A Mobile Forensic Readiness Model aimed at Minimizing Cyber Bullying

Victor R. Kebande
ICSA Research Lab
Department of Computer Science
University of Pretoria,
Private Bag X20, Hatfield
0028, Pretoria, South Africa

Nickson M. Karie
ICSA Research Lab
Department of Computer Science
University of Pretoria,
Private Bag X20, Hatfield
0028, Pretoria, South Africa

Stacey Omeleze
ICSA Research Lab
Department of Computer Science
University of Pretoria,
Private Bag X20, Hatfield
0028, Pretoria, South Africa

ABSTRACT
The existence of mobile devices in today's modern society has generated greater advantages to many users especially within the African continent with regard to how information is being disseminated. However, the efficacy of mobile device technology has not come without some drawbacks, especially with the proliferation of Internet enabled mobile devices among young people. Trends of cyber-bullying, for example, are on the increase and recent studies in South Africa have shown that the use of mobile devices among school pupils between the ages of 2 to 17 years is at 60%. This can only be attributed to mobile device proliferation, increased cyber technologies like social network and change of communication modes. For this reason, one might end up being excluded from this environment if one excludes oneself from the modern communication culture. However, with all this advances in mobile communication technologies, there lacks proper guidance on the side of young people with regard to the proper use of mobile devices and their forensic readiness capability. This is aggravated by the fact that a bigger percentage of parents also have no knowledge of what young people do online especially with their mobile device features such as online chat rooms, cyber-bullying, and sexting.

Therefore, the problem being addressed in this paper is that: by the time of writing this paper, there exist no reliable and effective mobile forensic readiness models that can be used to create awareness to both young people and their parents on how to minimize cyber-bullying. This paper thus proposes a mobile forensic readiness model that can minimize cyber bullying, enhance awareness on issues of cyber bullying as well as the creation of parental guidance information on cyber bullying. The model can also act as a monitoring tool that can be embedded on different mobile devices assigned to, for example, learners and minors. The embedded model can then help parents and guardians to identify and maintain control of the various information and online activities that children engage in. Mobile forensic readiness model aimed at minimizing cyber bullying, as well as enhance awareness on issues of cyber bullying, constitutes the main contribution of this paper.

General Terms
Mobile forensic readiness model, cyber bullying.

Keywords
Mobile forensic readiness model, cyber bullying, Mobile devices, content monitoring.

1. INTRODUCTION
The increased usage of mobile computing devices and constant connectivity in our society has led to increased pervasiveness in cyber technologies and this has brought about a new way of thinking and disseminating information. The broader impact of mobile computing devices has been on the ease of communication and being able to plan daily routines, activities and schedules. Moreover, these devices have also played a very significant role, perhaps more importantly, in the education sectors where people have seen a boost because a majority of handheld devices have been used as tools that have increased learning collaboratively through engagement in learning through video conferencing, participatory simulations and collaborative data gathering [3],[4].

Despite all the positive benefits, there exist a number of drawbacks that comes with constant connectivity of mobile devices. As mobile devices continue to become a staple in our society, the impact they have had on the relationship that we have with one another remains a question that is yet to be answered. One of the notable impacts that have been witnessed is Cyber-bullying. The concepts of cyber-bullying can be traced to the early nineties and it was portrayed by Olweus [2] as "an intentional act that is conducted by one or a group of people against a victim using electronic means or Information and Communication Technology (ICT) tools. These acts are done through SMS bullying, mobile bullying, cyber-stalking, and cyber-grooming. This may happen through internet-based bullying tools for example: Email, chatting rooms, Instant messaging, social networks and other mobile-based bullying tools like: Smart phones, Personal Digital Assistant (PDA), mobile devices, Short Message Service (SMS), Multimedia Messages (MMS), social groups, and iPod's. To illustrate the problem associated with mobile bullying, consider the following hypothetical scenario:

Alice is 13 years old student at Talent High school. She is a very bright and promising student of above average academic potential. Three students in Alice's class came to school drunk one day and on seeing their actions, the Head teacher decided to suspend them. One of the student named Peter felt aggravated after his friends were suspended and he went ahead to create a group online through iknowho.com and used it to orchestrate an attack on Alice who was innocent, as the one who set up his friends to be suspended. The group was shared to all their classmates through their mobile devices and Alice was attacked frequently. Alice remained strong but slowly depression started eating her up. Alice tried to convince the group that she was not responsible for the suspension but the following words were disseminated to her

through mobile devices: "if you die, the world will be a better place", "kill yourself". Eventually, Alice succumbed to the bullying and she hanged herself.

