Towards a Model for Acquiring Digital Evidence using Mobile Devices

S.Omeleze[1] and H.S.Venter[2]

[1,2]Information and Computer Security Architecture (ICSA) Research Group
Department of Computer Science, Information Technology Building
University of Pretoria, Private Bag X20 Hatfield 0002 Pretoria, South Africa
e-mail: staceyaomeleze@gmail.com; hventer@cs.up.ac.za

Abstract

In recent years, many criminal activities have gone unsolved due to lack of sufficient evidence to convict the perpetrators. However, with the evolution in mobile technology, mobile devices can now be used to provide such evidence. The advanced features of mobile devices such as photo, video and voice recording options have the ability to transform such devices into real-time potential digital forensic evidence-capturing devices. This paper therefore proposes a model that enables the use of mobile and portable devices to capture potential digital evidence and preserve the integrity of such evidence. This model therefore, takes into consideration the privacy policies, laws and ethics that may apply due to the devices' generated metadata, especially during a digital evidence presentation in a court of law or in civil proceedings.

Keywords

Digital evidence, SHA-2, Cryptographic Hash Function, privacy, Online Neighbourhood Watch (ONW) Model, Mobile devices, Crime and Law.

1. Introduction

In 2012, a survey conducted by Tsirulnik (2012) placed mobile devices as one of the most purchased items of electronic equipment in the world. This is attributed to the popularity of mobile applications (popularly known as apps) that are available for almost all activities, from health monitoring, news update alerts to real-time online gaming. The influence of digital forensic technology on crime management, especially with the exploding trend of mobile technology in society, can be explored in very beneficial ways. Over the years, many criminal activities have gone unsolved due to the lack of sufficient evidence to convict the perpetrators. The advanced functionality of mobile devices and portable devices can be used as a tool in the fight against crime. Cameras, voice recording and image capturing functions can become real-time digital evidence-capturing options for potential digital forensic evidence acquisition.

This paper attempts to aid the fight against crime by creating an online neighbourhood watch (ONW) model to acquire potential digital evidence using mobile and portable devices in South African neighbourhoods. The ONW model generates and stores potential digital evidence of criminal acts, which is then available to law enforcement agents and digital forensic investigators. The goal of

the ONW model is to increase the volume of available digital evidence in order to enhance success in trials and to help secure conviction of the actual culprits. The ONW model can be applied in scenarios such as road traffic offences, domestic violence, robberies and other incidents that require concrete evidence as proof in a court of law or in a civil proceeding. For the purpose of admissibility of potential evidence acquired using the ONW model, digital data integrity checks are employed using the SHA-2 cryptographic hash function, digital watermarking, time stamps, geo location and digital signatures. According to Saleem et al. (2011), these are the appropriate methods to use when the integrity of data is paramount.

It is important to note that this work is part of an ongoing project to develop a tool/application that enables the integrity validation of potential evidence acquired using mobile /portable devices, to be used for further investigative analysis of a case. This potential evidence can be used to obtain a court warrant, or could be employed as potential evidence in a trial-within-a-trial, or gauge evidential weight for admissibility in civil or criminal proceedings.

This paper is structured as follows: Section 2 contains an introduction to the background on digital forensics, digital evidence and the legal issues involved. Section 3 presents the online neighbourhood watch (ONW) model with a detailed discussion of the use cases and how the integrity of acquired evidence is upheld. Section 4 evaluates and critiques the ONW model, while section 5 discusses the related research works. Finally section 6 concludes this paper with recommendations for future work.

2. Background

This background section is devoted to the discussion of a review of digital forensic science, digital evidence from a legal perspective, and its application to this research.

