Current and Future Trends in Mobile Device Forensics: A Survey

KONSTANTIA BARMPATSALOU, TIAGO CRUZ, EDMUNDO MONTEIRO, and PAULO SIMOES, University of Coimbra

Contemporary mobile devices are the result of an evolution process, during which computational and networking capabilities have been continuously pushed to keep pace with the constantly growing workload requirements. This has allowed devices such as smartphones, tablets, and personal digital assistants to perform increasingly complex tasks, up to the point of efficiently replacing traditional options such as desktop computers and notebooks. However, due to their portability and size, these devices are more prone to theft, to become compromised, or to be exploited for attacks and other malicious activity. The need for investigation of the aforementioned incidents resulted in the creation of the Mobile Forensics (MF) discipline. MF, a subdomain of digital forensics, is specialized in extracting and processing evidence from mobile devices in such a way that attacking entities and actions are identified and traced. Beyond its primary research interest on evidence acquisition from mobile devices, MF has recently expanded its scope to encompass the organized and advanced evidence representation and analysis of future malicious entity behavior. Nonetheless, data acquisition still remains its main focus. While the field is under continuous research activity, new concepts such as the involvement of cloud computing in the MF ecosystem and the evolution of enterprise mobile solutions—particularly mobile device management and bring your own device—bring new opportunities and issues to the discipline. The current article presents the research conducted within the MF ecosystem during the last 7 years, identifies the gaps, and highlights the differences from past research directions, and addresses challenges and open issues in the field.

CCS Concepts: • **Applied computing** → **System forensics**; *Network forensics*; • **Security and privacy** → *Mobile platform security*; Mobile and wireless security;

Additional Key Words and Phrases: Mobile forensics, digital forensics, mobile cloud forensics, evidence acquisition, forensic ontologies, evidence parsing, digital investigations

ACM Reference format:
Konstantia Barmpatsalou, Tiago Cruz, Edmundo Monteiro, and Paulo Simoes. 2018. Current and Future Trends in Mobile Device Forensics: A Survey. *ACM Comput. Surv.* 51, 3, Article 46 (April 2018), 31 pages.
https://doi.org/10.1145/3177847

1 INTRODUCTION

The increased involvement of electronic devices in criminal actions "has led to the development of Digital Forensics (DF)" (Palmer 2001), a discipline concerning evidence collection, investigation, and presentation in an accepted manner upon court. However, the term *digital* incorporates

This article was partially funded by the Centro 2020 Mobitrust Project (reference CENTRO-01-0247-FEDER-003343).
Authors' addresses: K. Barmpatsalou, T. Cruz, E. Monteiro, P. Simoes, Centre for Informatics and Systems of the University of Coimbra, Department of Informatics (CISUC/DEI), University of Coimbra, Polo II—Pinhal de Marrocos, Coimbra, 3030-290, Portugal; emails: {konstantia, tjcruz, edmundo, psimoes}@dei.uc.pt.

https://doi.org/10.1145/3177847

many categories that cannot be regarded as a whole and, therefore, they require further classification. Some of the DF sub-disciplines encountered throughout literature encompass aspects such as Computer (CF), Network (NF), *database, Audio (AF), Video (VF) (Shanableh 2013), and Mobile Forensics (MF).*

Despite the similar functionalities of mobile devices and computers, they cannot be handled in the same way during a criminal investigation. Substantial differences in terms of hardware, software, power consumption, and overall mobility make them unsuitable for classification under the CF category. As a result, the MF discipline was formulated so as to incorporate the criminal investigation of different types of mobile devices (handsets, tablets, and, more recently, wearable devices). Fundamentally, MF "is the process of gathering evidence of some type of incident or crime that has involved mobile devices" (D' Orazio et al. 2014). More precisely, it is in charge of the whole routine of "gathering, retrieving, identifying, storing and documenting" (Marturana et al. 2011) evidence from small-scale digital devices.

Mobile device operation has its own specific constraints, constituting a compromise between processing power usage, storage capabilities, and portability/autonomy. The progressive balancing and/or offload of computing resources to external entities has provided a solution to cope with device shortcomings, thus creating an intersection between the mobility concept and the cloud ecosystem. While this strategy provides a solution for dealing with device energy, storage, and processing power trade-offs, it also brings new challenges, as cloud services can potentially host relevant evidence.

For many, cloud computing is the future of mobility. In a recent survey by the Right Scale company (RightScale 2016), 95% of the surveyed organizations have adopted a private, public, or hybrid cloud strategy. In the same survey, security on the cloud is ranked second in the list of the most precarious issues in need of improvement. Such a concern is rather realistic: since cloud services cope with increased amounts of sensitive data, they are expected to become a preferred target of criminal activity. This creates a whole new perspective for DF, beyond the self-contained device approach. Moreover, it generates new requirements for the performance of robust investigations.

MF is based on the premise that mobile devices contain important information about an individual's personal or professional activities, which are crucial pieces of evidence during an investigation. As the amount of valuable data stored in cloud services increases, traditional MF techniques cannot solely focus on mobile devices. Cloud forensics addresses this gap, expanding the scope of the investigation process to the cloud environment and encompassing CF, NF, and MF concepts.

In this article, we present the elements that characterize MF as a research discipline, while we highlight its most critical and rising challenges. By observing the advances that occurred during the past 7 years, we examine the research trends and analyze their scope and potential to identify aspects in need of further development.

The rest of the article is structured as follows. Section 2 contains the state-of-the art and background knowledge in the MF discipline, as it has evolved during the past few years. Section 3 presents some noteworthy surveys in the field. Section 4 classifies the existing literature in different categories according to the object of research, while Section 5 performs an analysis of the challenges and literature gaps. Last, Section 6 discusses potential solutions and concludes the article.

2 BACKGROUND

This section provides a background for the current state-of-the-art in MF. Initially, the authors propose a reference scenario incorporating contemporary aspects. Afterward, the investigation process standards are elaborated and an extension of the existing model is proposed. Acquisition

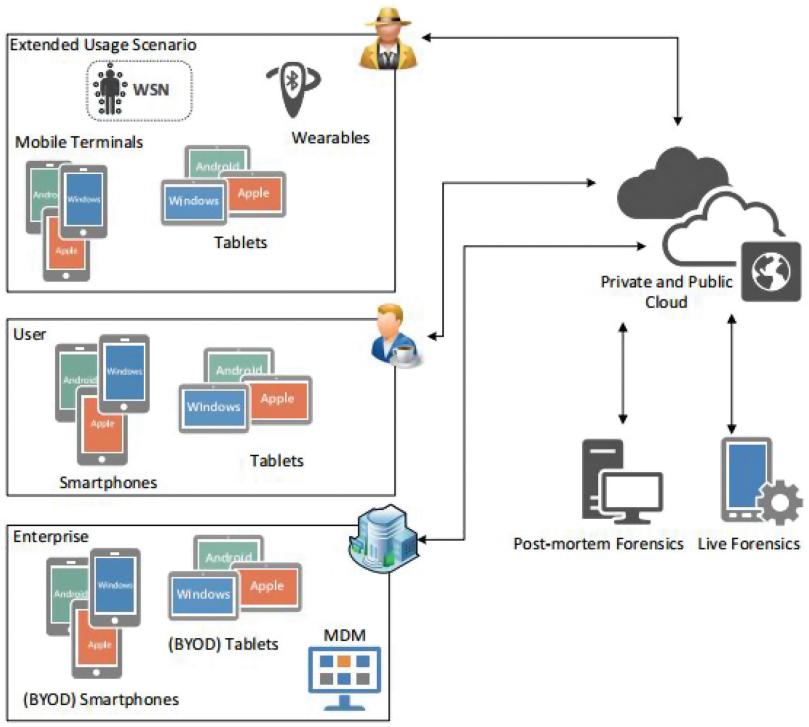

Fig. 1. Reference scenario.

methods and relevant advances are presented in the following section. Last, the impact of the cloud computing discipline is discussed.

2.1 Reference Scenario

The role of computational devices is pretty much akin to a double-edged sword: despite their value as tools for simplifying daily tasks, they can also be abused for criminal purposes. In this perspective, internet-connected devices are particularly vulnerable, as they can easily become targets or even active participants, by performing attacks and spreading cyber threats. The need to investigate these events has prompted for the adoption of guidelines similar to those used for traditional forensics, in the form of DF. DF is the science of retrieving evidence out of digital devices with legally and scientifically acceptable methodologies for "preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence" (Palmer 2001). The aim of this procedure is to provide substantial aid to forensic specialists in terms of reconstructing events and generating reports associated to the crime scene. However, the technological differences among the existing digital media led to the creation of different DF subcategories, varying from CF and NF, to AF, VF, and MF. Figure 1 depicts the contextualization of MF within a contemporary digital environment, which is also described in the following paragraphs.

MF is concerned with several aspects that are orthogonal to the mobile device ecosystem, such as usage profiles or managed asset requirements. This is a direct consequence of the pervasive role mobile devices have acquired as personal and business tools in our daily lives. A smartphone will likely reveal more details about the user's habits and behavior than a desktop or a notebook computer.

Moreover, MF needs to transcend the device boundaries, encompassing the aforementioned public and private cloud service domains. This adds complexity and expands the boundaries of forensic investigation beyond the traditional *post-mortem* examination. In such a volatile environment as the cloud, more recent live techniques have proven highly efficient. Furthermore, mobile devices often act as mediators for personal area networks (wearables), wireless sensor networks or Internet of Things devices. Dataflows between these devices are also of potential interest for forensic purposes.

Until recently, the perception of mutual exclusivity between personal and business usage profiles deemed the need for separate devices, as it was inconceivable to use the same equipment for both roles. It was assumed that companies had no other choice than to provide their workforce with the mobile equipment required for professional usage—to ensure adequate control over costs, management, and security. Lately, several organizations have started encouraging employees to use their own devices within the corporate environment, in an effort to reduce the total cost of ownership for mobile assets. This Bring Your Own Device (BYOD) principle implies that enterprise networks no longer consist exclusively of corporate devices. As such, Information Technology (IT) staff is prompted to "adopt more flexible and creative solutions in order to maintain a satisfactory security level, while enabling access to collaborative technologies" (Thomson 2012).

Enterprise environments are in greater need of protection than individuals. The amount of assets to be protected and the sensitive nature of information stored and transmitted makes them a more attractive target to any sort of illegal activity. Within such environments, "Mobile Device Management (MDM)" (Souppaya and Scarfone 2013) platforms provide organizations with the means to establish and enforce managed device policies via a dedicated platform. After enrolling in the platform and installing an MDM client application, devices start being monitored and the platform policy starts being enforced (e.g., restricting usage to corporate applications). MDM monitoring is a prerequisite, especially for BYOD users that already have a certain level of unknown interaction with the device before enrolling. This avoids exposure to untrusted content or applications that may cause irreversible damage. In this perspective, MDM helps to establish the basic security principles to fit the requirements of each organization.

Considering the fact that contemporary mobile devices are becoming apt at replacing desktop and notebook computers for a variety of tasks, it could be deducted that CF-like techniques might be applied during their forensic investigation. This intuitive reasoning proves wrong, as the similarities between the two device categories are only superficial. In fact, hardware and software components have substantial differences between computers and mobile devices. As a result, different techniques have to be implemented so as to carry out a successful investigation. Nonetheless, specific smartphone components such as external SD cards can be examined effectively by classic CF methods (Hoog 2011), but this is not enough to cover more critical parts of mobile devices, such as the flash memory.

All the aforementioned factors resulted in the birth of a separate discipline for MF, a field dedicated solely to forensic investigation in mobile devices, and which will be presented analytically in the next sections.

2.2 Investigation Phases in Mobile Forensics

The process model for conducting forensic investigations on mobile devices includes the following stages: "preservation, acquisition, examination/analysis and reporting of digital evidence" (Ayers et al. 2014) (see Figure 2). It is a structured procedure that investigators need to follow upon device seizure. It provides guidance and recommendations for secure preservation and storage, device handling, as well as user, application, and network activity tracing. Moreover, guidelines on "good practice methods for forensic investigation of digital evidence" (ISO/IEC 2012), which include the

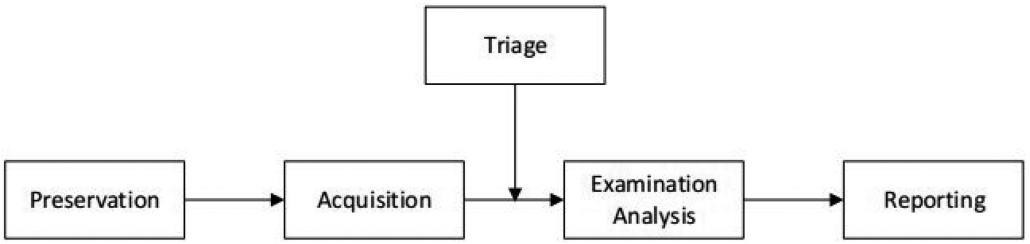

Fig. 2. Mobile Forensics Investigation Process Model, extended from Ayers et al. [2014].

aforementioned investigation process model are "fundamental concepts of the ISO/IEC 27037:2012, 27041:2012, 27042:2012 and 27043:2012 DF standards" (Barmpatsalou et al. 2013). The ISO/IEC 273037:2012 document serves as a complementary prerequisite for the ISO/IEC 273042:2015 and ISO/IEC 273043:2015 standards. While the former document is mainly dedicated to procedures concerning the "analysis and interpretation of digital evidence" (ISO/IEC 2015a), the latter focuses on "providing guidance on the investigation of security incidents" (ISO/IEC 2015b).