In such a scenario, Digital Forensic Readiness (DFR) would be significant because the death of Alice would have been prevented had there been forensic readiness and monitoring in the mobile devices that were owned by the students. To mitigate the above hypothetical scenario, the authors have proposed in this paper, a generic mobile forensic readiness model aimed at minimizing cyber bullying as well as enhance awareness on issues of cyber bullying and thereafter evaluate the model for its possible applicability

As for the remainder of this paper section 2 gives a background of the study while Section 3 concentrates on discussing related work of the study. Thereafter Section 4 briefly outlines the legal aspects of content monitoring on mobile devices. Section 5 proposes the model while section 6 evaluates the proposed concept. The paper is concluded in Section 7 and makes mention of possible future work.

2. BACKGROUND

This section discusses the background on the following: Mobile computing, digital forensic readiness and cyber-bullying. Mobile computing is being discussed because the model will be based on mobile devices; digital forensic readiness is discussed to show how a proactive process can be employed in mobile devices to help curb unwanted activities. Finally cyber-bullying is discussed to show the harm that is inflicted through the use of mobile digital devices.

2.1 Mobile Computing

Mobile computing provides an interaction between human and computers through an engagement of applications that transmit data and information without a pre-defined location. This interaction happens through the use of a mobile operating system that is available from different vendors. According to Brown and Singh [5], mobile computing is an extension of distributed computing that adds mobility to the hosts like PDA and portable computers. However, Peng and Chen [6] presents it as a computing system that has stationary servers and mobile computers which implies that stationary servers are used as information servers while mobile computers represent mobile devices that use batteries for their operation without connecting to a direct power source coupled with limited bandwidth of wireless communication. Additionally these devices provide very powerful capabilities like processing data through storage of a small database.

2.2 Digital Forensic Readiness

Digital forensic Readiness (DFR) is a proactive process that has an aim of getting incident preparedness before potential security incidents occur. Rowlingson [7] defines it as having an objective to maximize the use of potential digital evidence while minimizing the cost of conducting digital forensic investigation. Forensic readiness can be achieved through gathering of evidence that might be deemed important to detect an incident. This is represented as foreground evidence which involves what one would be doing in real-time. Forensic readiness as a process has been defined in the ISO/IEC 27043:2015 standard as a process that occurs before incident identification that involves collection, preservation, storage and analysis of digital evidence [8]. Note that ISO/IEC 27043 is an international standard for information technology, security techniques, incident investigation principles and processes. Notwithstanding that, Kebande and Venter [9],[18] have proposed a readiness model that uses a botnet as a service that is able to gain incident preparedness. Even though this model is aimed at helping future investigative technologies it was hardly based on mobile devices, its main target was the cloud environment.

2.3 Cyber-Bullying

The increased use of mobile devices and the human-computer interaction associated with mobile devices have seen a sporadic increase on the trend of cyber-bullying. According to Menesini and Žukauskienė [10], cyber-bullying represents some kind of harassment against a cyber-victim by means of new electronic technologies like mobile phones over the internet. A cyber-victim in this context is the individual that the cyber-attack is conducted against. If we refer to the hypothetical scenario highlighted in Section 1, Alice was a cyber-victim that was victimised through iknowwho.com by a group of individuals. Nevertheless, cyber-bullying comes in many forms. Some of the notable forms of cyber-bullying include: Electronic bullying, SMS bullying, Mobile bullying and Internet bullying. Research conducted by Hinduja and Patchin [11] of the cyber-bullying research center has shown that adolescents especially girls experience cyber-bullying attacks in their lifetime. However, 34% of their research showed students were also cyber-victims. Figure 1 shows the statistics based on a survey done on a random sample of 457 students between the age of 11 and 15. Based on this research at least 34% of students have been cyber-bullied, 12.8% reported hurtful comments while 19% reported rumour spread. Interestingly 15% of student admitted cyber-bullying others. Furthermore, previous statistics show that 20% of cyber-victims have considered suicide which is twice as likely as students who have not been cyber-bullied; these statistics can still be linked to the case of *Alice* in the hypothetical scenario in Section 1 of this paper. Having looked at these statistics the next section provides related work to this study.