2.1. Digital Forensic Science

Digital forensics is a young science drawn from the traditional science of forensics that has been developed in conjunction with the biological sciences. Digital forensics is used in the identification of digital evidence by employing mathematically derived methods in proving consistency of bits in a digital forensic investigative scenario (Bunge, 1998);(Valjarevic & Venter, 2011); (Karie & Venter, 2013). Digital forensic field requires exploring, especially with the rapid developmental growth in technological advancement, the generation of big data and connectivity of the Internet of things. In defining digital forensics, Cohen (2009) considers digital forensics as a subject that started between art and craft, and contains a scientific body of knowledge with an underlying scientific methodology, which consists of four basic elements. These elements are the study of previous and current theories, methods and experimental bases, the identification of inconsistencies between current theories and experimental repeatability. Digital forensics could be viewed in terms of Bunge's (Bunge, 1998) classification of scientific problems, namely that digital forensics is a young science at its conceptual level of scientific development. Therefore, in digital forensics, the use of scientifically derived and proven mathematical methods is adhered to in the acquisition, preservation,

collection, validation, identification, analysis, interpretation and documentation of digital evidence (Barske et al., 2010);(Cohen, 2009). In the verification of the integrity of digital evidence, numerous mathematical techniques are employed such as, the cryptographic hash function, the time stamp, bit stream, digital signature, chain of evidence, the chain of custody and geo-location (Dang, 2012); (Hargreaves, 2009). Since digital evidence consists entirely of sequences of bit binary values, it provides a means to aid the preclusion of criminal-related offences involving data messages.

2.2. Legal perspective

In dealing with digital evidence acquired using the ONW model, there is a need to explore the aspect of legal standards and what is acceptable in terms of privacy and human rights in South Africa.

In the Privacy of Personal Information (PPI) Act, Act 4 of 2013, Section 6 (c) (i) and (ii) and Section 37 (2) (a) and (b), the exclusions and exemptions to an individual's privacy rights are outlined. These exemptions apply when the interests of national security are at stake and when they involve the prevention, detection and prosecution of criminal behavior (Mujinga, 2013). Furthermore, the Electronic Communication and Transaction (ECT) Act, Act 25 of 2002, section 15(1), (2) and (3) defines the digital data that is admissible, the evidential weight of data information and the best evidence rule to be allowed in the usage of digital evidence in a South African court of law (Gazette, 2002). The ECT Act also states that data evidence must not be dismissed merely because it originates from a digital data message.

2.3. Integrity of digital evidence

One of the major roles of digital investigators is to ensure and provide proof that digital evidence has not only been acquired, retrieved and stored in a forensically sound process, but can also stand up to scrutiny in a court of law. The integrity of digital evidence is proven to render acquired digital evidence admissible. The integrity of digital evidence is elaborated on in section 14(1) (a) of the ECT Act, Act 25 of 2002 which states that digital data must maintain its integrity from the time of data generation to when it is analysed (Gazette, 2002).

The way that integrity is employed in the ONW model includes the use of cryptographic hash algorithms, digital watermarking, digital signatures and public key infrastructure (PKI) cryptography. These concepts are elaborated on in the next paragraphs.

A cryptographic hash function is used to prove the integrity of a message. The cryptographic hash function generates a hash value that can be used to put a seal on a message. It can be implemented using a hashed message authentication code (HMAC), secure hash algorithm (SHA) that generates 160-bit hash value and a SHA-2 that generates a unique 256-bit (32-byte) signature for every piece of digital data (evidence) received (Dang, 2012); (Pfleeger & Pfleeger, 2006). Furthermore, a

digital signature is used to demonstrate the non-repudiation, authenticity and the integrity of a message.

Digital watermarking is a method that applies tamper detection, traitor tracing and integrity maintenance of digital data. This is achieved by using steganography techniques (i.e. information hiding) to embed unique data in a noisy signal to identify when an alteration occurs on the data file (Halder & Cortesi, 2010).

A PKI cryptography system utilizes a key pair to encrypt and decrypt data respectively. PKI is used in conjunction with hash values, i.e. by encrypting the hash value of a message in order to add a unique 'stamp', so that only the intended recipient of the message can decrypt the message with a public key, proving non-repudiation.

A Password management policy is a recommendation of the ISO/IEC 27002 (Calder & Watkins, 2008) (ISO27001, 2012) with a guideline for managing the security of a system effectively. According to ISO/IEC 27002, password selection must meet certain requirements such as, minimum length and strength of a password, maintenance of previous password records to avoid repeatability and the storage of user's password must be encrypted using a one-way algorithm. This is in order to achieve and ensure confidentiality and integrity of a system.