Preservation includes all the tasks first responders are responsible for. Particularly for MF, it consists of seizing and securing the mobile devices, tracking their state, and ensuring that no intentional or unintentional alteration will occur to them or their contents (Raghav and Saxena 2009). Afterward, during the *acquisition* phase, a bitwise replication or parts of the internal device memory and peripherals are extracted so as to provide the investigation material for the *examination* and *analysis* phase. Its purpose is to extract conclusions about the criminal actions by "applying established scientifically based methods to acquired evidence. Meanwhile, the examination and analysis phase should describe the content and state of the data, including the source and the potential significance" (Chen et al. 2011). Finally, during *reporting*, every relevant detail or incident observed in the previous phases is completely documented, preferably in a correct chronological order.

Marturana et al. (2011) proposed enhancements for the process model, such as quantitative approaches or the inclusion of a *triage* stage (Rogers et al. 2006) between the *acquisition* and *examination/analysis* phases. Recently acquired data are normalized before analysis, so as to be kept relevant to the investigation needs and avoid delays caused by big amounts of raw information. However, this latter proposal is still undergoing preliminary research and is yet to be incorporated into the aforementioned MF standards as a stand-alone stage.

Nevertheless, the investigation process model is only an orientation roadmap for MF activities. The vast range of research objectives and MF methodologies regarding all phases of the model form a complex and rich body of knowledge, encompassing, for instance, acquisition methods, Operating Systems (OSs), and threat/attack vectors. Such a broad environment is rather challenging for newcomers.

Despite the recognized significance of all stages within the investigation process model, the amount of research dedicated to each part is uneven. This is due to the fact that not every stage is equally important for all fields. For example, even though data preservation is critical for the investigation itself, most of its procedures are fixed and concern notions such as chain of custody and physical security, which have already been extensively researched in the past. Moreover, the majority of preservation techniques, such as the use of Faraday cages for network isolation, require the involvement of disciplines other than computer science. Overall, the fields of acquisition and examination/analysis show increased research activity when compared to the other two.

The following sections will delve into each of the categories hereby introduced, presenting a structured outline of related literature and proposed methods. They will also provide an overview

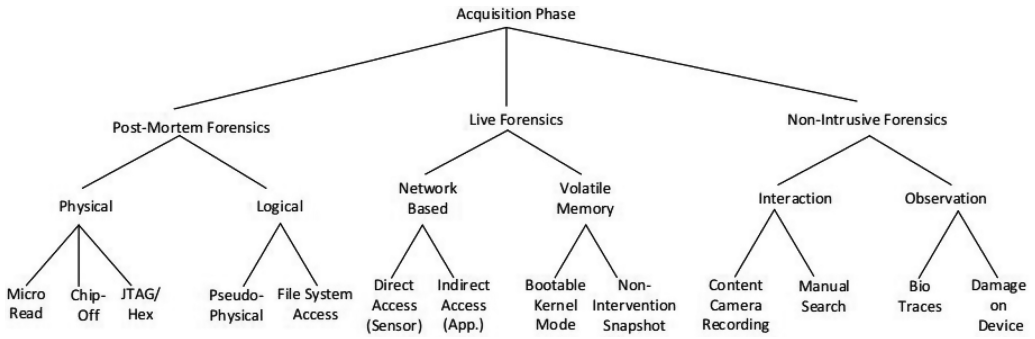

Fig. 3. Detailed acquisition phase.

of the most significant developments, while easing the identification of research gaps. Works prior to 2011 and many acquisition-related milestones are intentionally omitted, due to the fact that around 40 of them have already been discussed by the first author (Barmpatsalou et al. 2013) in a previous article.

2.3 Mobile Forensic Acquisition Methods

Data acquisition is a popular research area within the MF discipline, mainly because its proper execution is crucial for a successful investigation. Without a successfully extracted and validated bitwise memory image or part of the file system, performed with respect to the rules of forensic soundness (Vomel 2013), it is impossible for the rest of the procedure to take place. Figure 3 presents the main subdisciplines of MF acquisition, as they appeared in various research papers throughout literature.

The basic acquisition disciplines comprise the post-mortem, live, and non-intrusive forensics categories. *Post-mortem*, also known as dead forensics, includes physical and logical acquisition methods and takes place upon the seizure of damaged, destroyed, or powered-down devices, requiring a bit-by-bit copy of their memory. Acquisition takes place with devices in off-line mode (i.e., without any kind of network connectivity), so as to avoid minimal modification of its contents (Jansen and Ayers 2007). However, recent research (Barmpatsalou et al. 2013) reveals a trend toward alternative directions, such as the usage of boot loader modifications, which ensure the forensic soundness of the data partition, and the real-time acquisition of volatile memory contents, which are able to collect crucial evidence (Dezfouli et al. 2012).

Physical acquisition methods interact directly with the device hardware, being able to retrieve unallocated (deleted) data, at the cost of using more invasive procedures. Additionally, there is a high probability of a target device being rendered useless after their execution. Among physical acquisition techniques, the "Hex Dumping and *Joint Test Action Group (JTAG)"* (Ayers et al. 2014) methods provide investigators with an easier way to access the raw information stored in the flash memory. *Hex Dumping* is conducted with the use of special devices, known as flasher boxes, which are responsible for creating "an image of the RAM in hexadecimal format" (Luttenberger and Creutzburg 2011). The JTAG method derives from the standard which bears the same name (Joint Action Test Group), "which defines a common test interface for processor, memory and other semiconductor chips, supported by the majority of smartphone manufacturers" (Ayers et al. 2014). This particular method requires the attachment of a cable or a wiring harness to a *JTAG* header or connector on the mobile device, being significantly more invasive than *Hex Dumping*. There are plenty of commercial and open-source forensic tools with physical acquisition features, such

as Cellebrite UFED, EnCase Forensics, *NowSecure* (formerly ViaExtract) (NowSecure 2016) and CDMA Workshop. Also considered as a physical acquisition method, *chip-off* techniques involve direct data retrieval from non-volatile memory chips of the target device. Data are extracted as an adjoining file in binary format, by reverse-engineering the wear-leveling flash algorithms. This method is also considered invasive, incurring in a higher risk of causing irreversible damage to the device. Some of the forensic tools supporting *chip-off* are Soft-Center NAND Flash Reader, BeeProg2,*and NFI Memory Toolkit* (Ayers et al. 2014).

Micro Read is a recently introduced method (Murphy 2013). It involves the use of an electron microscope to observe the gates on a NAND or a NOR flash memory chip. Its usage is not publicly disclosed and it is currently limited to the extreme cases of national and international security crisis.

Logical acquisition is performed by establishing a connection between the device and a forensic workstation via a wired or wireless link; the appropriate security precautions are also taken. Such methods interact with the mobile device file system (Casey 2011) to extract bitwise copies or memory segments. Contrary to *physical acquisition* methods, they are incapable of retrieving deleted files, being less invasive. Many forensic tools with physical acquisition features also support logical acquisition (Cellebrite UFED, NowSecure ViaExtract), while others have solely logical acquisition features, such as Autopsy (Autopsy 2016) and Nyuki Forensic Investigator (Silensec 2016). *Pseudo-physical* acquisition is performed with the use of a boot loader, which alters only the protected area of the device (e.g., RAM) where it is uploaded (Klaver 2010). *File system access* is performed either by a logical dump on the phone's memory partitions (Hoog 2011) or by access to the OS's databases.

Live acquisition deals with near real-time content extraction. It allows dumping parts of the runtime mobile device execution environment, such as the kernel process list, the kernel hash table (Hanaysha et al. 2014), and logs, so as to acquire evidence that would otherwise be lost after a potential device shut-down. It is divided into the network-based and volatile memory subcategories.

Live acquisition procedures take place between the two prevailing non-persistent elements of the mobile device, i.e., the volatile memory and network data. For the first case, the most common approach employs a modified bootable kernel (Volatile Systems 2011), albeit a less invasive technique is also used by the Nyuki Android Process Dumper (AProcDump) (Silensec 2016). This particular implementation consists of an executable running on Advanced RISC Machine (ARM) Android devices (Nguli et al. 2014), which performs a dump of all running applications. The tuples of the dumped applications and their process IDs are then saved in a file for future association to events and other activities of forensic interest. For the network data case, live forensics can also be applied and acquisition takes place either by direct access to the network interface and the packet buffers, or indirectly, via an application. Linux Memory Extractor (LiME) (504ensics Labs 2013) is claimed to have this particular functionality (Heriyanto 2013).

The non-intrusive forensics category encompasses the simplest forms of retrieval, classified between the observation and interaction categories. Observation techniques include "whatever an individual is capable of acquiring from a device via direct interaction with the installed applications" (Mokhonoana and Olivier 2007) and their manual registration or via third party recording (Grispos et al. 2011) with a digital camera. This approach has three major drawbacks: it can become extremely time-consuming when the amount of data to be extracted is relatively big; it is totally ineffective when the device screen is destroyed; and, finally, the acquisition accuracy is neglected, due to the probability of human error. The interaction category makes use of physical or biological traces on a device, such as fingerprints and DNA or other damage types that may be used as evidence upon court.

Due to several factors, the forensic acquisition method landscape is constantly expanding toward new directions and changing over time. The increased popularity of live forensic techniques

is such an example, as they provide a way to overcome the limitations of post-mortem forensics, enabling the acquisition of volatile elements. Moreover, the fact that mobile devices are becoming increasingly involved in the usage and consumption of cloudservices is also a game-changer from a forensic perspective. This happens because cloud infrastructures are not fully compatible with the functionality of current forensic tools and methods, neither in legal nor in technical aspects. The next section offers a detailed presentation of the cloud computing discipline and its influence on MF.

2.4 Cloud Computing and Mobile Forensics

As a result of the increasing need for flexible computing power and storage capabilities while reducing infrastructure costs, organizations are migrating to remote, virtualized, and on-demand services (Grispos et al. 2012), known as cloud services. They offer "virtually unlimited dynamic resources for computation, storage and service provision" (Khan et al. 2014).

The cloud-computing paradigm is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management efforts or service provider interaction" (Mell and Grance 2011). Cloud services provide the means for organizations to scale their IT infrastructure with a level of efficiency, agility, and flexibility, which is difficult to meet solely with in-house resources.

Currently, the prevailing models related to cloud services are: "Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS)" (Ninawe and Ardhapurkar 2014), often referred together as the cloud stack. SaaS applies to the cases where Cloud Service Providers (CSPs) offer applications to the clients, often accessible via a web browser, thus dispensing the need for software distribution or deployment. In the PaaS model, users' flexibility and control levels are relatively higher, since they are able to create and distribute their applications using an Application Programming Interface (API) and even manage their own databases. Last, in the IaaS model, clients can lease virtualized servers, where they can set up whichever type of virtual machine suits their needs. They also may have partial control over network infrastructure, such as firewalls and other solutions. There also exist other service models, such as Database-as-a-Service (DBaaS), where users "store their data in a key-value pair" (Motahari-Nezhad et al. 2009) or even STorage-as-a-Service (STaaS), which is exclusively dedicated to users' data handling, allowing them to store, download, and share their data (Shariati et al. 2015). Some of the most popular STaaS solutions are Dropbox, Box, Microsoft OneDrive, Google Drive, SugarSync, and Ubuntu One.

From a cyber-security perspective, cloud computing also has its own downsides. Cloud services can be used to support criminal activity, by spreading different malware types, or even by providing crimeware-as-a-Service. Moreover, the multi-tenancy capabilities used to support concurrent virtual infrastructure management also contribute for hampering tracing procedures, and subsequently, promoting cloud-based crime (Zawoad and Hasan 2013). Despite being the future of internet services, cloud computing is also the future of electronic crime.

Beyond desktop or notebook computers, cloud services are increasingly involved in providing infrastructure, resource, and complementary service needs for the mobile device consumption. An estimation for the next 2 years (2017–2019), predicts that the average market share of cloud applications worldwide will reach 13,7% (Pang 2015). This poses a challenge for MF investigators, who have to account for the usage of cloud services in the investigation process.

The adoption of cloud services has led to the creation of a specific forensic discipline, defined as "the application of digital forensic science in cloud computing environments" (Badger et al. 2012). This discipline can be defined from several different perspectives. "Technically, it consists of a hybrid forensic approach geared towards the generation of digital evidence" (Samet et al. 2014).

From an organizational aspect, "it involves interactions among cloud actors for the purpose of facilitating both internal and external investigations" (Farina et al. 2015). From a legal standpoint, it often involves "dealing with multi-jurisdictional and multi-tenant situations" (Ruan et al. 2013).

Cloud investigation involves forensic operations both in the cloud and the equipment sides, requiring the use of CF, MF, and NF techniques. Even though investigation in mobile devices can be accomplished by applying already existing forensic methods or tools, the same cannot be said about cloud resources. Most post-mortem forensic tools have limited capabilities over cloud-hosted data. This constitutes a challenge for the DF discipline, since users are increasingly relying on cloud services, decreasing the amount of forensically relevant data hosted on mobile devices. This situation is leading researchers toward alternative approaches, based on the use of live acquisition and interaction techniques. However, these features are not yet referenced by the existing standards (Ayers et al. 2014), as cloud forensics is a developing discipline, yet in its early stages.

The impossibility of gaining physical access to the cloud infrastructure constitutes an impediment to the investigators' work (Marturana et al. 2012), aggravated by the fact that cloud data are frequently spread among various locations on different countries—often with different legal jurisdictions. The high volatility of virtual infrastructure logs creates an additional problem, as this information is vital for non-repudiation purposes. Finally, another dilemma in the field of mobile cloud forensics relates to the need to ensure network device connectivity during an investigation process, without risking a remote wipe or data alteration from a potentially compromised CSP.

Overall, the cloud forensics discipline requires new procedures to be developed for evidence acquisition, while avoiding data loss or corruption. For instance, Cheng (2011) proposes a cloud-based engine, responsible for monitoring information flows and network traffic via interaction with various cloud nodes. The mechanism aims to collect evidence from volatile (data related to the virtual infrastructure of the CSPs) or non-volatile data. Additionally, Chung et al. (2012) describe an investigation procedure for cases involving the use of cloud storage services. It begins with the acquisition of an OS image from the target device, according to platform-specific procedures, which is later parsed for cloud-storage application-related artifacts. If such artifacts are present, legal procedures (such as requesting search and seizure warrants or international judicial assistance) are taken to proceed with further data analysis and reporting.

