

Athanasopoulos *et al.* [4] report that OSN consists of some intrinsic properties that make them ideal for exploitation by an adversary. Some of the properties that were highlighted are: 1) a very large and highly distributed user-base; 2) clusters of users sharing the same social interest; and 3) platform openness for deploying fraudulent resources and applications that lure users to install them. Obviously, all of these properties are the reasons why cyber criminals find there is a huge opportunity to manipulate OSN as a platform to commit crimes.

Website phishing is among other criminal activities that have become a particular risk for OSN, whereby phishers will entice users into visiting fraudulent websites and ask them to enter personal identification information such as username, password, address, national identification number and personal identification numbers (PINs). Such sites can be created so as to appear very believable [5]. Tom *et al.* [6] reported that it is very straightforward and very effective for a phisher to exploit social network data on an OSN site, and they suggest that Internet users may be over four times more likely to become victims if they are solicited by someone appearing to be a known acquaintance. There are a huge number of OSN sites for phishers to extract information about similar interests in a group and relationships of users. Most OSN sites develop groups of friends for each profile that allow phishers to collect any relevant social network information. It has been known that malware authors exploit such sites to increase the yield of phishing attacks. For example, it is estimated that more than 72% of users have been targeted by email phishing attacks that exploit information from OSN [6]. The study showed that most OSN users are vulnerable to phishing attacks that can jeopardise their sensitive information such as banking information or credit card details. Personal information obtained through phishing schemes from OSN could also facilitate identity theft, whereby cyber criminals can create a fake profile to impersonate a renowned person by getting the victim's personal details. The most common form of reported identity theft is Credit Card fraud, followed by phone or utilities fraud, then bank and employment fraud [7].

Online sexual predators have also been known to make use of OSN as a medium to attract their victims. Wolak [8] reports that these criminals use information publicly divulged in online profiles and social networking sites to identify potential targets; they contact victims using deception to cover up their age and sexual intentions, enticing unknowing victims into meetings, stalking and/or abducting them. Explicitly, these reports have highlighted the threats of OSN for children and youngsters and also the safety of Internet activities, for instance online communication with strangers, disclosure of personal information online and being involved in OSN generally.

Choo *et al.* [9] note that terrorists could use online chat rooms and OSN as vehicles to reach an

international audience, to solicit funding, to recruit new members and to distribute propaganda. Such *Internet-driven radicalisation* includes cases of radical youths and other individuals linking up with like-minded people, making contact with extremists from overseas involved in terrorist recruitment, and financing over the Internet and in chat rooms. It also includes the use of blogs and OSN. The Simon Wiesenthal Center [10] published a report stating that 8,000 websites espousing radical ideologies such as hosting hate and terrorism-related content have reportedly been identified. Apparently, cyber criminal groups make use of the advances of OSN and other online websites as a medium to communicate among them and exploit the benefits of those websites.

B. Standard Models

The increase of OSN users has resulted in an increase in cyber crimes as reported by various researchers [11, 12]. One of the most significant problems that investigators are currently facing is a lack of standardization, as well as the lack of a theoretical framework for the field of digital forensics. Using ad-hoc methods and tools for the elicitation of digital evidence can limit the reliability and credibility of evidence, especially in a criminal prosecution where both the evidence and the processes used for collecting it can be disputed [13]. To deal with these shortcomings, there is a need to establish a standardized forensic investigation process for OSN. We have therefore developed a new model that will combine the existing frameworks and models, allowing us to compile a comprehensive digital forensic investigation model specifically for OSN. Based on the issues and problems discussed, we therefore propose a standard model of digital forensic investigation for OSN.

III. RELATED WORK

In many ways the Internet has become a major tool for the development of our social networks. Social networking has encouraged new ways of communicating and sharing information and is used regularly by millions of people; it now seems that social networking will be an enduring part of everyday life. OSN generally provides various functionalities including networks of friends, person surfing, private messaging, discussion forums or communities, event management, blogging, commenting (sometimes as endorsements on people's profiles), and media uploading.

There are various types of crimes that can potentially be committed using OSN sites, and most of the evidence of such criminal activity is stored on the service provider's server, such as in cases of identity theft, stalking, digital property theft and child pornography (to name a few). Criminals get in contact with victims via OSN sites and conduct crimes through these networks, thus a variety of evidence is

posted on OSN sites. This might include data, photos or videos [14].