3. Online Neighbourhood Watch Model (ONW)

This section proposes a contribution of how potential digital evidence can be acquired using mobile devices through the ONW model.

The (ONW) model is an application model accessible via mobile devices or computers over the Internet. It enables users to upload digital evidence such as audio, video and digital photographs of a potential crime scene or incident to the ONW repository. It also allows an investigator to access the uploaded evidence whenever it is required, especially during criminal investigations.

Figure 1 illustrates the high-level view of the two main aspects of the ONW model. Part A is concerned with the activities of the user (uploader) and maintaining the digital evidence integrity which is achieved using the SHA-2 hash algorithm, digital signature, timestamp and geographical location of the user (uploader). Part B depicts the role of the Forensic Investigator/Law Enforcement Agent (the downloader) and the measures employed in maintaining the integrity of the potential evidence and the access control of the ONW repository. The repository employs sound access control measures, such as the role and attribute based access control policies, to manage the users' uploads to the repository. These policies include the concept of need to know so that the number of law enforcement agents accessing any particular piece of evidence is strictly limited and monitored. This paper, however, focuses on Part A of Figure 1 while Part B will be dealt with in further work.

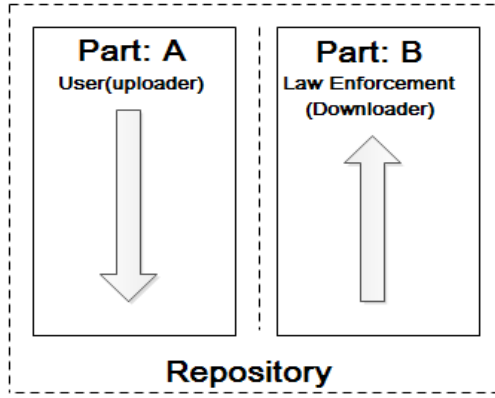

Figure 1: View of the ONW Model indicating Parts A and B

The (ONW) model as shown in Figure 2 consists of a process involving seven steps. The users' (i.e. uploader and downloader) operations in the ONW model are permitted based on their roles and access rights. The user (uploader) is enabled to upload potential data evidence into the repository, while the law enforcement agent or digital forensic examiner (downloader) is entitled to download and view the potential digital evidence stored in the repository during criminal or digital forensic investigations. The interactive processes of the ONW model are described in the following paragraphs and are based on the diagram in Figure 2.

3.1. ONW application

The ONW model application being developed is to accept potential digital evidence via a mobile application or web application. This application ensures the integrity of the potential evidence through the use of the geo-location, timestamp and the SHA 2 algorithm, which is embedded in the system. The potential captured evidence is then uploaded to the ONW repository following the processes shown in Figure 2. This can be done directly from the user's (uploader) mobile device or using a computer system where the ONW application installed.