However, the cloud is not only a source of challenges for digital investigation; it can also provide several benefits. When designing forensic solutions for mobile devices, aspects concerning computational and energy trade-offs have to be taken into consideration, because they are responsible for limiting the incorporation of specific functionality. Cloud technologies can be used to support and improve the efficiency of forensic tools, providing the required computing resources (such as data processing or storage) in a flexible and on-demand fashion (Lee and Hong 2011). Furthermore, "current forensic investigation requires correlative analysis of multiple devices and previous cases" (Lee and Hong 2011). This procedure is rather time- and resource-consuming and can be streamlined by taking advantage of cloud computing resources.

Also, cloud-based forensic tools could eventually help to alleviate the problem of heterogeneous mobile OS platforms. Such platforms are substantially different among them, requiring different approaches for developing forensic tools. For this reason, most developers prefer to target popular device ecosystems (such as Android and iOS), for whom a plethora of tools exist. A cloud-based tool could provide a potential platform-agnostic solution to this particular issue, enabling data acquisition and analysis even from devices that belong to less representative platforms (i.e., with a smaller market share).

Despite the fact that cloud computing is becoming a mature and widely used discipline, cloud security and forensics need substantial improvement. In the next section, surveys related to CF, NF, MF, and their equivalent cloud computing contributions are presented.

3 RELATED SURVEYS

The current section provides a literature review of publications about forensic practices that are directly related or relevant to the MF field. The key for developing effective MF tools and methods is a deep and detailed understanding of the field, with a particular focus on two factors. First, technical knowledge, acquired either theoretically through research, or by actual practical involvement with the subject. Second, formal manners such as the use of logical or mathematical languages, aiming to model the field's basic elements. Despite the specific characteristics of each domain, there are several different approaches covered in surveys on CF and NF techniques that can be transposed to the MF scope, thus remaining relevant to the latter context.

One of the most exhaustive surveys on forensic techniques was presented by Kohn et al. (2013). The authors gathered and formalized into pseudo-code the existing scattered process models for digital forensic investigation and provided their comparative summary. Moreover, they introduced a process model of their own, called Integrated Digital Forensic Process Model (IDFPM), which addresses some of the more persistent investigation issues by schematically organizing the most critical steps in a timeline. IDFPM and forensic process models, in general, can serve as a base for new formal models involving additional concepts, such as cloud computing.

In the field of NF, the survey by Pilli et al. (2010) provides a complete view of the evolution of this discipline, the existing Network Forensic Analysis Tools (NFATs) and related research challenges. Moreover, the authors introduce a novel generic process model for NF.

Specifically for MF, Barmpatsalou et al. (2013) provide a state-of-the-art study on forensic techniques, updated for smartphone-era devices. Besides describing MF-standardization efforts, they also classify existing research, which is presented in a timeline according to the acquisition type, mobile OS, low-level modifications (root-jailbreak), and acquired data types. The aim of such a representation is to aid future researchers to locate research trends within a time context and to observe the evolution of MF through time.

Martini and Choo (2014) conducted a literature survey on cases involving cloud services as sources of evidence. The survey examines technical or conceptual cloud-aware solutions for collection of forensic evidence. It also includes works related to analysis of specific cloud-based products and services (Dropbox, OneDrive). The authors analyze the data types that can be acquired directly from a cloud service and focus on what can be retrieved from a device after interacting with cloud applications.

An overview of the current research trends in the intersection of the fields of MF and the mobile cloud was provided by Samet et al. (2014). The authors enumerated the most significant mobile cloud forensics challenges, such as limitations of post-mortem and live forensic tools or limited investigator control over the device and legal issues. Since mobile cloud forensics is a relatively new discipline without much dedicated research, they included references related to computer cloud forensics, with a potential application to the mobile domain.

A survey on the trends and future challenges of MF concerning the fourth quarter of 2014 was published by Cellebrite Predictions (2015). Despite not being a purely academic work, it provides useful metrics concerning the state of forensic investigations. Among others, it is mentioned that the most significant data sources are (by descending order of relevance): the mobile devices themselves, third party applications, wireless, cellular, and cloud service providers. Moreover, device and application encryption, data stored in CSPs, and big data manipulation are considered as the most prominent emerging challenges.

In their survey, Ardagna et al. (2015) expand the concept of cloud security toward cloud assurance. They claim that assurance as a notion is the expectation that security measures taken will be as effective as initially planned. While security consists of the implemented solutions for

system protection and threat prevention, assurance incorporates techniques concerning evidence collection and analysis. Moreover, they present various cloud security solutions and their cloud assurance equivalents.

Kechadi et al. (2015) conducted a survey on forensic investigations in the cloud computing ecosystem. Initially, the authors identify the resource and computational trade-offs in contemporary mobile devices and highlight the significance of the mobile cloud computing discipline. Additionally, they enumerate the potential challenges that may arise during a forensic investigation in the cloud environment. They also present the differences between traditional and cloud-based mobile forensic techniques within the investigation process. The article concludes with a presentation of some state-of-the-art milestones about application of forensic methodologies in cloud storage services with mobile device involvement.

The current survey aims to expand the time span of the previous work by Barmpatsalou et al. (2013) and observe how the MF discipline evolves over time. It covers a wide span of areas of expertise that are considered MF sub-disciplines and includes them in a special taxonomy scheme, which integrates older and contemporary research papers in a flexible manner. Thus, it can serve as a springboard for further research and open new development roadmaps as extensions of older trends or recent advances in the area of MF. A more detailed overview is presented in the following section.

4 REVIEW OF FORENSIC METHODS

One of the main purposes of this article is to analyze new and emerging trends in MF to provide a comprehensive review of existing approaches and methods. More precisely, the next section describes the adopted methodology and the following sections classify the encountered research trends.

4.1 Methodology

To the best of the authors' knowledge, this article constitutes one of the first attempts toward creating a complete survey on MF. Some efforts, notably Ntantogian et al. (2014) already proposed a preliminary classification regarding MF research directions. In the same line of reasoning, Kaart and Laraghy (2014) provide insights about expanding the research of MF beyond acquisition methodologies. In this perspective, they use the broad term *data analysis* to determine the ensemble of the cases where data acquisition is not a primary concern and investigation targets the characteristics of the evidence instead.

Beyond data analysis or acquisition, other emergent MF concepts and methodologies started appearing in related literature. To help better organize and understand these contributions, this section provides a classification of the most relevant papers in the last 7 years, organized by their scope. We queried high-quality publishers (IEEE, Elsevier, ACM, Springer) for journal and conference papers about MF. The subject of these papers falls along six main categories, namely:

(1) File acquisition and data integrity
(2) Identification of malicious activity and malware analysis
(3) Evidence reconstruction and presentation
(4) Evidence parsing
(5) Knowledge representation
(6) Automated classification and analysis of user and application behavior.

File acquisition has been one of the very first concerns among MF researchers, since the acquisition phase is a critical part of the investigation process model, constituting the initial information-gathering procedure. During this phase, investigators also have to maintain data integrity so as to

preserve evidence admissibility upon court. No further actions can be taken during an investigation if acquisition is not properly performed and retrieved content is not validated.

Beyond forensic purposes, evidence retrieved from mobile devices can also be useful for cybersecurity analysis. When target devices are attacked, compromised by malware or forced into becoming part of a botnet, data acquired from them can provide useful insights to security professionals concerning behavioral patterns and signatures of malicious software. Post-mortem device analysis or live examination can be performed so as to achieve identification of malicious activity and further malware analysis (Casey 2013).

Evidence reconstruction and presentation is another rising concern in the MF research world, since evidence presentation modeling aids the investigation procedure. Interestingly, Kasiaras et al. (2014) noted the existence of an unbalanced distribution between the amount of research papers corresponding to data acquisition and integrity preservation and the number of papers concerning presentation of evidence and further facilitation of the investigators' role.

Evidence parsing is mainly related to the parsing and decoding of acquired data. Due to the wealth of available tools and resources for this purpose, this area has been lagging behind in terms of available research. Moreover, even though current solutions are not exactly suitable for every purpose, it is not difficult for an individual to create a customized script for file parsing.

The structured knowledge representation of MF concepts, methods, and evidence acquired from various sources in the format of formal expressions such as ontologies and rules, provides the capability to observe, evaluate, and obtain valuable insight. Formal knowledge representation is a fundamental requirement for better understanding of the MF discipline, as well as for future design and implementation of forensic tools. It is also a base for creation of automated procedures in classifying and analyzing user and application behavior.

Despite the fact that the need for such methods has been highlighted relatively early (Marturana et al. 2011), few research papers have been published toward that direction. However, the use of automated procedures, based on technologies such as machine learning and soft computing algorithms or rule- and knowledge-based systems would not only facilitate investigations, but also automate many procedures without the need for continuous expert supervision.

Finally, as observed throughout the literature, the more mobile devices are using cloud services, the bigger will be the need to expand the current MF theories and mechanisms so as to encompass them. Cloud forensics is a relatively new concept and, as a result, research papers concerning cloud services and CF can also serve as a starting point for equivalent techniques in mobile devices. The next section presents the literature review, organized accordingly to the previously identified categories.

4.2 File Acquisition and Data Integrity

This section comprises two different families of techniques: conventional (or classic) techniques, that acquire information from stand-alone devices and cloud-aware techniques, which are oriented towards the incorporation of cloud service awareness.

4.2.1 Conventional Techniques. Thing et al. (2010) presented an automated mechanism for retrieving volatile memory parts from Android devices. The authors developed memgrab, a memory acquisition tool, which tracks process IDs and memory addresses "from the procfs virtual file system provided by the kernel" (Thing et al. 2010). Once elements related to the processes are extracted, a Perl-based script, named *memory dump analyzer*, searches for the needed evidence elements.

Dezfouli et al. (2012) proposed an acquisition method of volatile memory contents in Android devices, which claims minimal data modification when compared to existing alternatives. A part

of the non-volatile memory of the device is reserved for storing the information deriving from the process acquisition mechanism. The technique involves updating the initial dump by using the deltas (i.e., the different parts) from consecutive captures.

Aiming to extend the research horizon of iOS acquisition methods, Gomez-Miralles and Arnedo-Moreno (2012) proposed a technique for iPads based on the Camera Connection Kit. The authors claim that this method, equally to the one proposed by Zdziarski (2008), is less invasive in terms of device data alteration. They also highlight the need for data acquisition techniques that are more complete than their predecessors, such as the iTunes backup, which is not capable of retrieving unallocated data. Their pseudo-physical acquisition method consists of the following steps: jailbreaking the device to gain administrative rights, installing openssh (SSH Server) and coreutils libraries, deactivating the network auto-lock feature, connecting the device to a hard disk drive by the Camera Connection Kit and, finally, performing a disk duplicate command. One of the advantages of the proposed method is that, despite the existence of device encryption (in iOS 4), most of the acquired files can be decrypted since the key stored in the device is acquired as well. The authors conclude by evaluating the solution and expressing their concern about the next generation encryption layers and the private user encryption keys that could not be acquired.

Kotsopoulos and Stamatiou (2012) discuss the problem of forensic data acquisition in the simultaneous presence of countermeasures. Their existence may become an impediment for the investigators, since data obfuscation, alteration, and detection of forensic tools are able to hamper their work. The authors suggest a consolidation of open source tools for acquisition of volatile content and encryption key detection that aims to reveal potentially malicious content hidden in encrypted files.

Data encryption and its effectiveness against potential eavesdroppers is discussed by Al Barghouthy and Said (2013). The authors performed logical forensic acquisition in an Android device after using Instant Messaging (IM) applications, private browser sessions, or social media over the latter. They attempted to examine the actual readability of artifacts from messaging applications with and without applied encryption. While additional encryption is proved effective in the majority of social media message exchange, it can also hamper DF procedures for the same reasons.

Votipka et al. (2013) introduced a modified boot image for Android devices to balance between the potential data loss arising from logical acquisition methods and the invasive tactics of physical acquisition strategies. As a result, an alternative, device-agnostic version of an Android boot mode was proposed. More precisely, before proceeding to acquisition via recovery mode, the presented methodology incorporates a software collection package, which gathers the essential elements for booting the specific target device.

Cold-boot attacks in Android smartphones were introduced by Müller and Spreitzenbarth (2013), when the authors proved that data in smartphone RAM chips fade in a slower pace once the device remains frozen for a certain period of time. They also introduced Forensic Recovery of Scrambled Telephones (FROST) recovery image, a custom bootloader that was flashed on the device after the cold-boot attack and provided the potential investigators with the options of acquiring encryption keys, brute-force attacking weak user passwords and unlocking and accessing the user data partition.

Most of the classic acquisition techniques introduced during the last 7 years are experiments in novel fields, an encouraging fact for the future of MF. In the following section, more details about techniques that are destined for a cloud environment can be encountered.

4.2.2 Cloud-Aware Techniques. Apart from describing the current trends concerning DF in the presence of cloud services, Marturana et al. (2012) created a case study of forensic acquisition from CSPs in a Windows 7 environment, with the use of already existing methods. The described use

case consisted of a forensic acquisition procedure performed at the client side after interacting with various CSPs. Despite the fact that the research is not purely related to mobile devices, the described methodology has potential for future use in such an environment.

One of the main risks present in the cloud is associated to information volatility. If information is not acquired within a specific time window, its integrity can be compromised, since it is often impossible to be aware of which entities have accessed, altered, or deleted the cloud data by the time the investigation began. As a solution to this issue, Zawoad et al. (2013) introduced a method that stores "virtual machines' logs and provides access to forensic investigators, ensuring the cloud users' confidentiality, named Secure Logging as a Service" (Zawoad et al. 2013).