Philip D. Dixon in his article “An overview of computer forensics” [15] states that the core goals of computer forensics are: the preservation, identification, extraction, documentation, and interpretation of computer data. There are various models and frameworks that have been defined and considered to ensure that the forensic data is valid and useful in legal affairs. However, none of the models have been specifically built with digital forensic investigation of OSN in mind. The motivation of this research comes from a number of sources that are discussed further in the following paragraphs.

Lee *et al.* proposed The Scientific Crime Scene Investigation Model [16] that consists of four steps, but only highlights a part of the forensic investigation process: recognition; identification; individualisation and reconstruction [17]. Casey [18] proposes a framework similar to Lee but the framework focuses on processing and analysing digital evidence with two other steps that are preservation and classification. In both Lee and Casey’s models, the first and last steps are identical and they explicitly focus on the investigatory process without any process before the investigation takes place or afterwards, such as might occur for documentation or presentation.

The U.S. Department of Justice published a model [19] that consists of four process. These are: collection; examination; analysis; and reporting. The analysis and examination process of this model are not well described and are even somewhat confusing. The process seems redundant since the analysis and examination process look at the same potential evidence, and in certain cases, are examined by the same person. The Digital Forensics Research Working Group (DFRW) developed by the National Institute of Justice subsequently proposed a framework [20] that combines the stages in the three previous models but adjoins two further final stages: presentation and decision. This framework introduces a number of important stages into the digital forensic investigation and generally combines all of the crucial processes needed for a general investigation.

Carrier and Spafford [21] propose a model that clusters 17 process into five groups. The groups are made up of readiness process; deployment process; physical crime scene investigation process; digital crime scene investigation process; and review process. This model seems ideal; it includes issues of data protection and acquisition, imaging, extraction, interrogation, normalisation, analysis and reporting. Nevertheless, this model still has a number of shortcomings. Baryamureeba and Tushabe [22] note that the first issue arises in the deployment process involving the confirmation process of an incident.

However in real practice it is not viable to confirm a digital crime until an investigation is carried out. The second issue highlighted is that the framework does not provide details of the process, for example, by drawing a clear distinction between investigations at the victim’s scene and those at the potential suspect’s scene. Since a computer can play the role of being both a tool for committing a crime and as the target of a crime, the investigation should be performed entirely to make sure that accurate digital evidence is collected [9].

Ciardhuáin [23] proposed another model in which the processes in the model are called ‘activities’. The model consists of 13 activities, four of which are applied by previous models. The new activities that he includes in his model are: awareness; authorization; planning; notification; transportation; storage; hypothesis; proof/defence and dissemination. The steps are discussed in depth in the paper. Even though the activities seem novel, some of the activities play the same role as in other models. For instance, the dissemination activity is the same process as presentation as used by a number of other models.

From these previous models and frameworks, a number of important issues can be identified. Firstly, the models and frameworks proposed are basically developments of earlier models and most have quite similar approaches. Secondly, some of the models are generic and do not focus on the purpose of the investigation [24]. Obviously there is no standard and consistent model – only sets of procedures and tools – thus many digital crime investigations are performed without proper guidelines. Moreover, there is no model built specifically for OSN but in contrast digital crimes related to OSN are growing rapidly as discussed above.

Based on these issues and problems, we have tried to create a coherent and encompassing model that focuses on the best elements of other models, as well as those elements more applicable to digital forensic investigations involving OSN.

IV. PROPOSED MODEL

As we have identified, one of the significant problems being faced for digital forensic investigations of OSN is a lack of standardization, as well as the lack of a theoretical framework for the field. Using ad-hoc methods and tools for the elicitation of digital evidence can limit its reliability and credibility. Based on the literature, we can identify some common features of digital forensic investigation models. Subsequent to an analysis as shown in Table 1, we have discovered various additional features of OSN digital forensic investigation models as follows.

