


Digital Forensics: Challenges and Opportunities for Future Studies

Reza Montasari, University of Huddersfield, Huddersfield, UK


Richard Hill, University of Huddersfield, Huddersfield, UK

Simon Parkinson, University of Huddersfield, Huddersfield, UK

 <https://orcid.org/0000-0002-1747-9914>

Pekka Peltola, CAR-CSIC, Center of Automation and Robotics, Spanish Research Council, Madrid, Spain

Amin Hosseini-Far, University of Northampton, Northampton, UK

 <https://orcid.org/0000-0002-2534-9044>

Alireza Daneshkhah, Coventry University, Coventry, UK

ABSTRACT

Considering the ever-growing ubiquity of technology, there is an associated growth in the possibility of digital devices related to a criminal investigation or civil litigation. As the variety of digital devices is increasing, the storage capacity of each is also rising exponentially. Due to the varied and large volumes of data produced, law enforcement agencies (LEAs) worldwide are facing a significant backlog of cases. This has culminated in significant delays in dealing with cases that urgently require digital forensic investigations (DFIs). It is of paramount importance that new research approaches be adopted to address such challenges. This article evaluates the existing set of circumstances surrounding the field of digital forensics (DF). The article provides two important contributions to the field of DF; it identifies and analyses the most important mid- and long-term challenges that need to be considered by LEAs. It also proposes important specific future research directions, the undertaking of which can assist LEAs in adopting a new approach to addressing these challenges.

KEYWORDS

Digital Forensics, Digital Investigation, Big Data, IoT Forensics, Cloud Forensics, Cybersecurity, Encryption

1. INTRODUCTION

Over the past few years, technology has become prevalent in many aspects of day to day life. We have witnessed rapid advancements in Information and Communication Technology (ICT) features. Technologies such as communication networks, mobile devices, Internet of Things (IoT) solutions, Cloud-Based Services (CBSs), Cyber-Physical Systems (CPSs) have brought many benefits to technologically advanced societies (Montasari & Hill, 2019; Montasari, 2017b; Cavaglione et al., 2017; Pichan et al., 2015). As a result, commercial transactions and governmental services have rapidly grown, revolutionising the lifestyles of many individuals living in these societies. While technological advancements undoubtedly present many advantages, at the same time they pose new cybersecurity threats (Jahankhani et al., 2014), which have significant impacts on a variety of domains such as government systems, enterprises, ecommerce, online banking, and critical infrastructure

DOI: 10.4018/IJOI.2020040103

(Hosseini-Far et al., 2017). According to an official survey conducted by The Office for National Statistics (BBC, 2017), there were an estimated 3.6 million cases of fraud and two million computer misuse offences in a year.

Some of the challenges resulting from such technological advancements include, but are not limited to: high volume of data, heterogeneous nature of digital devices, advanced hardware and software technologies, anti-forensic techniques, video and rich media, whole drive encryption, wireless, virtualisation, live response, distributed evidence, borderless cybercrime and dark web tools, lack of standardised tools and methods, usability and visualisation. The deployment of IP anonymity and the ease with which individuals can sign up for a cloud service with minimum information can also pose significant challenges in relation to identifying a perpetrator (Caviglione et al., 2017; Lillis et al., 2016; Chen et al., 2012; Ruan et al., 2011; Cameron, 2018). As a result, the number of cases that necessitate DFIs are on the rise, culminating in the creation of a backlog of cases for LEAs worldwide (Montasari, 2016a; Montasari, 2016c). Without a clear plan to facilitate research efforts that extend one another, forensic research will lag behind, tools will become outdated, and law enforcements' products will be incapable of relying on the results of DF analysis (Garfinkel, 2010; Montasari et al., 2019).

In recent years the area of digital forensics has attracted interest from researchers, with notable survey and position papers being published. One recent position paper (Watson & Dehghantanha, 2016) states the high-level challenges associated with performing digital forensics on IoT devices. The authors focus their attention on the location and inability to extract meaningful data from IoT devices. However, they provide little information on what the future direction of this field might be, which could for example, include IoT producers accommodating forensic capabilities from the design stage of the technology. In another study, the authors focus their attention on suggesting future challenges within Smart Infrastructure, which includes IoT devices (Baig et al., 2017). IoT forensic can be related to data, service and/or architecture fusion. Sometimes fusion with other data and users is common. Innovative solutions/recommendations are required to resolve some of the known existing issues (Kuo et al., 2018). The paper provides a comprehensive speculation as to the threats facing Smart Infrastructure and how digital forensics might be performed.

A widely cited key survey published in 2010 (Garfinkel, 2010) provides future paradigms of research, and although relevant, changing IT patterns have resulted in the need for this subject to be revised. For example, in the position paper, future research directions are presented and justified. These areas are: 1) modulization; 2) alternative analysis mechanisms; 3) scale and validation; 4) abstraction. Directions 1, 2, and 3 have demonstrated to be true and areas of continuing research; however, direction 4 (abstraction) is somewhat understated and premature to the needs of current digital forensics. Although, there is clearly a need to abstract the forensic challenge and make it easier, quicker and more reliable for the investigator, the introduction of IoT devices has resulted in the absence of low-level techniques and processes for forensic acquisition. This therefore motivates the perusal of IoT forensics is a precursor to abstraction.

Therefore, in light of the discussion above, it is of paramount importance that new research approaches be undertaken to address the aforementioned challenges. To this end, we evaluate the existing set of circumstances surrounding the field of DF. Our research study makes two important contributions to the field of DF. First, it analyses the most difficult mid and long-term challenges that need to be considered by LEAs. Second, it proposes important specific future research directions, the undertaking of which can assist LEAs in adopting a new approach to addressing such challenges.

2. CHALLENGES

The current states of DF encounters numerous challenges, from both ethical and technological perspectives. As the field of DF continues to evolve, its development is severely challenged by the growing popularity of digital devices and the heterogeneous hardware and software platforms being utilised (Caviglione et al., 2017). For instance, the increasing variety of file formats and OSs hampers

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/digital-forensics/250211

Related Content

Performance-Enhancing Techniques

E. Parsopoulos Konstantinos and N. Vrahatis Michael (2010). *Particle Swarm Optimization and Intelligence: Advances and Applications* (pp. 133-148).
www.irma-international.org/chapter/performance-enhancing-techniques/40632

Moth-Flame Optimization Algorithm for Efficient Cluster Head Selection in Wireless Sensor Networks

Pitchaimanickam Bose (2022). *International Journal of Swarm Intelligence Research* (pp. 1-14).
www.irma-international.org/article/moth-flame-optimization-algorithm-for-efficient-cluster-head-selection-in-wireless-sensor-networks/302604

Optimal Power Flow with TCSC and TCPS Modeling using Craziness and Turbulent Crazy Particle Swarm Optimization

P. K. Roy, S. P. Ghoshal and S. S. Thakur (2012). *Innovations and Developments of Swarm Intelligence Applications* (pp. 148-164).
www.irma-international.org/chapter/optimal-power-flow-tcsc-tcps/65811

A Review of a Smart Roadside and On-Street Parking System

Abdelaziz Tami and Sofiane Boukli Hacene (2022). *International Journal of Organizational and Collective Intelligence* (pp. 1-14).
www.irma-international.org/article/a-review-of-a-smart-roadside-and-on-street-parking-system/313599

Applications in Bioinformatics and Medical Informatics

E. Parsopoulos Konstantinos and N. Vrahatis Michael (2010). *Particle Swarm Optimization and Intelligence: Advances and Applications* (pp. 204-221).
www.irma-international.org/chapter/applications-bioinformatics-medical-informatics/40636