The probability of mobile devices serving as proxies for data leaks from cloud services was addressed by Grispos et al. (2013). Dropbox, Box, and SugarSync Cloud storage services were used as testbeds. After conducting physical acquisition on various Android and iOS devices, with different usage scenarios, the obtained images were examined for artifacts related to the cloud services.

One of the approaches to cope with cloud services in a forensic context favors the introduction of continuous monitoring techniques to gather information for DF purposes. In this line of reasoning, Grover (2013) implemented Droidwatch, a prototype monitoring system for Android devices. Droidwatch consists of an on-phone application and a remote enterprise server. The application tracks the occurrence of incidents in the device and reports them back to the server. The system is also equipped with a mobile database, which gets unloaded upon information syncing with the remote instance. The collection of datasets makes the tool an interesting aspect for security auditing, forensic investigations, and MDM, especially in BYOD scenarios.

Baggili et al. (2015) performed a forensic retrieval procedure in two smartwatches. The authors used a variety of proprietary and open source forensic tools, popular in the MF community. Their preliminary research showed that information of critical forensic interest that does not usually reside in mobile handsets, such as data from heart-rate monitors and pedometers, can be acquired through a relatively easy process. Wearable devices upload data concerning the users to the cloud for monitoring and processing purposes, and their acquisition provides the investigators with potentially high-quality evidence.

Daryabar et al. (2015) experimented with the MEGA cloud storage mobile client application. Their research key points included detection of alterations in files and metadata used by the application and discovery of forensic evidence in target devices running iOS and Android. The authors used an adapted version of the investigation framework proposed by Martini and Choo (2012). Afterward, they retrieved a bitwise copy of the Android Jellybean 4.2 internal memory and extracted an iTunes backup from the iOS 7.1.2 handset. TCPDump and Wireshark were used for capturing sent and received network packets. Additionally, they created an experimental scenario that included the following interactions with the MEGA mobile application: logging in with a set of custom credentials, uploading, downloading, and deleting different files, and sharing a file to a custom e-mail address. MD5 hashes and timestamp comparisons were applied to detect changes occurring to the uploaded and downloaded files. While "MD5 values of the original and downloaded files matched" (Daryabar et al. 2015), timestamps showed a certain level of instability and they were always dependent to the date and time settings of the target devices. Installation activity and usernames from the logging-in activities were encountered in both devices. Moreover, the authors were able to detect a non-encrypted file version of the password used in the Android device. Data corresponding to upload activity was only tracked in the iOS device, whereas download activity data was present in both devices. The name of the deleted file was present in both devices as well. Last, no elements concerning the sharing activity were present in any device.

Adversary models are a known practice in the field of information security and cryptography, with little or no expression in terms of DF- or MF-related research activity. In a novel approach,

Do et al. (2015) created an adversary model aiming to collect and analyze data from six widely used cloud applications. With respect to the principles of forensic soundness, such as keeping any device modification to a bare minimum to avoid interference with the forensic process, the authors developed an acquisition and analysis methodology based on this model. Its main innovative characteristic results from combined factors: using a live OS, avoiding modification of the boot or recovery partitions to securely acquire evidence, and providing data analysis capabilities.

A complex study on evidence acquisition of cloud storage applications in mobile devices was performed by Grispos et al. (2015). The authors used practitioner-accepted forensic tools, such as the Cellebrite UFED or the FTK Imager and FTK Toolkit, in devices running iOS and Android. Their concerns went beyond the data recovery process and how it can be affected by the usage of cloud services. They also encompassed aspects such as how different application versions alter the acquisition outcome, what acquired metadata reveal about remote storage at the provider's side, and if the evidence retrieved from two different versions of cloud application sources provides a more detailed dataset of results. One of their most useful findings is that data acquired from a mobile device can serve as a snapshot of the CSP-hosted data.

Even though changes such as file deletions may occur in the future, an acquisition prior to that precise moment constitutes proof that the file existed beforehand. Moreover, the way in which the device is used is able to affect the acquisition outcome. For example, fewer files are recovered if the user had previously performed a cache cleaning. It was discovered that different cloud storage application versions lead to a variation in the number of acquired files. Additionally, information stored in metadata could be used to hint at the storage state in the CSP side, or even to give access to download files that did not exist in the acquisition data. The methods adopted by this study could be easily used with contemporary OS versions, different cloud storage application versions, as well as with applications simultaneously hosting and monitoring multiple cloud storage accounts.

Martini et al. (2015a) proposed "a device-agnostic evidence collection and analysis methodology for mobile devices." The authors use a custom bootloader and a live OS to perform a physical dump of the device partitions—a sound approach from a DF perspective, also adopted by others. Afterward, all the available applications are obtained and different locations are explored for data of forensic interest. Practical use cases involved acquisition and analysis of seven popular Android applications for cloud storage, password sync, and notes [Dropbox, OneDrive, Box, ownCloud, Universal Password Manager, EverNote and OneNote (Martini et al. 2015b)] to retrieve evidence of forensic interest (including sensitive data such as credentials and authentication tokens) in private and public application storage locations.

Shariati et al. (2015) investigated the effectiveness of forensic acquisition for artifacts of the Ubuntu One Cloud storage service in devices running Windows 8.1, MacOSX 10.9, and iOS 7.0.4. The explored use cases covered the acquisition of artifacts after accessing a cloud service via its own application and by browser access. Volatile content and network artifacts were examined separately. While traces of application usage were present in every platform, the same cannot be claimed for sensitive data, such as credentials and authentication tokens, whose vestiges varied among different platforms. Recently, Shariati et al. (2016) conducted a similar study concerning the SugarSync service and included Android in the list of the test platforms, obtaining similar results.

A comparative study concerning the acquisition and discovery of forensic artifacts between Android and Windows Phone devices was conducted by Cahyani et al. (2016b). The authors distinguish three different use cases of "Cloud storage and communication applications, namely information propagation, information concealment and communications" (Cahyani et al. 2016b). The first case is related to signing in, accessing, and downloading files saved in cloud storage services. The second case corresponds to exchange of files modified by a steganography technique via e-mail, communication (Skype, WhatsApp, Viber), and cloud storage applications. Last,

communication applications are used as means of information exchange and activity (friend addition, chat) tracking. The authors used physical, logical, and manual acquisition techniques, depending on each method's applicability on the different target devices. Logical acquisition of Android devices resulted in successful retrieval of user credentials, actions, and downloaded data. On the contrary, only the latter pieces of evidence were available in devices running the Windows Phone operating system. The authors concluded that only physical acquisition is capable of retrieving a significant amount of artifacts from Windows Phone smartphones, thus cross-validating the assumption made in one of their previous papers (Cahyani et al. 2016a).

In the last few years, an explosion in the use (and misuse) of cloud services was observed. As a result, research on cloud-aware forensic acquisition techniques grew significantly to face the upcoming challenges in cloud-based cyber crime. One of the fields strongly correlated to criminal activities that is also in need of new, adaptable mechanisms and continuous surveillance is the one of malicious activity identification, which is presented in the next section.

4.3 Identification of Malicious Activity and Malware Analysis

This section analyzes live methods, which occur in real time, and classic methods, which take place upon malware infection.

4.3.1 Live Methods. Taking into account the energy and processing trade-offs that occur when a continuous monitoring application is running, Houmansadr et al. (2011) introduced a high-level architecture of a cloud-based Intrusion Detection System (IDS). This IDS uses a cloud proxy server to perform off-loaded forensic analysis and malware recognition on the extracted data from the device. However, the practical feasibility of such a method is debatable and requires further research and experimentation, mainly due to the large amount of exchanged data.

The Volatility Framework is a multi-platform memory forensics solution. Whether the extracted memory product is in "raw format, a Microsoft crash dump, a hibernation file, or a virtual machine snapshot" (Volatile Systems 2011), it provides the investigators with a complete view of the examined system. Identification of malicious activity was one of its initial concerns, but nowadays its functionality has expanded. Since the release of version 2.3.1 in October 2013, support for Android kernels was also added, expanding the potential of Android forensics to a new level.

A fake, intentionally set up GSM/GPRS network was created by Schutz et al. (2013) for intercepting network traffic to and from a potentially compromised mobile device. This way, network traces get trapped and are further processed by the Wiretrap application.

Frequently, criminal actions are directly associated to device compromising from malware or third-party attacks. Analysis of audit data from forensic associations can help investigators to create behavioral patterns of several mobile device threats. This can be achieved by exploring "hidden processes, their structure, suspicious executed code and other entities" (Hanaysha et al. 2014). The creation of an open source Android memory forensic investigation environment was the main subject of the solution proposed by Hanaysha et al. (2014). Focusing on live acquisition, the authors used a combination of the Volatility Framework with LiME, aiming to identify and trace the assets compromised by malware. They simulated use cases by installing common Android malware, such as the O Bada Trojan and ZitMo in the target device. By accessing hidden processes and gathering information about their structure from the kernel process list, the kernel hash table and the kmem_cache, they were able to trace them back to the malware activity. However, an automated version of this procedure is yet to be researched.

Even though live methods are indisputably the future of the race against malware, classic methods—presented in the next section—can still produce meaningful contributions.

4.3.2 Classic Methods. Di Cerbo et al. (2011) presented the functionality of a forensic tool (AppAware), especially designed for detecting Android malware based on permission abuse. As soon as the developed application is executed on the device side, it generates an eXtensible Markup Language (XML) file containing the permissions requested for the selected application. Then, the investigators are prompted to manually compare the results to a classified list of potential malware. Despite the fact that the particular forensic tool is relatively useful, automated comparison and classification of the malware would be a considerable evolution.

A typical guideline for recognizing mobile malware via a forensic procedure consists of the following steps: identification of suspicious programs, neutralization of any anti-forensics code, code extraction from the malware body, and deduction of malicious functions (Li et al. 2012). In this article, the authors propose a method of identifying mobile malware via reverse engineering, analysis, and reconstruction of events related to their functionality.

Eradicating malicious activity at the highest possible scale can be rather characterized as an achievement. Nevertheless, mobile criminology is not solely dedicated to the malware identification and taken countermeasures, but to the potential crime scene as a whole. The next section introduces the subdiscipline of evidence reconstruction and presentation as a means of facilitating the investigator's duty.

4.4 Evidence Reconstruction and Presentation

This section enumerates and analyzes research papers concerning the reconstruction of evidence deriving from forensic data. It presents two different groups of approaches: event presentation as a whole and reconstruction of specific elements.

4.4.1 Event Presentation. While aiming to enrich the chronological evidence presentation for forensic tools, Kasiaras et al. (2014) created the Android Forensic Data Analyzer (AFDA). Its operation is summarized in two phases. During the first phase, the tool executes common forensic investigation tasks, such as image mounting, evidence retrieval, hash creation, and report generation. The second phase consists of a timeline where the events associated to the acquired evidence and their correlated assets are presented in a chronological order. Moreover, it provides the investigator with the option of tracing the exact location history of the device by parsing geodata used by many different applications.

Zawoad and Hasan (2015) created a conceptual model of a mechanism responsible for preserving (in a secure database) and presenting [via GET requests to a "Representational State Transfer (REST) API" (Fielding 2000)] data acquired from mobile cloud investigations. The model was designed after enumerating the challenges the field of mobile cloud forensics is facing and highlighting the requirements for secure mobile cloud transactions.

The presentation of events that occurred during the conduction of a crime is undoubtedly a useful element. Its effectiveness is complemented by the reconstruction of evidence and other elements, which is elaborated below.

4.4.2 Reconstruction of Specific Elements. IM applications contain significant data for the outcome of an investigation. Reconstructing the information from various points of an Android device memory image has been the primary concern mentioned by Anglano (2014). Apart from the reassembly task, the author attempts to correlate various different events and timestamps related to the forensic artifacts.

Law enforcement agents, judges, and prosecutors need to have detailed answers to the questions rising when a series of incidents takes place. Kaart and Laraghy (2014) highlight this importance and perform a case study on detecting the intentional clock skewing in an Android device, by accessing the mmssms.db database.

The paper by Saltaformaggio et al. (2015) introduces GUITAR, an application-independent method capable of reconstructing Android application Graphical User Interfaces (GUIs) from their memory heaps, which reside in a forensically acquired memory image. The method uses a "depth-first topology recovery algorithm' to sort the fragmented application hierarchy. Afterwards, the application graphical pieces are united in the correct order with the aid of a "bipartite graph weighted assignment solver and a drawing content-based fitness function" (Saltaformaggio et al. 2015). In the end, a windowing system binary is used so as to create the final form of the redrawn application.

The next section discusses the recent advances in evidence parsing, one of the most fundamental concepts in the field of MF.

4.5 Evidence Parsing

The research works discussed in this section have two different objects of study. The first category contains data from social media and messaging applications, while the second category concerns various data and focuses on personal and hybrid information from various sources.

4.5.1 Messaging Data Parsing. Investigation for Skype artifacts in the NAND and RAM memory of mobile devices running the Android OS was performed by Al-Saleh and Forihat (2013). Live process dumping and logical acquisition methods were used and experiments took place with different Skype usage scenarios. Evidence parsing for Skype usage traces was performed manually and by utilities such as the grep tool and the Eclipse Memory Analyzer. The research pointed out that elements concerning Skype activities remain in both memory types and can be traced even after deletion.

In a mobile device forensic investigation, all acquired evidence should be taken into consideration, handled, and combined so as to reach a satisfactory conclusion. Data deriving from Social Networks (SNs) and their equivalent messaging applications are evidence sources that can facilitate an investigation process. Dezfouli et al. (2015) investigated SN applications in Android (4.2) and iOS (7.1.2) devices for elements of forensic interest. Examination of Facebook, Twitter, LinkedIn, and Google+ applications revealed that the majority of the user-related data (such as usernames, profile pictures, posts, and messages) other than passwords could be retrieved.