Fig 1. Cyber-bullying victimization, source (Hinduja and Patchin, [12])

3. RELATED WORK

There exists several related work from different researchers which have made valuable contributions towards the development of the mobile forensic readiness model aimed at minimizing cyber bullying presented in this paper. In this section, a summary of some of the most prominent efforts in previous research work is provided.

To begin with, Karthik et al., [13] argues that the menace of cyber bullying has assumed alarming proportions with an ever-increasing number of young people admitting to having

dealt with it either as a victim or as a bystander. This is evident from the hypothetical scenario of *Alice* given in Section 1 of this paper. Karthik et al.'s paper however concentrates on modelling the detection of textual cyber-bullying, hence did not present any forensic readiness model as is the case of this paper[13]. Their findings though show that the detection of textual cyber-bullying can be tackled by building individual topic-sensitive classifiers.

In another paper, Lambros et al., [14] present a process model of cyber-bullying in adolescence. In their study they state that cyber bullying is an emerging form of aggression that utilizes information and communication technologies. They then employ an integrated theoretical model incorporating empathy, moral disengagement, and social cognitions related to cyber bullying. In this paper however the authors' concentrates on building a mobile forensic readiness model aimed at minimizing cyber bullying.

Serra and Venter [15] also added that, the current mobile communication technology brought on by the internet has meant that people now have mobile access to a wealth of information and services. Despite the fact that, the benefits of mobile information access are acknowledged through the empowering influence over its audience, a concern is noted with reference to largely uncensored forums offering mobile communication exchange to children. They then propose a solution to address cyber bullying problem that is driven by static configurations. Their proposed solution seeks to avail a state of digital forensic readiness (DFR) in order to deliver a proactive solution through risk profiling of a user through usage which dictates the level of protection accordingly.

Several other related works on issues of cyber bullying exist, however, neither those nor the cited references in this paper have presented a mobile forensic readiness model aimed at minimizing cyber bullying as well as enhance awareness on issues of cyber bullying in the way that is discussed in this paper. However, the authors acknowledge the fact that the previous research works have offered valuable insights toward the development of the model in this paper.

4. LEGAL ASPECTS ON CONTENT MONITORING ON MOBILE DEVICE

According to Darryl [16] content monitoring can be understood as a form of electronic monitoring which covers a very broad range of activities such as: content monitoring, video cameras, phone eavesdropping, and location tracking. The California Senate Bill No. 1841, (2004) explains "Electronic monitoring'' as the collection of individually identifiable information concerning individual's activities or communications through the use of electronic devices including, but not limited to, a computer , computer software or other computer program, telephone, wire, radio, camera, or electromagnetic, photo-electronic, or photo-optical system [1].

One of the reasons why people do content monitoring is the avoidance of lawsuits. People can harass each other via mobile devices, email and other electronic medium. Cyber bullying can be done using different electronic resources which can as well create a hostile environment. Darryl [16] adds that, by not performing any content monitoring, you are not addressing any risk of litigation directly. Policies alone will not sufficiently mitigate the risks. Different courts have often made judgments against organisations and individuals based on the fact that they should have known of the abuse (in the case of this paper cyber bulling) if the abuse was deemed flagrant enough.

The authors in this paper therefore argue that the legal aspects of content monitoring should be considered while implementing the forensic readiness model on mobile devices. This helps to safe guard the privacy of individuals. Besides, content monitoring should not be done with the intention of harming privacy. The next section explains the proposed mobile forensic readiness model.