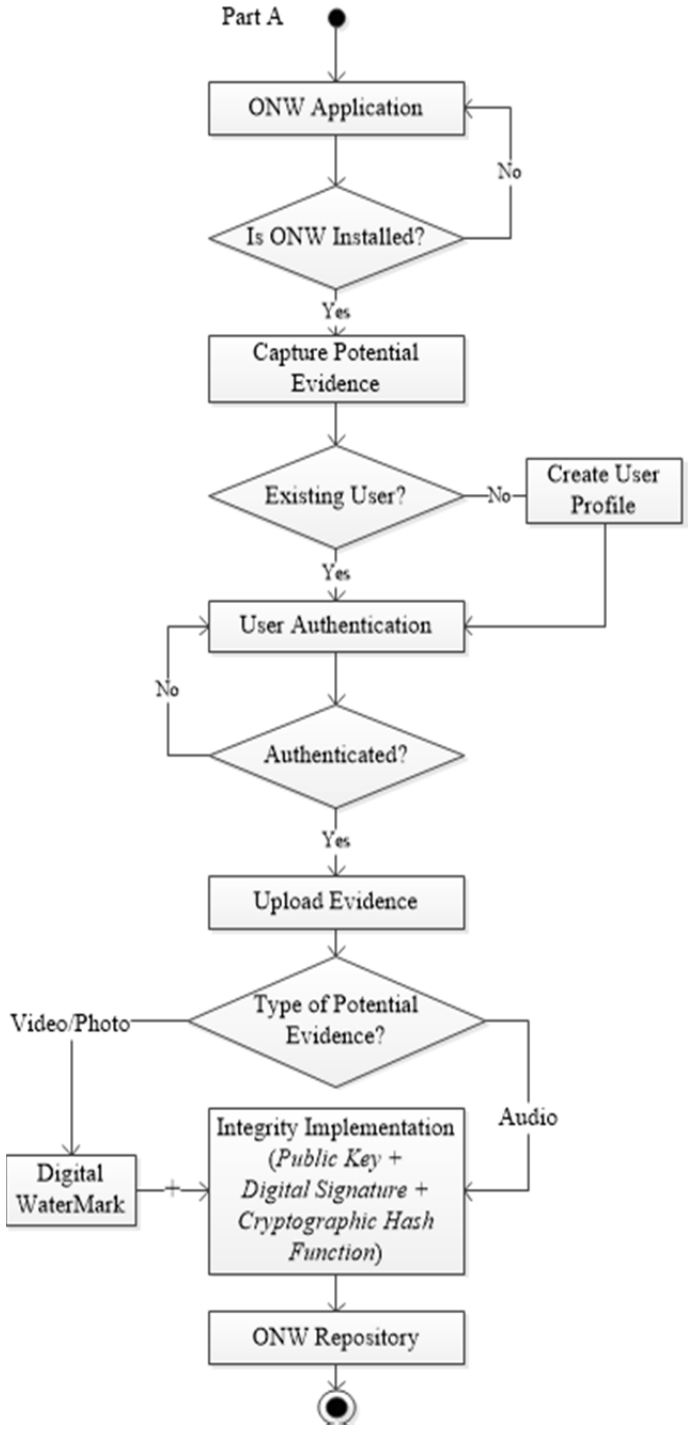

Figure 2: Flow Diagram of the ONW Model

3.2. Capture potential evidence

Potential evidence is obtained when the user notices an incident that could be viewed as a crime. The user may capture evidence in the form of a digital photo, video, or an audio recording of the criminal activity. The potential evidence must be captured in the domain of ONW in order to maintain and preserve the integrity of the potential digital evidence. This is to assure the applicability of the potential evidence in solving the cases and ensuring the admissibility of the evidence in a court of law. Digital evidence captured outside the ONW application domain is rejected when an upload is attempted.

3.3. Create a user profile

This step enables the user to create a profile for authenticating into the system and to allow for upload of the acquired potential evidence. An existing user need not create a profile on subsequent use of the system. However, a new user must create a profile to allow interaction between the user and the ONW model. On the creation of this profile, the user is authenticated to log in. User profile creation is compulsory to allow access to the ONW system.

3.4. User authentication

User authentication is to ensure that the user is who he/she claims to be. The registering of the device in the system and the gathering of the audit trail commence at this stage of the user's interaction with the system. An existing user has to login when evidence is captured, but a first-time user must create a user profile, as discussed in step 3 above, in order to gain access to the system. Authentication at this stage of the model design involves the use of a username and password retaining the password requirement policy of the ISO/IEC 27002 (ISO27001, 2012) (Calder & Watkins, 2008). Subsequently, however, other forms of authentication such as biometric and the implementation of authorization, i.e access control is employed. This authentication aspect of the model also helps in the system's audit trails, in terms of who does what in the system.

3.5. Uploading evidence

Once potential digital evidence of a crime is acquired, it is then uploaded to the ONW repository (as shown in Figure 2). The uploaded potential evidence is secured using encryption and access control mechanisms embedded in the system. The acquisition of this evidence must be done in the domain of the ONW application. This is to enable the inbuilt integrity checks in the application domain. The cryptographic hash algorithm seals the digital evidence in order to avoid/detect digital evidence alteration. The timestamp helps in determining the time that potential evidence was acquired and the geo-location shows where the potential evidence was acquired using cellular tower triangulation. The uploading of evidence is only possible if the user has created his/her profile and is logged into the system via the mobile or web application.