The next section describes the research conducted in a more diverse data type environment.

4.5.2 Personal/Hybrid Data Parsing. Data deriving from anonymizing services had also been a concern in the MF community. A case of forensic investigation of Orweb browser data in rooted and non-rooted Android devices was examined by Al Barghouthy et al. (2013). Acquisition was performed by the general purpose Titanium Backup application instead of a dedicated forensic tool. The use of the latter might have different effects on the amount of collected information. Moreover, the use of a backup tool created an unnecessary impediment, since the backup utility only functions properly in rooted devices. As a result, an image of the non-rooted device could not be retrieved, a fact that could have been avoided if a forensic tool was used. On the other end, data acquisition from a rooted device was successful: databases were parsed with the SQLite Database Browser and artifacts such as URLs, Facebook IDs and chat conversations were identified.

The FROST recovery image mentioned in Section 4.2 was further improved by Hilgers et al. (2014), by including the Volatility Framework (Volatile Systems 2011) and the LiME plug-in (504ensics Labs 2013). With this addition, the authors were still able to access the device RAM in case the user data partition was wiped due to manufacturer security measures. They also managed to successfully parse the RAM for call logs, information typed by the user in a short timeframe before the cold-boot attack, Personal Identification Numbers (PINs), passwords, and photo metadata.

Ntantogian et al. (2014) conducted experiments concerning the discovery of user credentials in different usage scenarios of various applications and use cases. The examination took place after live memory dumping of the target devices. The authors verified that as long as a mobile device remains powered on, it is highly likely that some user credentials will remain in its memory. Findings from the specific research also unveiled the incapability of task-killers and password protection applications to safeguard sensitive personal information (or to wipe it, if necessary). The research also revealed many application vulnerabilities and simultaneously opened new future perspectives in data protection and prevention of anti-forensic techniques.

Immanuel et al. (2015) highlighted the importance of searching various sources of information within a smartphone-acquired memory image that may contain data of forensic interest. They created an Android cache taxonomy out of 11 installed applications of different kinds and modeled the classification process. Each cache type (WebView, SQLite, Volley, Serialized Java Objects, Network File, and Custom) has different parsing methods. The authors developed a unified cache viewer application so as to facilitate the investigation procedure.

The next section is related to a subject with a higher degree of complexity than the acquisition of raw evidence: the actual representation of knowledge acquired from one or multiple mobile devices.

4.6 Knowledge Representation

In the case of MF, knowledge representation is present as a subset of the bigger DF set and not as a stand-alone discipline. In this section, we broaden the previously mentioned 7-year chronological span of research, because, to the best of our knowledge, some significant earlier papers are not present in previous surveys. This section is split in two categories: generic forensic concepts and digital evidence structural representation.

4.6.1 Generic Forensic Concepts. Brinson et al. (2006), created a cyber-forensics ontology as a tool for promotion of further research in the areas of specialization and certification, which were relatively weak at the time the article was published. More precisely, they constructed a high-level ontology, organized along the technological and professional contexts of every entity involved in a DF investigation. On the one hand, the professional branch classifies all the specialists who can make use of the forensic discipline or conduct forensic investigations. On the other hand, the technological branch involves hardware and software elements of forensic interest. Considering the current state of DF, this ontology looks somehow outdated in several aspects, a situation that highlights the need for continuous updates of such formal snapshots. For instance, Micro Read and live acquisition methods, as well as the Android OS itself were introduced after 2007.

An ontology branch can serve as a starting point for deeper conceptual analysis. Harrill and Mislan (2007) expanded the research work presented by Brinson et al. (2006). They dug deeper into the small-scale digital devices field and performed further analysis upon the devices themselves. Thus, they created a new, lower-level ontology from a branch of a previous version.

Finally, Karie and Venter (2014) created an ontology that fragments the DF discipline in smaller and more detailed subcategories, providing further specification on the objects of investigation. Such a classification is useful for investigators, academics, and forensic tool developers, thus offering a complete outline of elements to be taken into consideration.

While the current category is dedicated to concepts related to the forensic science in general, the following section is actually related to the fragmentation of evidence and the presentation of their structural elements.

4.6.2 Digital Evidence Structured Representation. Kahvedzic and Kechadi (2009) designed a generic format, application-independent ontology named Digital Investigation Ontology

(DIALOG), which they claim that can be used as an independent semantic vocabulary for describing any forensic event at different depths of detail. Moreover, they expanded their work by using it as a means of modeling the Windows Registry.

In an effort to create a starting point for future intelligent NF implementations, Saad and Traore (2010) used the Web Ontology Language (OWL) to structure an ontology containing both NF concepts and problem-solving sets. Network entities, assets, attacks, and interactions between them are represented in a detailed knowledge base.

The increasing volume of acquired data (Quick and Choo 2014), together with the evolving diversity of forensic techniques and the variety of systems under investigation, contribute to the increased complexity of the MF discipline. Consequently, creating rules and other formal representations for the aforementioned categories is rather complicated. As a result, some researchers have considered other aspects, such as the presentation of digital evidence and associated investigation activities as a more convenient approach. This is the case of the Cyber Observable eXpression (CybOX) (The MITRE CORPORATION 2015), developed by the U.S. Department of Homeland Security Office of Cybersecurity Communications. Its purpose is to classify digital evidence and relevant actions within their context from a generic point of view, which can be applied to various use cases, such as intrusion detection, data correlation, and DF.

CybOX was also extended by Casey et al. (2014), who proposed the Digital Forensics Analysis eXpression (DFAX) ontology. This classification involves technical information, data representation, and corresponding actions in higher and lower levels of abstraction. Moreover, they describe the concept of a Unified Cyber Ontology (UCO), which allows the interoperation of DFAX and similar CybOX-based ontologies, such as Structured Threat Information Expression (STIX) (Barnum 2012).

Among the considerable advances enabled by representation of knowledge for mobile criminal investigation, automation of investigation processes stands out. This will be the subject of the next section.

4.7 Automated Classification and Analysis of User and Application Behavior

The current section addresses research in the field of automation for digital investigation. It is organized in two categories: research works dedicated specifically to the discipline of MF, and general-purpose forensic methodologies, which can be applied to the MF field with some modifications.

4.7.1 Methodologies Related to MF. In an effort to optimize the investigation process during triage, Walls et al. (2011) proposed DEC0DE, a library of Probabilistic Finite State Machines (PFSMs) based on successfully imaged devices. The tool operation includes two steps. First, the byte stream of an acquired physical image is inserted into a filtering mechanism of hashes belonging to previously examined devicesto exclude a load of insignificant information. Second, the remaining data enter a multi-step inference component, based on a set of PFSMs so as to conclude the automatic recognition of critical data sequences, such as phone numbers, names, messages, photographs, videos, documents, and audio clips.

Marturana et al. (2011) introduced a triaging method based on self-knowledge algorithms to predict user behavior and to classify mobile devices between suspects of content abusing or not. Their experiment consisted of tests with 21 different Android devices, applying three different machine learning techniques (Bayesian networks, decision trees, locally weighted learning) and validating the method that was initially used.

During their operation, mobile applications produce volatile and non-volatile traces that can be associated to the users' activities. Michalas and Murray (2016) introduced MemTri, a memory forensics tool based on the principles of the Volatility Framework (Volatile Systems 2011).

MemTri uses regular expressions to identify illegal activity patterns from a seized memory image. Afterwards, a Bayesian network is used to calculate the device owner's probability of criminal involvement. The specific tool was successfully evaluated in a later paper by Michalas and Murray (2017).

4.7.2 General Purpose Forensics Methodologies. This section discusses some research papers with general purpose forensic methodologies which, nonetheless, may be relevant to MF.

Text mining and content clustering from documents were addressed by Nassif and Hruschka (2011). The authors applied six clustering algorithms on text documents acquired from actual CF investigations and discovered verbal patterns that could aid future examinations conducted by experts.

Upon adoption of the cloud as a forensic platform, Lee and Hong (2011) propose a service named Forensic Cloud, which applies a logic-centered approach to the way a digital investigation is conducted—replacing the prevailing technology-centered approaches. The authors applied a model of index search on forensically acquired data, supported by a distributed system on cloud servers. Even though the indexing process is rather slow, the final result compensates the time spent. Moreover, their framework uses data abstraction techniques to provide a more realistic data representation to the investigator on the client side. Instead of bulk evidence listing, relevant data are grouped, thus facilitating decision-making and association procedures.

Platzer et al. (2014) introduced Skin-Sheriff, a method which uses machine learning techniques for detecting nude skin among acquired data. Despite not being dedicated to MF, this is applicable to every sub-discipline of DF where photographs are retrieved as evidence.

4.8 Wrap-Up

Table 1 enlists the key research works discussed in this survey, grouped by the six categories mentioned at the beginning of this section. Despite the fact that research in the field of MF has advanced in quite an impressive and multi-purpose way, there are many issues and research challenges that still need to be addressed. In the following section, we identify and discuss these open issues.

5 OPEN ISSUES AND RESEARCH CHALLENGES

This section addresses the open issues and key research challenges of the MF discipline, organized in the following categories: data-related issues, forensic tools, device and operating system aspects, security-related issues, and cloud-related aspects. This grouping, combined with the literature classification, provides useful research directions for the future of the field. Some of the following challenges and issues do not belong exclusively to the MF field and may as well affect other DF disciplines. However, their influence on MF makes them noteworthy.

5.1 Data-Related Issues

Anonymity on the internet can bring a number of new issues to researchers. Usage of incognito browsers and other anonymity services may unintentionally create additional difficulties in recovering the true identity behind the user's profile. This also facilitates intentional IP and MAC address spoofing (Wazid et al. 2013).

One of the more persistent issues is the considerable volume of data acquired during an investigation. Such volumes may cause management issues, increasing costs and processing time (Quick and Choo 2014). Especially when acquired data need to be accessed more than once, such as in cases of training datasets or behavioral analysis, the storage problem also arises. Ever-increasing storage capacity in smartphones and support of cloud storage services further aggravates this situation.

Table 1. Literature Review Timeline

Year	Subject	Reference
	File Acquisition and Data Integrity	
2010	Memgrab: live acquisition tool	Thing et al. (2010)
2012	Live backup file with process updates	Dezfouli et al. (2012)
	iOS camera connection kit acquisition	Gomez-Miralles and Arnedo-Moreno (2012)
	Live backup discovery of encrypted files	Kotsopoulos and Stamatiou (2012)
	User and cloud interaction study	Marturana et al. (2012)
2013	Testing encryption efficiency of acquired artifacts	Al Barghouthy et al. (2013)
	Search for cloud storage application artifacts	Grispos et al. (2013)
	Prototype monitoring for live acquisition	Grover (2013)
	Cold boot attacks recovery	Müller and Spreitzenbarth (2013)
	Especially modified bootloader	Votipka et al. (2013)
	Secure-logging-as-a-service	Zawoad et al. (2013)
2015	Smartwatches acquisition	Baggili et al. (2015)
	MEGA cloud storage acquisition	Daryabar et al. (2015)
	Live OS adversary model for cloud storage acquisition	Do et al. (2015)
	CSP snapshot	Grispos et al. (2015)
	Storage and notes cloud application acquisition	Martini et al. (2015a)
	Ubuntu One WP and iOS acquisition	Shariati et al. (2015)
2016	Android and WP cloud and communication applications acquisition	Cahyani et al. (2016b)
	SugarSync Android, WP, and iOS acquisition	Shariati et al. (2016)
	Identification of Malicious Activity and Malware Analysis	
2011	Cloud Proxy IDS	Houmansadr et al. (2011)
	Volatility framework	Volatile Systems (2011)
	AppAware permission abuse detection	Di Cerbo et al. (2011)
2012	Malware reverse engineering	Li et al. (2012)
2013	Mobile wiretrap fake network	Schutz et al. (2013)
2014	Process dumping malware analysis	Hanaysha et al. (2014)
	Evidence Reconstruction and Preservation	
	Event reconstruction from WhatsApp artifacts	Anglano (2014)
	Clock skew detection and timestamp study	Kaart and Laraghy (2014)
	AFDA: Tool with extended presentation capabilities	Kasiaras et al. (2014)
2015	Database and REST API of cloud MF data	Saltaformaggio et al. (2015)
	GUITAR: GUI reconstruction technique	Zawoad and Hasan (2015)
	Evidence Parsing	
2013	Anonymous evidence tracing	Al Barghouthy et al. (2013)
	Search for Skype artifacts in NAND and RAM memory	Al-Saleh and Forihat (2013)
2014	FROST expansion with the Volatility Framework	Hilgers et al. (2014)
	Search for authentication credentials in forensic data	Ntantogian et al. (2014)
2015	Search for forensically interesting data in social media apps	Dezfouli et al. (2015)
	Knowledge Representation	
<2011	Technical and professional DF concepts	Brinson et al. (2006)
	Brinson's expansion for small digital devices	Harrill and Mislan (2007)
	DIALOG	Kahvedzic and Kechadi (2009)
2012	STIX for CybOX	Barnum (2012)

(Continued)

Table 1. Continued

Year	Subject	Reference
2014	CybOX expansion	Casey et al. (2014)
	DF fragmentation and expansion	Karie and Venter (2014)
	Automated Classification and Analysis of User and Application Behavior	
2011	Forensic Cloud: High-level indexed model	Lee and Hong (2011)
	DEC0DE: Library of probabilistic finite state machines	Walls et al. (2011)
	Classification of legal and illegal smartphone usage	Marturana et al. (2011)
2014	Skin-Sheriff: Machine learning-based nude image recognition	Platzer et al. (2014)
2016	MemTri: Illegal pattern identification	Michalas and Murray (2016)

Apple devices running iOS version 8 or newer and Android devices shipping with Android version 6.0 and onwards will have mandatory full disk encryption enabled by default [Apple Inc. 2016; Google Inc. 2016]. Particularly in Android devices, the encryption key will no longer be derived by the user-defined lock-screen password, but will be hardware-based instead. Even though this helps in securing users' sensitive data, it creates a major obstacle for law enforcement. Investigators will no longer be able to acquire access to the data in the same way as in the past. Forensic tools will also need to be adapted to be capable of handling the new OS versions. Alternatively, RAM acquisition and analysis techniques should be further researched, so as to become capable of acquiring or searching for data that would otherwise be found in the user data partitions.

