final necessary prerequisite to build the MCD model and to perform the subsequent analysis.

Expected value graphs at different levels of contraction, cardinal and total rankings were computed using the MCD model with the help of an in house developed tool called DecideIT (Preference AB). Visual representation of the results in the form of graphs and charts helped in an obvious and formal selection of the best tool for a particular type of investigation. Theoretical and mathematical background of decision analysis, MCD model, total and cardinal ranking