3.6. Integrity implementing

The ONW model implements and maintains the integrity of the acquired evidence by using mathematical techniques and an approved algorithm. These measures are employed to preserve the authenticity and integrity of evidence uploaded to the ONW repository, in order to corroborate the occurrence of a certain incident and further the admissibility of the potential digital evidence in a court of law (Gazette, 2002). Therefore to achieve the integrity of the acquired potential evidence the cryptographic hash function, digital signature, public key infrastructure (PKI) cryptography, time stamp and geographical location tag are employed. In this model, the hypothesis is based on the assumption that users can acquire three data formats, i.e. audio, video and digital photos, that can be used as potential digital evidence as shown in Figure 2.

In order to ensure the integrity of the potential evidence in the ONW model, a digital seal is placed on the digital evidence. The seal is a "tamper proof" feature placed on the acquired potential digital evidence that generates cryptographic hash values that can be compared during potential digital evidence download, to determine whether an alteration has been made to the digital evidence. For example, two digital images can be assured to be identical only if the hash values generated from each digital data item, using the same cryptographic hash function, are identical. When an alteration is detected, the message is discarded. In using a digital signature to ensure the integrity and authenticity of potential digital evidence, the use of a public/private key encryption system is employed to ascertain that data transmission between the mobile/portable device and the ONW repository is trusted and secure. For example, the integrity of potential video data evidence is achieved by using a digital signature within the cryptographic hash function and by encrypting the resulting cryptographic hash value with a private key (as shown in figure 2). The integrity of potential digital evidence obtained through digital photo image or video is achieved using a combination of methods. These methods include the cryptographic hash function, digital signature and PKI cryptography in conjunction with watermarking.

3.7. Storing evidence in the repository

The ONW repository stores the acquired potential digital evidence to be accessed by the user in part B of the ONW model (i.e. the investigator/law enforcement agent). In Part B of the ONW model (figure 1), digital forensic investigators and law enforcement agents will access the required potential digital evidence from the ONW repository. The data is then downloaded with the stored cryptographic hash value and digital signature with the matching half of the encrypted PKI. A re-computation of these functions is performed to verify potential digital evidence consistency and integrity.

Furthermore, a strict implementation of the chain of custody is adhered to so as to determine who accessed what, at what time and on what date. This process is followed in order to retain integrity and confidentiality of the acquired potential digital evidence and the ONW system. The law enforcement agent's access to the ONW model is based on role-based access control (RBAC) policies. Further discussion on RBAC is beyond the scope of this paper, as it will be covered in the

Part B of the model in future work.

4. Appraisal of the ONW Model

The application of mobile devices as a means of generating potential digital evidence in a bid to minimize crime in a South African context is not without its difficulties. One of these difficulties may be the need to protect the privacy of individuals as outlined in the Privacy of Personal Information (PPI) Act, Act 4 of 2013 (Mujinga, 2013). However, in Section 6 (c) (i) and (ii) and particularly in Section 37 (2) (a) and (b) of this Act, there are numerous exclusions and exemptions to an individual's privacy rights when the interests of national security are at stake and when the prevention, detection and prosecution of criminal offences are involved.

The concept of the ONW model may be seen as infringing with law and ethics. However, in his analysis of the ECT Act 25 of 2002, Watney (2009) states that the Act sets out to facilitate digital data (evidence) generation and admissibility rather than inhibit it. With the ONW model in place, it becomes much easier to apprehend suspects involved in various nefarious activities in the community, thereby reducing crime and anti-social behaviour.