5.2 Forensic Tools-Related Issues

For a relatively long timespan, MF research papers were mainly focusing on acquisition techniques, while minor importance was given to the other phases of the investigative process model. This problem is noticeable in various proprietary and open source MF tools, which require investigation to be performed manually or off-tool (using third party software). More specifically, a "significant lack of advanced tools that enable the correlation among various events of forensic interest in order to reduce the cognitive load on the analysts' side" (Kasiaras et al. 2014) has been noted.

In the long term, forensic tools should also adopt common models for formal representation of acquired data. This would not only facilitate the standardization procedure, but also encourage future evaluation of different tools for academic and corporate purposes—serving as a body of knowledge and source of rule generation for automated and intelligent MF.

Anti-forensics consist of "any attempt to compromise the availability or usefulness of evidence to the forensics process" (Harris 2006). This can be achieved by means such as data hiding, artifact wiping, trail obfuscation, and attacks on the forensic tools themselves (Kessler 2007), and will remain a major threat for forensic practitioners. Efficient counter-measures and continuous software updates are the key to battle this threat, since anti-forensic techniques will continue to evolve side-by-side with the progress of forensics tools.

5.3 Device and Operating Systems Diversity

Another major challenge is how the enormous diversity of devices, hardware components, OSs, and software is affecting the roadmap towards a general methodology of data collection and analysis upon investigation. Different technologies increase divergence between the implemented MF tools in terms of functionality and presentation of results (Votipka et al. 2013). Moreover, they may cause compatibility issues even between devices of the same family.

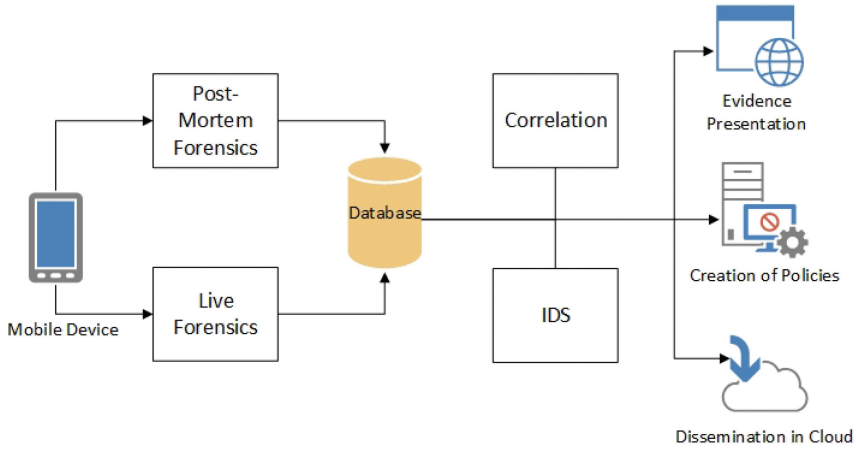

Fig. 4. Forensics architecture proposed in the SALUS project (SALUS 2014).

This issue also reflects on the existing literature. Most of the research papers and tools focus either on Android or iOS devices, with few generic solutions applicable to both ecosystems or even to different versions within the same ecosystem. Furthermore, other ecosystems, such as Windows Phone, are usually left out of research. A report about the results of a JTAG acquisition on a Nokia Lumia 520 device running WP8 (Murphy et al. 2016) and a journal paper about acquisition of a tablet running Windows RT (Iqbal et al. 2014) were some of the few exceptions to the rule.

5.4 Security Aspects

The non-stop evolution of new and zero-day malware brings new challenges to the forensic ecosystem. Tools should be updated towards the new state-of-the-art, so as to meet the current functionality requirements and to be designed in a way that anti-forensic methods should be avoided or halted.

The discipline of MF plays a crucial rule in environments such as Public Protection and Disaster Relief (PPDR) systems, where preservation of information is rather critical and mobility is a requirement. In the context of a PPDR system, agencies prompted to "cope with unexpected disasters and emergencies of any scale are dependent on the infrastructure and support that they have in place for their day-to-day operations" (Jamieson 2004). Information collected by the PPDR system devices not only serves as valuable evidence in case of need, but also as an analysis background for malicious activity recognition and identification.

Previous work from the authors proposes a high-level architecture, which incorporates live and post-mortem forensic acquisition, for the mobile device data to serve as a ground for malicious activity detection and recognition (Barbatsalou et al. 2015). The proposed architecture (depicted in Figure 4) was implemented in the context of the SALUS FP7 European Project (SALUS 2014).

In the SALUS framework, a mobile device is examined both with *post-mortem* and *live* forensic tools, to acquire volatile and non-volatile content that is stored on a database. With data deriving from a correlation engine and alerts generated from an IDS that coexist in the system, data can be associated to malicious activity and logical rules can be generated. Moreover, statistics concerning the overall system performance can be exported and reports or rule updates can be disseminated. Last but not least, acquired data can be used for visualized event reconstruction.

5.5 Cloud-Related Issues

The cloud involvement does not stop at the excessive data issues. MF with cloud contribution needs to have a whole new perspective on the investigative process model, since factors such as data storage in remote virtual machines and their availability affect the investigation process, which needs to address both mobile device and cloud levels (Samet et al. 2014).

The majority of existing MF tools do not consider cloud aspects. There are reported cases of tools that have some support for remote acquisition (Dykstra and Sherman 2012) but, to the best of the authors' knowledge, no serious effort towards effectively cloud-aware MF tools has been made yet. Moreover, it is important to note that forensic tools with cloud support will have different requirements for the different service models (SaaS, IaaS, Paas) (Zawoad and Hasan 2013).

The cloud environment is a distributed system, so when it comes to forensic investigations, data can be stored in different virtual systems. This raises two questions. First, if data from different users stored at the same location are safe from accidental trespassing or alteration. Second, if the legislation of the country where the firms providing cloud services are located complies with the regulations and standards of current forensic investigations (Grispos et al. 2012).

Creating the appropriate circumstances so as to ensure that evidence is not altered during a cloud investigation is another obstacle to overcome (Rogers 2013). Delport et al. (2011) expressed their concern on the fact that a cloud entity under investigation should be isolated to avoid intentional or unintentional damage. The confusion of multiple CSP instances on different devices and its management is also a factor to be taken into consideration during the investigation process.

Cloud service security breaches that led to data leakage and large-scale denials of service have been some of the most persistent issues during the past few years for both CSPs and end users (Barona and Anita 2017). Evidence from previous device and CSP investigations should be used so as to facilitate the generation of countermeasures against data leaks and other attack types.

Last, a framework that allows access to CSP logs has to be generated. In an environment as volatile as the cloud, logging can be very crucial for the course of an investigation, and information with respect to individual and third-party privacy has to be disseminated to the entities involved.

5.6 Process Automation

It is notable that the MF categories less addressed by research are evidence reconstruction and presentation and automated classification and analysis of user and application behavior, despite their obvious relevance. Concerning automated evidence classification in particular, it is rather disappointing to infer that, after early attempts around 2011, to the best of our knowledge, only a couple of papers addressed the issue.

Meanwhile, many authors are concerned with the lack of automated methods during the analysis phase of the investigative process model. Data analysis and classification are still performed mostly manually, leading to the need for further research towards the automation of such procedures. The investigation parts that are in need of automation have to be clarified and formalized. There are five main categories for which automation and application of hard and soft computing methods would be feasible:

(1) Data and artifacts classification
(2) User behavioral patterns and their adaptation
(3) Application and system related process categorization for potential discovery of malicious activity
(4) Correlation between incidents after data analysis from different sources
(5) Creation of logical rules deriving from data patterns and tuning among them, so as to pinpoint towards specific crime types.

More precisely, machine learning can be used to classify retrieved elements from memory images according to their data types, whether they are user-, application-, or system-generated. Moreover, the same memory, process, or file system dumps can be examined and user behavior patterns can be extracted from them. Those patterns can be used in the future for user identification and serve in cases when unauthorized use by identity theft has to be traced and halted. Last, machine learning techniques can contribute to the evolution of automatic categorization of malicious activity. Additionally, acquired data can be normalized and used as inputs for rule generation for fuzzy inference systems, neural networks, or neuro-fuzzy systems (Barmpatsalou et al. 2017).

6 CONCLUSIONS

Mobile devices and wearables are literally connected to people's lives, in a higher level than personal computers or other digital devices. For instance, people have become highly dependent on smartphones, using them for significantly more tasks than desktop computers or laptops, therefore increasing the amount of data being stored and processed in such equipment. Moreover, most users do not hesitate to voluntarily sacrifice a certain level of privacy in exchange for additional convenience, by storing valuable personal data for ubiquitous and immediate accessibility. Cloud-based applications are also partly to blame for this reality, by removing the portability barriers from the devices. In fact, they have become so commonplace that several users are not even aware of their usage. For these reasons, mobile devices have become their owners' digital witnesses, a situation which highlights the importance of the MF discipline in future criminal investigations.

After the literature review in Section 4, it is noteworthy that the notion of MF is something more than physical or logical data acquisition. Research in MF has shown substantial advances during the last 7 years. However, further efforts should be made in favor of automated procedures, so as to actually facilitate future investigations (Homem 2016). Moreover, advances in research and development should also require the reviewing of standards and regulations for synchronization purposes and to avoid the characterization of innovative methods as invasive or prohibited.

Another discussion point concerns the future of forensic tools and their interoperability. Forensic tools store data in different formats, including various types of databases and data structures. However, the specific trait makes the procedure of future standardization rather inconvenient and not easily achievable. A possible scenario that would facilitate the specific procedure is the creation of unified data formats for data acquired by forensic tools.

New contextualization, such as the participation of mobile devices in scenarios including moderate to heavy use of cloud services, should be taken into consideration. The particular fact gives a whole new direction to the way that jurisdictional events are taking place and to how an investigation for elements of forensic interest is conducted. Industry and academia should follow the specific path for integrating the cloud concept into their future implementations.

ACKNOWLEDGMENTS

This work was partially funded by the Centro 2020 Mobitrust Project (reference CENTRO-01-0247-FEDER-003343). We also thank the team of the ATENA H2020 EU Project (Reference No. H2020-DS-2015-1, Project No. 700581) for the support, fruitful discussions, and feedback.

REFERENCES

504ensics Labs. 2013. LiME—Linux Memory Extractor. Retrieved April 10, 2015, from https://github.com/504ensicsLabs/LiME/tree/master/doc.

Cosimo Anglano. 2014. Forensic analysis of Whatsapp messenger on Android smartphones. Special Issue: Embedded Forensics, *Digital Investig.* 11, 3 (2014), 201–213.

Apple Inc. 2016. *iOS Security White Paper*. Technical Report. Apple Inc. https://www.apple.com/business/docs/iOS_Security_Guide.pdf.

Claudio A. Ardagna, Rasool Asal, Ernesto Damiani, and Quang Hieu Vu. 2015. From security to assurance in the cloud: A survey. *ACM Comput. Surv.* 48, 1 (July 2015), Article 2, 50 pages. DOI: http://dx.doi.org/10.1145/2767005

Autopsy. 2016. Autopsy—The Sleuth Kit. Retrieved January 12, 2016, from http://www.sleuthkit.org/autopsy.

Rick Ayers, Sam Brothers, and Wayne Jansen. 2014. *NIST Special Publication 800-101, Guidelines on Mobile Device Forensics: Revision 1.* Technical Report SP 800-101. National Institute of Standards and Technology, Gaithersburg, MD. DOI: http://dx.doi.org/10.6028/NIST.SP.800-101r1

Lee Badger, Tim Grance, Robert Patt-Corner, and Jeff Voas. 2012. *NIST Special Publication 800-146, Cloud Computing Synopsis and Recommendations.* Technical Report SP 800-146. National Institute of Standards and Technology, Gaithersburg, MD.

Ibrahim Baggili, Jeff Oduro, Kyle Anthony, Frank Breitinger, and Glenn McGee. 2015. Watch what you wear: Preliminary forensic analysis of smart watches. In *Proceedings of the 2015 10th International Conference on Availability, Reliability, and Security (ARES'15)*, 303–311. DOI: http://dx.doi.org/10.1109/ARES.2015.39

Konstantia Barmpatsalou, Bruno Sousa, Edmundo Monteiro, and Paulo Simoes. 2015. Mobile forensics for PPDR communications: How and why. In *Proceedings of the 10th International Conference on Cyber Warfare and Security (ICCWS'15).* 30.

Nedaa Baker Al Barghouthy, Andrew Marrington, and Ibrahim Baggili. 2013. The forensic investigation of android private browsing sessions using Orweb. In *Proceedings of the 2013 5th International Conference on Computer Science and Information Technology (CSIT'13).* 33–37. DOI: http://dx.doi.org/10.1109/CSIT.2013.6588754

Nedaa Baker Al Barghouthy and Huwida Said. 2013. Social networks IM forensics: Encryption analysis. *J. Commun.* 8, 11 (2013), 708–715.

Konstantia Barmpatsalou, Tiago Cruz, Edmundo Monteiro, and Paulo Simoes. 2017. Fuzzy system-based suspicious pattern detection in mobile forensic evidence. In *Proceedings of the 9th EAI International Conference on Digital Forensics and Cyber Crime.*

Konstantia Barmpatsalou, Dimitrios Damopoulos, Georgios Kambourakis, and Vasilios Katos. 2013. A critical review of 7 years of mobile device forensics. *Digital Investig.* 10, 4 (2013), 323–349. DOI: http://dx.doi.org/10.1016/j.diin.2013.10.003

Sean Barnum. 2012. *Structured Threat Information eXpression.* Technical Report. MITRE corporation. http://stix.mitre.org/about/documents/STIX_Whitepaper_v1.0.pdf.