5. PROPOSED MOBILE FORENSIC READINESS MODEL

This section presents a Mobile Forensic Readiness (MFR) model as a contribution showing how the proactive process DFR can be achieved in the mobile device based on the hypothetical scenario that has been presented in Section I of this research paper. The model is presented in two approaches; firstly the authors present a high-level view of the model which is then followed by an all-inclusive MFR model. It is worth noting again that this research is inclined towards Tan [20] and Rowlingson [7] objectives, and the readiness processes defined in this paper complies with the ISO/IEC 27043:2015 standard [8]. Figure 2 show a high-level overview of the MFR model while an all-inclusive model is shown in Figure 3 at a later stage.

5.1 A High-Level Overview of the MFR Model

The high-level view of the MFR model is divided into five distinct parts namely: Mobile Agent (MA) in the part labelled 1, Proactive Forensic Monitoring (PFM) labelled 2, Forensic Report (FR) in the part labelled 3 and the reactive process in the part labelled as 4. Finally, Mobile Alert Management (MAM) is represented in the part labelled 5. The MA represents a mobile agent that monitors mobile events; next the PFM represents potential evidence gathering and preservation processes in a proactive monitoring approach. MAM is responsible for managing potential alerts and lastly the FR presents the forensic report of all the activities. The high-level overview is shown in Figure 1.

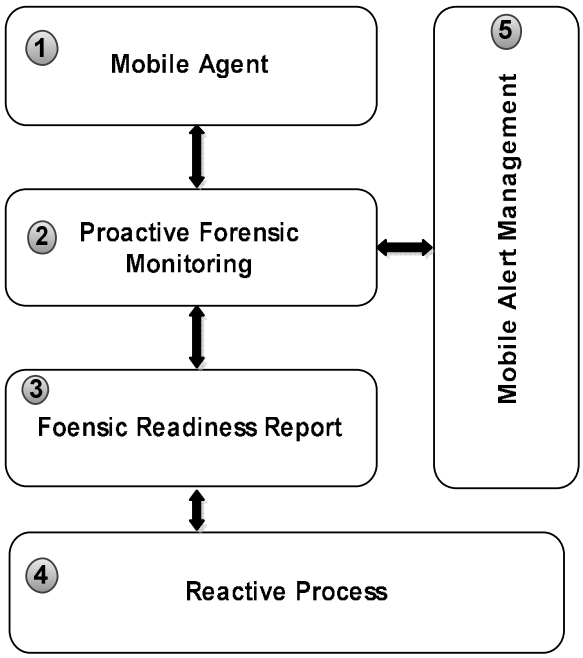

Fig 2. High-level view of the MFR Model

5.1 All-inclusive MFR Model

The all-inclusive MFR model is a detailed model of the high-

level MFR presented in Section 5.1. It consists of different components that represent the entire MFR model. We refer to the hypothetical scenario that was presented as a problem in Section 1. Based on this hypothetical scenario the authors present a discussion on each of the aforementioned distinct parts.

The MA consist of the following entities: Mobile device (MD) and Mobile Agent (MA), on the other hand the PFM consists of the following entities; Potential digital evidence (PDE) gathering and digital preservation. Next, MAM consists of created alerts and Mobile Event Manager (MEM). Lastly the reactive process is presented which represents the post-event response process. The last part represents a forensic report which according to ISO/IEC 27043:2015 should highlight the outcome based on the assumptions made, and probabilities corresponding to those assumptions. Figure 3 below shows the all-inclusive model and the discussions on each of the distinct parts are given in the subsequent sections.

5.1.1 Mobile Agent

The Mobile Agent (MA) consists of the following entities: Mobile device and the agent itself. A mobile device is a mobility device that has a small database as storage, with a mobile operating system which is able to transmit data or communicate without any pre-defined location. Based on the scenario in Section 1, mobile devices were used to orchestrate an attack on Alice, they were easily accessible and through their interactive operating system they could easily be shared amongst Alice's classmates.