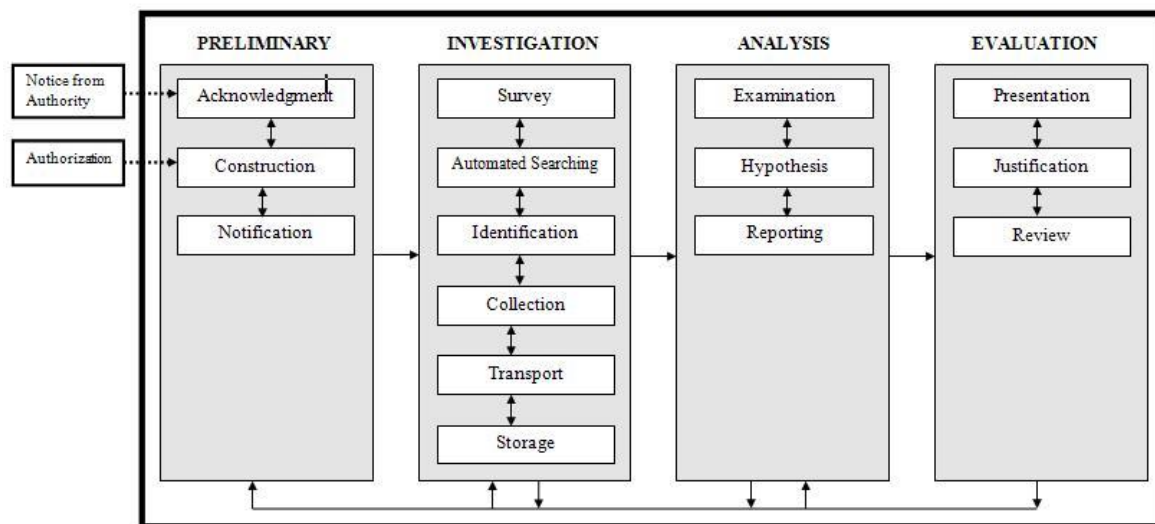


Fig. 1. The proposed model of digital forensic investigation for Online Social Networking.

- The investigation takes place through online mode where most of the potential evidence is stored in OSN providers' databases.
- There is a variety of information that can be obtained through an OSN account, and which is likely to be useful for an investigation. Such information includes the user's profile containing full name, home address, telephone number, location, history of education and work; links to other users with whom they have connections and relationships; and also media being shared.
- The evidence and information searching process is an iterative process whereby an investigator will search for the profiles of particular users, then profiles of these users' friends, also profiles of friends of the users' friends and so on. The depth of iteration will depend on the incident being investigated.

To include those additional features, we have proposed a new model that consists of four processes. The proposed model is shown in Figure 1. The next section will discuss the activities in each of the processes in detail.

A. Preliminary

After an incident occurs, the investigation will commence in the *Preliminary Process*. The purpose of this process is to validate, measure, and plan the strategy that will be applied in the proceeding processes.

The regular method used by traditional digital forensic investigations involves validation of the incident and assessment of the situation before developing an appropriate strategy. Then the process

is followed by checking on any requirements for the investigation such as human resources, special equipment or legal resources. In OSN digital forensic investigations, we will determine what to look for in the OSN site. Activities might involve planning which profiles to initially focus on, determining the important connections between profiles, or identifying what kind of information to look for in the profiles depending on the type of incident being investigated.

B. Investigation

The *Investigation Process* consists of a number of activities related to the OSN investigation. The aim of this process is to collect and store potential digital evidence and the information required in order to proceed with the investigation. During this process, the steps that will be involved will include the following.

- Online searching of users' or targets' profiles, the link between targets that can contribute to useful information related to the incident being investigated, and any potential evidence and information from the profile.
- Any potential evidence found will be collected in a forensic manner to make sure that the evidence is valid and presentable in a court of law or as part of any other relevant legal process or procedure.
- These steps will be repeated if it becomes necessary to collect information and evidence from more than one profile.
- Once the potential evidence has been found, it must be stored and the evidence transported for analysis.