R. Barona and E. A. M. Anita. 2017. A survey on data breach challenges in cloud computing security: Issues and threats. In *Proceedings of the 2017 International Conference on Circuit, Power, and Computing Technologies (ICCPCT'17).* 1–8. DOI: http://dx.doi.org/10.1109/ICCPCT.2017.8074287

Ashley Brinson, Abigail Robinson, and Marcus Rogers. 2006. A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Digital Investig.* 3 (Sept. 2006), 37–43. DOI: http://dx.doi.org/10.1016/j.diin.2006.06.008

N. D. W. Cahyani, B. Martini, K.-K. R. Choo, and A. K. B. P. Muhammad Nuh Al-Azhar. 2016a. Forensic data acquisition from cloud-of-things devices: Windows smartphones as a case study. *Concurrency and Computation: Practice and Experience* 29, 14, e3855. DOI: http://dx.doi.org/10.1002/cpe.3855 CPE-16-0086.R1.

Niken Dwi Wahyu Cahyani, Nurul Hidayah Ab Rahman, Zheng Xu, William Bradley Glisson, and Kim-Kwang Raymond Choo. 2016b. The role of mobile forensics in terrorism investigations involving the use of cloud apps. In *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications (MobiMedia'16).* 199–204. http://dl.acm.org/citation.cfm?id=3021385.3021421

Eoghan Casey. 2011. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press.

Eoghan Casey. 2013. Smartphone forensics and mobile malware analysis. Retrieved February 4, 2015, from http://www.caseite.com/content/smartphone-forensics-and-mobile-malware-analysis.

Eoghan Casey, Greg Back, and Sean Barnum. 2014. Leveraging CybOX to standardize representation and exchange of digital information. *Digital Investig.* 12 (2014), S102–S110. DOI: http://dx.doi.org/10.1016/j.diin.2015.01.014

Cellebrite Predictions. 2015. Mobile Forensics: A look ahead. Retrieved April 10, 2015, from http://www.cellebrite.com/Media/Default/Files/CellebritePredictions20Survey202015.pdf.

Sheng-Wen Chen, Chung-Huang Yang, and Chien-Tsung Liu. 2011. Design and implementation of live SD acquisition tool in Android smart phone. In *Proceedings of the 2011 5th International Conference on Genetic and Evolutionary Computing (ICGEC'11).* 157–162. DOI: http://dx.doi.org/10.1109/ICGEC.2011.46

Yan Cheng. 2011. Cybercrime forensic system in cloud computing. In *Proceedings of the 2011 International Conference on Image Analysis and Signal Processing (IASP'11).* 612–615. DOI: http://dx.doi.org/10.1109/IASP.2011.6109117

Hyunji Chung, Jungheum Park, Sangjin Lee, and Cheulhoon Kang. 2012. Digital forensic investigation of cloud storage services. *Digital Investig.* 9, 2 (2012), 81–95. DOI: http://dx.doi.org/10.1016/j.diin.2012.05.015

Christian D'Orazio, Aswami Ariffin, and Kim-Kwang Raymond Choo. 2014. iOS Anti-forensics: How can we securely conceal, delete and insert data? In *Proceedings of the 2014 47th Hawaii International Conference on System Sciences (HICSS'14).* 4838–4847. DOI: http://dx.doi.org/10.1109/HICSS.2014.594

Farid Daryabar, Ali Dehghantanha, and Kim-Kwang Raymond Choo. 2015. Cloud storage forensics: MEGA as a case study. *Aust. J. Forensic Sci.* 49, 3, 1–14. DOI: http://dx.doi.org/10.1080/00450618.2016.1153714

Waldo Delport, Martin S. Olivier, and Michael Kohn. 2011. Isolating a cloud instance for a digital forensic investigation. In *Proceedings of the Conference on Information Security for South Africa (ISSA'11)*.

Farhood Norouzizadeh Dezfouli, Ali Dehghantanha, Brett Eterovic-Soric, and Kim-Kwang Raymond Choo. 2015. Investigating social networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. *Aust. J. Forensic Sci.* 48, 4, 1–20. DOI: http://dx.doi.org/10.1080/00450618.2015.1066854

Farhood Norouzizadeh Dezfouli, Ali Dehghantanha, Ramlan Mahmoud, Nor Fazlida Binti Mohd Sani, and Solahuddin bin Shamsuddin. 2012. Volatile memory acquisition using backup for forensic investigation. In *Proceedings of the 2012 International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec'12)*. 186–189. DOI: http://dx.doi.org/10.1109/CyberSec.2012.6246108

Francesco Di Cerbo, Andrea Girardello, Florian Michahelles, and Svetlana Voronkova. 2011. Detection of malicious applications on Android OS. In *Computational Forensics*. Lecture Notes in Computer Science, Vol. 6540. Springer, 138–149. DOI: http://dx.doi.org/10.1007/978-3-642-19376-7_12

Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. 2015. A forensically sound adversary model for mobile devices. *PLoS ONE* 10, e0138449. DOI: http://dx.doi.org/10.1371/journal.pone.0138449

Josiah Dykstra and Alan T. Sherman. 2012. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investig.* 9, Supplement (2012), S90–S98. DOI: http://dx.doi.org/10.1016/j.diin.2012.05.001.

Jason Farina, Mark Scanlon, Nhien-An Le-Khac, and Mohand Tahar Kechadi. 2015. Overview of the forensic investigation of cloud services. In *Proceedings of the 2015 10th International Conference on Availability, Reliability, and Security (ARES'15)*. 556–565. DOI: http://dx.doi.org/10.1109/ARES.2015.81

Roy Thomas Fielding. 2000. *Architectural Styles and the Design of Network-Based Software Architectures*. Ph.D. Dissertation. University of California, Irvine.

Luis Gomez-Miralles and Joan Arnedo-Moreno. 2012. Versatile iPad forensic acquisition using the Apple camera connection kit. *Comput. Math. Appl.* 63, 2 (2012), 544–553. DOI: http://dx.doi.org/10.1016/j.camwa.2011.09.053

Google Inc. 2016. *Compatibility Definition Android 6.0*. Technical Report. Google Inc. https://static.googleusercontent.com/media/source.android.com/en//compatibility/android-cdd.pdf.

George Grispos, William Bradley Glisson, and Tim Storer. 2013. Using smartphones as a proxy for forensic evidence contained in cloud storage services. arXiv:1303.4078.

George Grispos, William Bradley Glisson, and Tim Storer. 2015. Recovering residual forensic data from smartphone interactions with cloud storage providers. In *The Cloud Security Ecosystem*, R. K.-K. R. Choo (Ed.). Syngress, Boston, MA, 347–382. DOI: http://dx.doi.org/10.1016/B978-0-12-801595-7.00016-1

George Grispos, Tim Storer, and William Bradley Glisson. 2011. A comparison of forensic evidence recovery techniques for a Windows mobile smart phone. *Digital Investig.* 8, 1 (July 2011), 23–36. DOI: http://dx.doi.org/10.1016/j.diin.2011.05.016

George Grispos, Tim Storer, and William Bradley Glisson. 2012. Calm before the storm: The challenges of cloud computing in digital forensics. arXiv:1410.2123. http://arxiv.org/abs/1410.2123

Justin Grover. 2013. Android forensics: Automated data collection and reporting from a mobile device. *Digital Investig.* 10, Supplement (2013), S12–S20. DOI: http://dx.doi.org/10.1016/j.diin.2013.06.002

Tareq Hanaysha, Dale Lindskog, and Ron Ruhl. 2014. Using open source tools to investigate malware in the Android operating system. In *Proceedings of the Master of Information Systems Security Research 2014 Convocation*. 1–8.

David Christopher Harrill and Richard P. Mislan. 2007. A small scale digital device forensics ontology. *Small Scale Device Forensics J.* 1, 1 (2007).

Ryan Harris. 2006. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investig.* 3, Supplement (2006), 44–49. DOI: http://dx.doi.org/10.1016/j.diin.2006.06.005

Andri P. Heriyanto. 2013. Procedures and tools for acquisition and analysis of volatile memory on Android smartphones. In *Proceedings of the 11th Australian Digital Forensics Conference*. http://ro.ecu.edu.au/adf/123.

Christian Hilgers, Holger Macht, Tilo Müller, and Michael Spreitzenbarth. 2014. Post-mortem memory analysis of cold-booted Android devices. In *Proceedings of the 2014 8th International Conference on IT Security Incident Management IT Forensics (IMF'14)*. 62–75. DOI: http://dx.doi.org/10.1109/IMF.2014.8

Irvin Homem. 2016. Towards automation in digital investigations: Seeking efficiency in digital forensics in mobile and cloud environments. In *Proceedings of the Afternoon Session on 1-Rootkit and Network Security and Forensics*.

Andrew Hoog. 2011. *Android Forensics: Investigation, Analysis and Mobile Security for Google Android*. Syngress Publishing.

Amir Houmansadr, Saman A. Zonouz, and Robin Berthier. 2011. A cloud-based intrusion detection and response system for mobile phones. In *Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems and Networks Workshops (DSN-W'11)*. 31–32. DOI: http://dx.doi.org/10.1109/DSNW.2011.5958860

Felix Immanuel, Ben Martini, and Kim-Kwang Raymond Choo. 2015. Android cache taxonomy and forensic process. In *Proceedings of the 2015 IEE Trustcom/BigDataSE/ISPA Conference,* Vol. 1. 1094–1101. DOI: http://dx.doi.org/10.1109/Trustcom.2015.488

Asif Iqbal, Hanan Al Obaidli, Andrew Marrington, and Andy Jones. 2014. Windows surface {RT} tablet forensics. *Digital Investig.* 11, Supplement 1 (2014), S87–S93. DOI: http://dx.doi.org/10.1016/j.diin.2014.03.011

ISO/IEC. 2012. *Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence.* ISO/IEC.

ISO/IEC. 2015a. *Guidelines for the Analysis and Interpretation of Digital Evidence.* ISO/IEC.

ISO/IEC. 2015b. *Guidelines for the Analysis and Interpretation of Digital Evidence.* ISO/IEC.

Alan R. Jamieson. 2004. *Radiocommunication for Public Protection and Disaster Relief.* Technical Report. International Telecommunication Union. https://www.itu.int/itunews/manager/display.asp?lang=en&year=2006&issue=03&ipage=publicProtection&ext=html.

Wayne Jansen and Richard P. Ayers. 2007. *NIST Special Publication 800-101, Guidelines on Cell Phone Forensics.* Technical Report SP 800-101. National Institute of Standards and Technology, Gaithersburg, MD.

Marnix Kaart and Susan Laraghy. 2014. Android forensics: Interpretation of timestamps. *Digital Investig.* 11, 3 (2014), 234–248. DOI: http://dx.doi.org/10.1016/j.diin.2014.05.001

Damir Kahvedzic and Mohand Tahar Kechadi. 2009. DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge. *Digital Investig.* 6, Supplement (2009), S23–S33. DOI: http://dx.doi.org/10.1016/j.diin.2009.06.014

Nickson M. Karie and Hein S. Venter. 2014. Toward a general ontology for digital forensic disciplines. *J. Forensic Sci.* 59, 5 (2014), 1231–1241. DOI: http://dx.doi.org/10.1111/1556-4029.12511

Dimitrios Kasiaras, Thomas Zafeiropoulos, Nathan Clarke, and Georgios Kambourakis. 2014. Android forensics: Correlation analysis. In *Proceedings of the 2014 9th International Conference for Internet Technology and Secured Transactions (ICITST'14).* 157–162. DOI: http://dx.doi.org/10.1109/ICITST.2014.7038797

Mohand Tahar Kechadi, Muhammad Faheem, and Nhien An Le-Khac. 2015. The state of the art forensic techniques in mobile cloud environment: A survey, challenges and current trends. *Int. J. Digit. Crime For.* 7, 2 (April 2015), 1–19. DOI: http://dx.doi.org/10.4018/ijdcf.2015040101

Gary C. Kessler. 2007. Anti-forensics and the digital investigator. In *Proceedings of the 5th Australian Digital Forensics Conference.*

Atta ur Rehman Khan, Mazliza Othman, Sajjad Ahmad Madani, and Samee Ullah Khan. 2014. A survey of mobile cloud computing application models. *IEEE Comm. Surve. Tutor.* 16, 1, 393–413. DOI: http://dx.doi.org/10.1109/SURV.2013.062613.00160

Coert Klaver. 2010. Windows mobile advanced forensics. *Digital Investig.* 6, 3–4 (May 2010), 147–167. DOI: http://dx.doi.org/10.1016/j.diin.2010.02.001

Michael Donovan Kohn, Mariki M. Eloff, and Jan H. P. Eloff. 2013. Integrated digital forensic process model. *Comput. Sec.* 38, 103–115. DOI: http://dx.doi.org/10.1016/j.cose.2013.05.001

Panayiotis A. Kotsopoulos and Yiannis Stamatiou. 2012. Uncovering mobile phone users' malicious activities using open source tools. In *Proceedings of the 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM'12).* 927–933. DOI: http://dx.doi.org/10.1109/ASONAM.2012.165

Jooyoung Lee and Do Won Hong. 2011. Pervasive forensic analysis based on mobile cloud computing. In *Proceedings of the 2011 3rd International Conference on Multimedia Information Networking and Security (MINES'11).* 572–576. DOI: http://dx.doi.org/10.1109/MINES.2011.77

Juanru Li, Dawu Gu, and Yuhao Luo. 2012. Android malware forensics: Reconstruction of malicious events. In *Proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW'12).* 552–558. DOI: http://dx.doi.org/10.1109/ICDCSW.2012.33