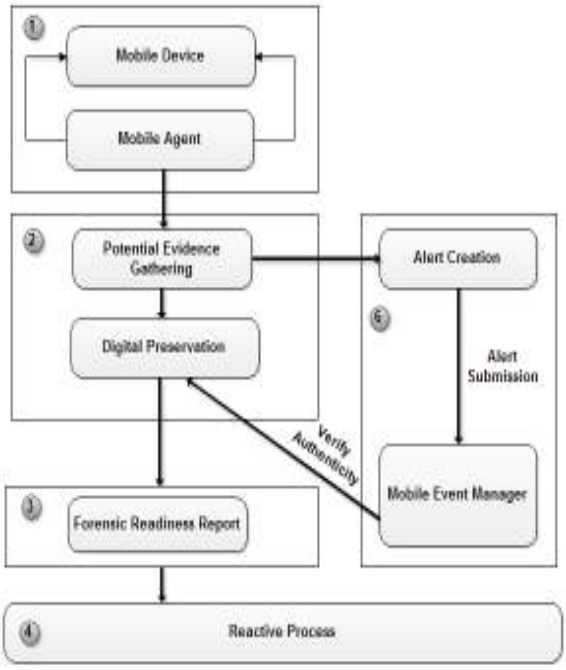

Fig 3. An All-inclusive MFR model

Next is the mobile agent which is used to collect digital evidence. A mobile agent is able to monitor the mobile user's activities and transmit them immediately to a secure storage to ensure proper integrated analysis is done for alert creation. A mobile agent should have collected and gathered the information that was being orchestrated against Alice in a forensic readiness approach which could have essentially sent an alert to prevent these attacks. This is discussed further in the next section.

5.1.2 Proactive Forensic Monitoring

This has been represented in the part labeled 2 of the MFR model that is shown in Figure 3. It mainly consists of potential digital evidence, digital preservation and send_data alert represented by the arrow pointing to the part labeled 5. PDE represents the forensic evidence that is gathered from the pages that are visited by the mobile device. The collected evidence is then digitally preserved through a creation of hashes as described in the ISO/IEC 27043 to maintain and safeguard the integrity or the originality of PDE. The send_data arrow is used to submit alerts of what has been visited which can be managed as explained in the section to follow.

If we refer to the hypothetical scenario: Peter and his accomplices might have gone unpunished because there existed no form of forensic readiness that could have created alerts to prevent *Alice* from hanging herself. In this context, if the law could be applied, Peter and his accomplices could still have managed to be exonerated for lack of sufficient forensic evidence. This is further discussed in the subsequent sections.

5.1.3 Alert and Event Management

The Alert and Event Management (AEM) module mainly consists of two distinct entities. This is shown in the part labeled 3. The entities for this module include: Alert creation and Mobile Event Manager (MEM). Immediately forensic evidence is gathered from the user activities of the mobile, an alert is sent to the AEM where it consists of the created alert from the send_data function. The MEM is able to filter the user activities based on the content data and logs generated through alerts. Verification is thereafter sent to the PDE to see if the generated logs match the digitally preserved evidence. If this is authenticated then a forensic readiness report is generated.

5.1.4 Forensic Readiness Report

In the module labeled 4, a forensic readiness report is generated which consists of a reconstructed and analysed set of user activities. These activities are utilized when performing an investigation through analysing the events between the mobile user and the mobile manager.

5.1.5 Reactive Process

The reactive process as shown in Figure 3 is a post-event response mechanism. It is not part of the readiness process; however, it has been presented to show that, if there is a potential detection of incidents then the digital investigation process should begin. This process has been highlighted by ISO/IEC 27043 as a process that comes after incident detection. In fact it is the process of conducting a digital forensic investigation. Having looked at the MFR model in detail the reader has an intuition on what the components of the MBR contains. In the next section the authors match a number of selected processes to the readiness processes in the ISO/IEC 27043:2025 international standard.