The digital evidence available in the repository of the ONW system can serve as the incident scene detection phase of an investigation. According to Valjarevic & Venter (2011) and Omeleze & Venter (2013), an incident scene conveys messages of what happened and how best to approach the investigation for both the law enforcement agents and the digital forensic investigators. The ONW evidence repository can also be employed during evidence front-loading (trial-within-a-trial) by the legal teams during pre-trial. A trial-within-a-trial as stated in the Criminal Procedure Act, Act 51 of 1977, is an avenue which enables two legal teams in a trial to share the available potential evidence with the trial Judge, who then determines what is admissible based on the case and the digital evidence available, especially in criminal proceedings (Bellengere et al., 2013). Furthermore, section 15(1) (2) (3) of the ECT Act emphasized the need to explore electronic evidence and its admissibility based on the generation, handling, collection and integrity of evidence (Gazette, 2002); (Mujinga, 2013); (Papadopoulos & Snail, 2012); (Watney, 2009). The possibility of creating the ONW system is based on the assumption that the majority of mobile phones/devices available are devices with features that can acquire video, audio and photo evidence at the scene of a crime.

Since the ONW model has no provision for a function that determines what a potential crime is or when a user (uploader) can commence potential evidence acquisition, the community member (user) must use his/her intuition and common sense to decide when/what is a potential crime. For instance, in Gedanken experiments, human senses/thoughts tend to play a great role in determining the current state of its environment (Kuhn, 1977). That is, the observation of the behaviour of a subject triggers responses to stimuli. These responses to environmental stimuli could help the community members in their decision as to what constitutes potential evidence. It is left to the law enforcement agents and judiciary to decide what is actual evidence and whether a crime has been committed.

As a result, throughout this paper, the term potential digital evidence is used rather than digital evidence.

In the ONW model, the user authentication is implemented by means of a user name and password. However, the password must meet the password standard requirement policies (i.e. the user must use at least a upper case character, lower case characters, numbers and a special character) (ISO27001, 2012). With the ONW model's integrity and authenticity implemented, the South African legal system benefits. This is by making the best use of the increasingly dynamic and diverse forms of potential digital evidence acquisition, especially those acquired using mobile and portable devices for proof and fact-findings in legal and civil proceedings (Roberts & Redmayne, 2007).

With the incorporated integrity features of the ONW model, digital forensic investigators and law enforcement agencies are able to employ the ONW repository during digital investigations. This will yield faster results in identifying the culprits by establishing what happened during investigations (Karie &Venter, 2013). The success of the ONW model will not only reduce crime but also foster a better and closer cooperation between the ordinary person on the street and the government.

Furthermore, the philosophy of Ubuntu in South Africa that is, a community-based mind set where the welfare of the group is greater than that of an individual can be brought to service (Olinger et al., 2007). Moreover, with the provisions of the ECT Act, Act 25 of 2002 (an extension of the United Nations' Model Law), the international standards such as ISO/IEC 27043 and the cooperation of the South African judiciary, the ONW model can be extended to other countries and ultimately become a global crime-fighting tool. For example, in the development of ISO/IEC 27043 proposed by Valjarevic & Venter, (2011); (ISO27001, 2014) the International Criminal Police Organization (INTERPOL) is one of the main contributors in promoting a standard for digital forensic investigation that is identical in it's member countries and the world in general, thereby paving the way for the ISO/IEC 27043 model to become an international one (Valjarevic & Venter, 2012). The ONW model can similarly become a model adoptable for the acquisition of potential digital evidence using mobile devices worldwide, once this South African pilot project has been attested to work effectively in achieving faster prosecution and reduction of crime levels.

5. Related Work

This section discusses relevant research works that are related to the integrity of digital evidence and its admissibility in a court of law. Much research on evidence integrity has been conducted. However, none has focused on a model to capture potential digital evidence using mobile devices. Furthermore, the existing work focuses only on digital evidence statically stored and its integrity, as opposed to the ONW model, which focuses on capturing potential digital evidence in a dynamic and real-time fashion.

Richter et al (2010) mentions that using digital signatures and non-repudiation are not enough to ensure digital evidence integrity. They presented an embedded system

that is able to collect admissible digital evidence through an automated process focusing on the non-repudiation of the digital evidence data by designing a secure environment and adding all relevant parameters to the measured data such as the location, identity of the device, timestamp, and the current status of the system.