Silas Luttenberger and Reiner Creutzburg. 2011. Forensic investigation of certain types of mobile devices. *Proc. SPIE* 7881 (2011), 78810Q. DOI: http://dx.doi.org/10.1117/12.879319

Ben Martini and Kim-Kwang Raymond Choo. 2012. An integrated conceptual digital forensic framework for cloud computing. *Digital Investig.* 9, 2 (2012), 71–80. DOI: http://dx.doi.org/10.1016/j.diin.2012.07.001

Ben Martini and Kim-Kwan Raymond Choo. 2014. Cloud forensic technical challenges and solutions: A snapshot. *IEEE Cloud Computing* 1, 4 (Nov 2014), 20–25. DOI: http://dx.doi.org/10.1109/MCC.2014.69

Ben Martini, Quang Do, and Kim-Kwang Raymond Choo. 2015a. Conceptual evidence collection and analysis methodology for Android devices. In *The Cloud Security Ecosystem*, R. K.-K. R. Choo (Ed.). Syngress, Boston, MA, 285–307. DOI: http://dx.doi.org/10.1016/B978-0-12-801595-7.00014-8

Ben Martini, Quang Do, and Kim-Kwang Raymond Choo. 2015b. Mobile cloud forensics: An analysis of seven popular Android apps. In *The Cloud Security Ecosystem*, R. K.-K. R. Choo (Ed.). Syngress, Boston, MA, 309–345. DOI: http://dx.doi.org/10.1016/B978-0-12-801595-7.00015-X

Fabio Marturana, Gianluigi Me, Rosamaria Berte, and Simone Tacconi. 2011. A quantitative approach to triaging in mobile forensics. In *Proceedings of the 2011 IEEE 10th International Conference on Trust, Security, and Privacy in Computing and Communications (TrustCom'11).* 582–588. DOI: http://dx.doi.org/10.1109/TrustCom.2011.75

Fabio Marturana, Gianluigi Me, and Sergio Tacconi. 2012. A case study on digital forensics in the cloud. In *Proceedings of the 2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC'12).* 111–116. DOI: http://dx.doi.org/10.1109/CyberC.2012.26

Peter Mell and Timothy Grance. 2011. *The NIST Definition of Cloud Computing*. Technical Report 800-145. National Institute of Standards and Technology, Gaithersburg, MD. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Antonis Michalas and Rohan Murray. 2016. *Mem Tri: Memory Forensics Triage Tool*. Technical Report. Cyber Security Group, University of Westminster. http://westminsterresearch.wmin.ac.uk/id/eprint/17867.

Antonis Michalas and Rohan Murray. 2017. MemTri: A memory forensics triage tool using bayesian network and volatility. In *Proceedings of the 2017 International Workshop on Managing Insider Security Threats (MIST'17)*. ACM, New York, NY, USA, DOI: https://doi.org/10.1145/3139923.3139926.

The MITRE Corporation. 2015. *Cyber Observable eXpression (CybOX^{TM})*. Technical Report. The MITRE Corporation. http://cyboxproject.github.io

Pontjho M. Mokhonoana and Martin S. Olivier. 2007. Acquisition of a Symbian smart phone's content with an on-phone forensic tool. In *Proceedings of the Southern African Telecommunication Networks and Applications Conference*.

Hamid R. Motahari-Nezhad, Bryan Stephenson, and Sharad Singhal. 2009. Outsourcing business to cloud computing services: Opportunities and challenges. *IEEE Internet Computing, Special Issue on Cloud Computing*. Submitted.

Tilo Müller and Michael Spreitzenbarth. 2013. FROST: Forensic recovery of scrambled telephones. In *Proceedings of the 11th International Conference on Applied Cryptography and Network Security (ACNS'13)*. 373–388. DOI: http://dx.doi.org/10.1007/978-3-642-38980-1_23

Cynthia Murphy, Adrian Leong, Maggie Gaffney, Shafik G. Punjad, JoAnn Gibb, and Brian McGarry. 2016. *Windows Phone 8 Forensic Artifacts*. Technical Report. SANS Institute. https://www.sans.org/reading-room/whitepapers/forensics/windows-phone-8-forensic-artifacts-35787.

Cynthia A. Murphy. 2013. Developing Process for Mobile Device Forensics. Retrieved April 9, 2018, from https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf.

Luis Filipe da Cruz Nassif and Eduardo Raul Hruschka. 2011. Document clustering for forensic computing: An approach for improving computer inspection. In *Proceedings of the 2011 10th International Conference on Machine Learning and Applications and Workshops, Vol. 1 (ICMLA'11)*. IEEE, Los Alamitos, CA, 265–268. DOI: http://dx.doi.org/10.1109/ICMLA.2011.59

Daniel Nguli, Almerindo Graziano, George Nicolaou, and Juma Fredrick. 2014. Nyuki Android Process Dumper User Guide. Retrieved April 9, 2018, from http://www.silensec.com/images/images/nyuki_aprocdump_user_guide.pdf.

Prashant N. Ninawe and Shrikant B. Ardhapurkar. 2014. Forensic-as-a-service for mobile devices (literature survey). *Int. J. Comput. Sci. Inform. Technol.* 5, 6 (2014), 7776–7778.

NowSecure. 2016. NowSecure: Power-efficient MF for Android and iOS. Retrieved January 12, 2016, from https://www.nowsecure.com/forensics.

Christoforos Ntantogian, Dimitris Apostolopoulos, Giannis Marinakis, and Christos Xenakis. 2014. Evaluating the privacy of Android mobile applications under forensic analysis. *Comp. Sec.* 42, 66–76. DOI: http://dx.doi.org/10.1016/j.cose.2014.01.004

Gary Palmer. 2001. *A Road Map for Digital Forensic Research*. Technical Report DTRT0010-01. Digital Forensic Research Workshop.

Albert Pang. 2015. Worldwide Cloud Applications Market Forecast 2015-2019. Retrieved April 9, 2018, from http://www.appsruntheworld.com/worldwide-cloud/applications-market-forecast-2015-2019.

Emmanuel S. Pilli, Rutvij C. Joshi, and Rajdeep Niyogi. 2010. Network forensic frameworks: Survey and research challenges. *Digital Investig.* 7, 2 (2010), 14–27. DOI: http://dx.doi.org/10.1016/j.diin.2010.02.003

Christian Platzer, Martin Stuetz, and Martina Lindorfer. 2014. Skin Sheriff: A machine learning solution for detecting explicit images. In *Proceedings of the 2nd International Workshop on Security and Forensics in Communication Systems (SFCS'14)*. ACM, New York, NY, 45–56. DOI: http://dx.doi.org/10.1145/259898.2598920

Darren Quick and Kim-Kwang Raymond Choo. 2014. Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investig.* 11, 4 (2014), 273–294. DOI: http://dx.doi.org/10.1016/j.diin.2014.09.002

Shivankar Raghav and Ashish Kumar Saxena. 2009. Mobile forensics: Guidelines and challenges in data preservation and acquisition. In *Proceedings of the 2009 IEEE Student Conference on Research and Development (SCOReD'09)*. 5–8. DOI: http://dx.doi.org/10.1109/SCORED.2009.5443431

RightScale. 2016. State of the Cloud Report. Retrieved April 4, 2016, from http://assets.rightscale.com/uploads/pdfs/RightScale-2016-State-of-the-Cloud-Report.pdf.

Marcus K. Rogers. 2013. Analysis of digital evidence. In *Encyclopedia of Forensic Sciences*, J. A. Siegel, P. J. Saukko, and M. M. Houck (Eds.). Academic Press, Waltham, MA 455–460. DOI: http://dx.doi.org/10.1016/B978-0-12-382165-2.00325-1

Marcus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge, and Steve Debrota. 2006. Computer forensics field triage process model. *J. Digital Forensics, Secur. Law* 1, 2 (2006), 19–38.

Keyun Ruan, Joe Carthy, Mohand Tahar Kechadi, and Ibrahim Baggili. 2013. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investig.* 10, 1 (2013), 34–43. DOI: http://dx.doi.org/10.1016/j.diin.2013.02.004

Sherif Saad and Issa Traore. 2010. Ontology-Based Intelligent Network-Forensics Investigation. Retrieved April 9, 2018, from https://pdfs.semanticscholar.org/3a33/c4f3215ddc284ff87532753fe40b4f1d1d4.pdf.

Mohammed I. Al-Saleh and Yahya A. Forihat. 2013. Skype forensics in Android devices. *Int. J. Comput. Appl.* 78, 7 (Sept. 2013), 38–44. DOI: http://dx.doi.org/10.5120/13504-1253

Brendan Saltaformaggio, Rohit Bhatia, Zhongshu Gu, Xiangyu Zhang, and Dongyan Xu. 2015. GUITAR: Piecing together Android app GUIs from memory images. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS'15)*. ACM, New York, NY, 120–132. DOI: http://dx.doi.org/10.1145/2810103.2813650

SALUS. 2014. Deliverable 7.1 SALUS PPDR Platform—Intermediate. Retrieved April 9, 2018, from http://www.sec-salus.eu/wp-content/uploads/2014/05/SALUS_D7.1_v1.1.pdf.

Nouha Samet, Asma Ben Letaifa, Mohamed Hamdi, and Sami Tabbane. 2014. Forensic investigation in mobile cloud environment. In *Proceedings of the 2014 International Symposium on Networks, Computers, and Communications*. 1–5. DOI: http://dx.doi.org/10.1109/SNCC.2014.6866510

Philip Schutz, Michael Breuer, Hans Hofken, and Marko Schuba. 2013. Malware proof on mobile phone exhibits based on GSM/GPRS traces. In *Proceedings of the 2nd International Conference on Cyber Security, Cyber Peacefare, and Digital Forensic (CyberSec'13)*. 89–96.

Tamer Shanableh. 2013. Detection of frame deletion for digital video forensics. *Digital Investig.* 10, 4 (2013), 350–360. DOI: http://dx.doi.org/10.1016/j.diin.2013.10.004

Mohammad Shariati, Ali Dehghantanha, and Kim-Kwang Raymond Choo. 2016. SugarSync forensic analysis. *Aust. J. Forensic Sci.* 48, 1 (2016), 95–117. DOI: http://dx.doi.org/10.1080/00450618.2015.1021379

Mohammad Shariati, Ali Dehghantanha, Ben Martini, and Kim-Kwang Raymond Choo. 2015. Ubuntu One investigation: Detecting evidences on client machines. In *The Cloud Security Ecosystem*, R. K.-K.-R. Choo (Ed.). Syngress, Boston, MA, 429–446. DOI: http://dx.doi.org/10.1016/B978-0-12-801595-7.00019-7

Silensec. 2016. Nyuki Forensic Investigator (NFI). Retrieved January 12, 2016, from http://www.silensec.com.

Murugiah Souppaya and Karen Scarfone. 2013. *NIST Special Publication 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise: Revision 1*. Technical Report. National Institute of Standards and Technology, Gaithersburg, MD. DOI: http://dx.doi.org/10.6028/NIST.SP.800-124.r1

Vrizlynn L. L. Thing, Kian-Yong Ng, and Ee-Chien Chang. 2010. Live memory forensics of mobile phones. *Digital Investig.* 7, Supplement0 (2010), S74–S82. *Proceedings of the Tenth Annual (DFRWS) Conference*. DOI: http://dx.doi.org/10.1016/j.diin.2010.05.010

Gordon Thomson. 2012. BYOD: Enabling the chaos. *Netw. Secur.* 2012, 2 (2012), 5–8. DOI: http://dx.doi.org/10.1016/S1353-4858(12)70013-2

Volatile Systems. 2011. The volatility framework: Volatile memory artifact extraction utility framework. Retrieved January 12, 2015, from https://www.volatilesystems.com.

Stefan Vomel. 2013. *Forensic Acquisition and Analysis of Volatile Data in Memory*. Ph.D. Dissertation. Faculty at the Friedrich-Alexander University Erlangen-Nurnberg.

Daniel Votipka, Timothy Vidas, and Nicolas Christin. 2013. Passe-partout: A general collection methodology for Android devices. *IEEE Trans. Inf. Forensics Security* 8, 12 (Dec. 2013), 1937–1946. DOI: http://dx.doi.org/10.1109/TIFS.2013.2285360

Robert J. Walls, Erik Learned-Miller, and Brian Neil Levine. 2011. Forensic triage for mobile phones with DEC0DE. In *Proceedings of the 20th USENIX Conference on Security (SEC'11)*. 7.

M. Wazid, A. Katal, R. H. Goudar, and S. Rao. 2013. Hacktivism trends, digital forensic tools and challenges: A survey. In *Proceedings of the 2013 IEEE Conference on Information Communication Technologies (ICT'13)*. 138–144. DOI: http://dx.doi.org/10.1109/CICT.2013.6558078

Shams Zawoad, Amit Kumar Dutta, and Ragib Hasan. 2013. SecLaaS: Secure logging-as-a-service for cloud forensics. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer, and Communications Security (ASIA CCS'13)*. ACM, New York, NY, 219–230. DOI: http://dx.doi.org/10.1145/2484313.2484342

Shams Zawoad and Ragib Hasan. 2013. Cloud forensics: A meta-study of challenges, approaches, and open problems. arXiv:1302.6312. http://arxiv.org/abs/1302.6312

Shams Zawoad and Ragib Hasan. 2015. Towards a systematic analysis of challenges and issues in secure mobile cloud forensics. In *Proceedings of the 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud'15)*. 237–238. DOI: http://dx.doi.org/10.1109/MobileCloud.2015.32

Jonathan Zdziarski. 2008. *iOS Forensic Investigative Methods*. Technical Report. International Telecommunication Union. http://www.zdziarski.com/blog/wp-content/uploads/2013/05/iOS-Forensic-Investigative-Methods.pdf.

Received October 2016; revised November 2017; accepted January 2018