6. MAPPING THE MOBILE FORENSIC READINESS PROCESSES TO THE ISO/IEC 27043:2015 STANDARD

In the previous sections the reader has been introduced to background, related work and the proposed model aimed at minimizing cyber-bullying. The authors' in this section map the MFR model processes proposed in this paper to that of the readiness processes that have been defined in the ISO/IEC 27043. This is shown in Table 1.

Table 1 shows the mapped MFR model processes against the ISO/IEC 27043: 2015 standard [8]. The authors have selected

nine processes to represent the Digital Forensic Readiness (DFR) process. It is worth noting again that the initialization, acquisitive and investigative process that is mapped to the reactive process does not represent the readiness process rather a Digital Forensic investigation Process (DFIP). The next section presents an evaluation of the proposed model.

Table 1. Mapping of the Mobile Forensic Readiness Model processes to ISO/IEC 27043 standard

	ISO/IEC 27043	Mobile Forensic Readiness Model
1	Scenario Definition	Risks against Mobile devices
2	Potential Digital Evidence Sources	Mobile devices
3	Planning pre-incident gathering	Use of Mobile Agent
4	Planning pre-incident storage	Storage in a forensic database
5	Planning pre-incident detection	Alert creation
6	Preservation	Digitally preserving PDE
7	Implementation of assessment result	Verify and authenticate results
8	Reporting process	Readiness Report
9	Initialization, acquisitive, investigative	Reactive process

7. CONCEPT EVALUATION

Considering how cyber-bullying statistics are presented in Figure 1, it is evident that at some point a student has been cyber-bullied. This is relevant to the case of Alice who had to hang herself as a result. The MFR model is aimed at reducing this cynical and anti-social behaviour over digital devices, therefore, parents must not have limited control over the user activities and applications use to store and navigate through different web pages.

Alice a victim of cyber bullying as discussed in Section 1 decided to hang herself because there was no control over what was shared and there was entirely no monitoring, or sufficient forensic evidence that could have incriminated Peter and his accomplices. If forensic readiness could have been applied in this case, there could have been an early control on the orchestrated attack.

At this point the authors believe that the proposed model complies with the ISO/IEC 27043: 2015 standard processes, which ensure that the collected digital evidence can regulate and minimize cyber-bullying if it is admissible in a court of law. This evidence may also be used to create a hypothesis for forensic investigation in order to link the suspect to the crime. Furthermore, the readiness processes for the MFR model have been successfully mapped to the ISO/IEC 27043: 2015 standard for forensic readiness, which makes the process acceptable. By combining both the proactive and the reactive processes, it is possible to implement this model as a tool that can assist the law enforcement agencies to access mobile evidence when needed. Moreover these aspects will maximize the use of digital forensic evidence when needed as highlighted by Rowlingson [7]

The possible applicability of the model is to help parents who wants to have secure control over what their school children are able to view, or to minimize the possibility of being cyber-bullied or bullying others with digital devices. The ramifications are very critical considering the case of Alice. It is vital that the threats that were emanating from the mobile devices as a result of cyber-bullying could have been mitigated if the computational methods used to install the mobile agent to collect potential digital evidence achieve readiness which could have been done by stealth mode as highlighted by Kebande and Venter [17],[18],[19].

Considering that mobile devices as sources of potential evidence have grown and the relevant security events are able to be drawn from these devices, by using the proposed MFR model, there will be a significant improvement based on the forensic outcomes and mitigating strategies. As a result, forensic investigators are able to distinguish the various forms of bullying attacks that are shown in Figure 1. In the next section, a conclusion of the study is given.

8. CONCLUSION AND FUTURE WORK

In this paper, the authors focus on presenting a mobile forensic readiness model aimed at minimizing cyber bullying, as well as enhance awareness on issues of cyber bullying. The details of the model and its applicability including a hypothetical scenario have all been explained. In addition, the model also allows for the addition of new components, including potential modifications in any one of the aforementioned areas.

In the authors' opinion such a model can be used not only to curb cyber bullying but also many other criminal activities. However, considering the current technological trends, more research needs to be conducted so as to improve on the model as well as evaluate its applicability in different scenarios. As part of the future work on this model, the authors will include a functional prototype for the aforementioned aspects of the model as a way to verify and validate any proposed component of the model.