Halder et al (2010) identified the challenges of using watermarking as a method for copyright identity protection, tamper detection and maintaining integrity due to issues such as usability, robustness, and interference. The ONW model employs digital watermarking as an added feature to digital signature, public key infrastructure (PKI) cryptography and cryptographic hash function to ensure the implementation of integrity. This is to support and manage the flaws that may otherwise occur when digital watermarking is solely used.

Furthermore, Ani et al (2013) analysed the threats to the integrity of digital evidence using the VMware hypervisors to strengthen the hash function and incorporate reliability rating factors, as a means of conceptualizing integrity levels of digital data. They further enumerated appropriate algorithms for the implementation of digital evidence integrity to include secured hash algorithm (SHAx), digital signature, PKI cryptography and message digest algorithm (MD5).

Casey (2011) listed five properties that digital evidence must retain in order to be admissible in any proceedings. These are authenticity, completeness, reliability, and believability and also, that potential digital evidence must be tied to an incident in order to prove that an incident occurred and is related to the incident in a relevant way. The ONW model satisfies these properties and requirements by implementing timestamp, geo-location and secure hash algorithm (SHA-2) of the acquired potential digital evidence at the point of upload to the ONW repository.

Watney (2009), Papadopoulos & Snail (2012) enumerated the Common Law requirements for digital evidence admissibility to include; production, meaning the digital evidence must be relevant; presentation, that is, the digital evidence must be in its original form and finally, the authenticity of the digital evidence must be provable.

In another research, Papadopoulos & Snail (2012) detailed a set of guidelines required by a South African court in the application and assessment of evidential weight. These are, the reliability of the manner by which the potential digital evidence was generated, stored, or communicated and also the manner in which the integrity of the potential digital evidence is maintained plus its originality. The ONW model also fulfils these requirements.

6. Conclusion

The ONW model concept is a project that involves a public drive to use mobile/portable device technology for the enforcement of neighbourhood security. This is achieved by developing a model that enables the uploading of potential digital evidence to the ONW repository. This will engage both the community members and the law enforcement agencies in crime reduction in South African neighbourhoods. It will assist not only the law enforcement agencies but also the

digital forensic experts and the judiciary to conduct conclusive and decisive case investigations.

The ONW model demonstrates a means to acquire potential digital evidence and at the same time maintain the integrity of the various potential evidence formats acquired. The integrity of a photo image and video recording is upheld by using a private key, digital signature, cryptographic hash function and an additional option of digital watermarking. In order to further protect the integrity and confidentiality of the acquired potential digital evidence from unauthorized access, a password policy is used.

For future work, the authors will develop part B of the ONW model as depicted in Figure 1. Part B manages the access to the acquired potential digital evidence in the repository taking into account the privacy rights of the evidence generators considering the Privacy of Personal Information (PPI) Act, while at the same time making the evidence available to the intended stakeholders during criminal, civil and disciplinary proceedings. With the development and implementation of the ONW model as a fully-fledged system, the fight against crime in South Africa will be given a significant boost.

7. References

Ani, U. P. D., Epiphaniou, G., and French, T (2013). *A Novel Evidence Integrity Preservation Framework (EIPF) for Virtualized Environments: A Digital Forensic Approach*. In the Second International Conference on Cyber Security, Cyber Peace fare and Digital Forensic (CyberSec2013) (pp. 97-106). The Society of Digital Information and Wireless Communication.

Barske, D., Stander, A., and Jordan, J. (2010) A *Digital Forensic Readiness framework for South African SMEs*. In Information Security for South Africa (ISSA), 2010, pages 1–6. IEEE. ISBN: 9781424454938.

Bellengere, A., Palmer, R., Theophilopoulos, C., Whitcher, B., Roberts, L., and et al, (2013). *The Law of evidence in South African - Basic Principles-Procedural Law*. Oxford University Press, Southern Africa.

Bunge, M. (1998). *Philosophy of Science: From Problem to Theory*. Transaction Publishers, New Brunswick, revised edition ISBN: 9780765804136 (Vol. 1).