9. REFERENCES

[1] California Senate Bill No. 1841. (April 19, 2004). Retrieved on February 23, 2016 from Website: http://www.steptoe.com/publications/315c.pdf

[2] Olweus, D. "Victimization by peers: Antecedents and long-term outcomes," in Social withdrawal, inhibitions and shyness, K. Rubin and J. Asendorf, Eds. Hillsdale, NJ: Lawrence Erlbaum Associates, 1993, pp. 315-341.

[3] Danesh, A., Inkpen, K., Lau, F., Shu, K., & Booth, K. (2001). Geney: De-signing a collaborative activity for the Palm handheld computer. Proceedings of CHI, Conference on Human Factors in Computing Systems.Seattle: WA.

[4] Roschelle, J. (2003). Unlocking the value of wireless mobile devices. Journal of Computer Assisted Learning 19, 260–272.

[5] K. Brown and S. Singh, "A Network Architecture for Mobile Computing," in Proc. of INFOCOM'96, IEEE, pp.1388-1396, March 1996.

[6] Peng, W. C., & Chen, M. S. (2005). Query processing in a mobile computing environment: Exploiting the features of asymmetry. *Knowledge and Data Engineering, IEEE Transactions on*, *17*(7), 982-996.

[7] Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence*, *2*(3), 1-28.

[8] ISO/IEC 27043: 2015. Information technology -- Security techniques -- Incident investigation principles and processes. Accessed at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44407

[9] Kebande, V. R., & Venter, H. S. (2014). A Cloud Forensic Readiness Model Using a Botnet as a Service. In *The International Conference on Digital Security and Forensics (DigitalSec2014)* (pp. 23-32). The Society of Digital Information and Wireless Communication.

[10] E. Menesini, Smith, P K and Žukauskienė, R, (2009): Cyberbullying: "Coping with negative and enhancing positive uses of new technologies, in relationships in educational settings," Mykolas Romeris University Publishing Center, Lithuania.

[11] S. Hinduja and J. Patchin,(2010) "Bullying, Cyberbullying, and suicide," Archives of Suicide Research, vol. 14, pp. 206-221.

[12] S. Hinduja and J. Patchin(2015)" Cyberbullying Research Center, accessed at" http://cyberbullying.org/2015-data/"

[13] Karthik D.,Roi R. and Henry L.(2011) Modeling the Detection of Textual Cyberbullying. Association for the Advancement of Artificial Intelligence

[14] Lambros L., Vassilis B., Despoina O., Haralambos T., (2013) A process model of cyberbullying in adolescence. Computers in Human Behavior.Vol. 29, No.3.,Pages 881–887.

[15] Serra, S.M. and Venter, H.S., (2010). Mobile cyber-bullying: A proposal for a pre-emptive approach to risk mitigation by employing digital forensic readiness. Information security South Africa conference.

[16] Darryl T. B., (2009). Content Monitoring Issues - Legal and Otherwise. SANS Institute InfoSec Reading Room.

[17] Kebande, V. R., & Venter, H. S. (2015, February). Obfuscating a Cloud-Based Botnet Towards Digital Forensic Readiness. In *Iccws 2015-The Proceedings of the 10th International Conference on Cyber Warfare and Security* (p. 434). Academic Conferences Limited.

[18] Kebande, V. R., & Venter, H. S. (2015, August). Adding event reconstruction to a Cloud Forensic Readiness model. In *Information Security for South Africa (ISSA), 2015* (pp. 1-9). IEEE.

[19] Kebande, V., & Venter, H. S. (2015, July). A Functional Architecture for Cloud Forensic Readiness Large-scale Potential Digital Evidence Analysis. In *Proceedings of the 14th European Conference on Cyber Warfare and Security 2015: ECCWS 2015* (p. 373). Academic Conferences Limited.

[20] Tan, J. (2001). Forensic readiness. *Cambridge, MA:@ Stake*, 1-23.