Casey, E. (2011). *Digital evidence and computer crime: forensic science, computers and the Internet*. Academic press.

Calder, A., & Watkins, S. (2008*). IT Governance A Manager's Guide to Data Security and ISO27001/ISO 27002* British Library Cataloguing-in-Publication. 4th edition. ISBN 978 0 7494 52711.

Cohen, F. A. (2009). *Digital Forensic Evidence Examination*, Fred Cohen and Associates out of Livermore, third edition. ISBN: 9781878109446.

Dang, Q (2012). *Recommendation for Applications using approved Hash Algorithms*. Computer Security Division Information Technology Laboratory. Accessed 19 November 2013.

Government Gazette (2002)*Electronic Communications and Transaction Act, Act 25 of 200*2. South Africa Government Printer. Accessed 02 February 2014.

Hargreaves, C. J. (2009). *Assessing the Reliability of Digital Evidence from Live Investigations involving Encryption*. Ph.D thesis, Department of Informatics and Sensors, Cranfield University,UK. Accessed 15 December 2013.

Halder, R., Pal, S., and Cortesi, A. (2010). *Watermarking Techniques for Relational Databases: Survey, Classification and Comparison*. *J. UCS*, *16*(21), 3164-3190.

ISO27001security.com (2014). *ISO/IEC 27043 Information Technology Security Techniques for Incident Investigation Principles and Processes* (DRAFT). Accessed 02 February 2014

ISO27001security.com (2012). *ISO/IEC 27001 Information Technology Security Techniques for Incident Investigation Principles and Processes* . Accessed 18 May 2014.

Karie, N.M. and Venter, Hein. S (2013).*Towards a Framework for enhancing Potential Digital Evidence Presentation*. In: Information Security for South Africa, 2013, pages 1–8. IEEE.

Kuhn, T. (1977). *A function for thought experiments*.

Mujinga, M. (2013). *Privacy and Legal Issues in Cloud Computing-the SMME position in South Africa.* SRI Security Research Institute, Edith Cowan University, Perth, Western Australia - Accessed 17 March 2014.

Omeleze, S. and Venter, H. S. (2013). *Testing the Harmonised Digital Investigation Process Model using an Android Mobile Phone*. In Information Security for South Africa, 2013, pages 1–8. IEEE.

Olinger, H. N., Britz, J. J., and Olivier, M. S. (2007). *Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa*. The International Information & Library Review, 39(1): 31–43.

Papadopoulos, S. and Snail, S. (2012). *Cyberlaw @South Africa III - The law of the Internet in South Africa*. Van Schaik Publishers, third edition. ISBN-10 (13): 9780627028076.

Pfleeger, P. C. andPfleeger, S. L. (2006). *Security in Computing*.Prentice Hall Publication, Upper Saddle Rivers, NJ, Boston, USA ISBN, fourth edition. ISBN-13: 978-0132390774 ISBN-100132390779

Richter, J., Kuntze, N., and Rudolph, C. (2010, May). *Security digital evidence*.In Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on (pp. 119-130). IEEE.
Roberts, P., and Redmayne, M. (2007). *Innovations in evidence and proof: integrating theory, research and teaching*.

Saleem, S., Popov, O., and Dahman, R. (2011). *Evaluation of security methods for ensuring the integrity of digital evidence*. Institute of Electrical and Electronics Engineers (IEEE Xplore Digital Library).

Tsirulnik, B. G. (2012). *Mobile Phone ranked most used electronic device*: Forrester. Information Security.

Valjarevic, A. and Venter, Hein. S. (2011). *Towards a digital Forensic Readiness framework for Public Key Infrastructure Systems.* In Information Security for South Africa (ISSA), 2011, pages 1–10. IEEE.

Valjarevic, A and Venter, Hein S (2012) *Harmonized Digital Forensic Investigation Process Model*. Information Security For South Africa (ISSA), IEEE, 2012.

Watney, M. (2009) *Admissibility of Electronic Evidence in Criminal Proceedings: An outline of the South African Legal position*. 2009 (1). Journal of Information, Law & Technology (JILT), 2.