TABLE 1
Mapping Of Previous Models With The Proposed Model

Proposed Model	Acknowledgment	Construction	Notification	Survey	Automated Searching	Identification	Collection	Transport	Storage	Examination	Hypothesis	Reporting	Presentation	Justification	Review
Department of Justice, 2001															
Collection							√								
Examination										√					
Analysis															
Reporting												√			
Reith et al, 2002															
Identification	√														
Preparation [for the current investigation]		√													
Approach strategy		√													
Preservation							√								
Collection							√								
Examination										√					
Analysis															
Presentation													√		
Returning evidence														√	
Carrier and Spafford, 2003															
Readiness	√														
Deployment		√													
Digital crime scene investigation															
Preservation															
Survey				√											
Documentation												√			
Search and collection															
Reconstruction											√				
Presentation													√		
Review															√
Ciardhuáin, 2004															
Awareness	√														
Authorization		√													
Planning		√													
Notification			√												
Search/Identify				√		√									
Collection							√								
Transport								√							
Storage									√						
Examination										√					
Hypothesis											√				
Presentation													√		
Proof/Defence														√	
Dissemination															√
Casey, 2004															
Recognition						√									
Preservation							√								
Classification										√					
Reconstruction											√				

C. Analysis

The *Analysis Process* is a crucial part of the forensic investigation. In this process, the investigator will need to verify that all evidence and information found is connected to the incident being investigated. The traditional activity during the analysis process usually involves the examination and analysis of evidence to determine its value and impact. In OSN digital forensic investigations, the steps that will be carried out are as follows.

- Analysing the suspect's information by recording any evidence found from the profile.
- In some incidents, it will be useful to map connections of the suspect's profile with other people in order to obtain constructive evidence.

D. Evaluation

The *Evaluation Process* of the OSN digital forensic investigation does not differ significantly from the evaluation process of previous models. In this process the investigator will present the evidence through documentation and report. The investigator

will have to make sure that the aim of the investigation is met by presenting valid evidence and information.

V. CONCLUSIONS AND FUTURE WORK

In this paper we have reviewed the existing literature in the area of digital forensic investigation models and frameworks, with a particular focus on OSN. We have proposed a comprehensive digital forensic investigation model specifically for OSN that will fulfil the essential requirements of OSN digital forensic investigations.

Since this is an ongoing project, we intend to develop the model further in a number of directions. First, we will make some refinement of the process to ensure that it is moulded carefully to the requirements of OSN digital forensic investigations. We will carry out a number of case studies to validate the refined model. Subsequently, we plan to develop a tool that can hierarchically map links or connections of a profile, in order to aid the investigatory process. Such a tool would be useful in OSN digital forensic investigations since it can help the investigator to find connections among people which can indicate the discovery of important evidence. Also, we will develop a prototype for this model and evaluation of the developed model will be carried out to make sure the purpose of developing the model is met, and that the functionality is faultless and meets the essential requirements of the OSN digital forensic investigation model.

REFERENCES

- [1] D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication*, vol. 13, pp. 210-230, 2008.
- [2] D. Hughes, P. Rayson, J. Walkerdine, K. Lee, P. Greenwood, A. Rashid, C. May-Chahal, and M. Brennan, "Supporting Law Enforcement in Digital Communities through Natural Language Analysis " in *Computational Forensics*, vol. 5158/2008: Springer Berlin / Heidelberg, 2008, pp. 122-134.
- [3] O. Angelopoulou, "ID Theft: A Computer Forensics' Investigation Framework," presented at Proceedings of The 5th Australian Digital Forensics Conference Perth, Western Australia, 2007.
- [4] E. Athanasopoulos, A. Makridakis, S. Antonatos, D. Antoniadis, S. Ioannidis, K. Anagnostakis, and E. Markatos, "Antisocial Networks: Turning a Social Network into a Botnet," in *Information Security*, 2008, pp. 146-160.
- [5] M. Tyler and C. Richard, "Examining the impact of website take-down on phishing," in *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*. Pittsburgh, Pennsylvania: ACM, 2007.
- [6] N. J. Tom, A. J. Nathaniel, J. Markus, and M. Filippo, "Social phishing," *Commun. ACM*, vol. 50, pp. 94-100, 2007.
- [7] F. T. Commission, "National and State Trends in Fraud & Identity Theft, January - December 2004," 2005.
- [8] J. Wolak, D. Finkelhor, K. J. Mitchell, and M. L. Ybarra, "Online 'predators' and their victims: Myths, realities, and implications for prevention and treatment," *American Psychologist*, vol. 63, pp. 111-128, 2008.
- [9] K.-K. R. Choo, R. G. Smith, and R. McCusker, "Future directions in technology-enabled crime: 2007-09 " Australian Institute of Criminology 2007.
- [10] "iReport: online terror + hate the first decade," Simon Wiesenthal Center 2008.
- [11] M. L. Ybarra and K. J. Mitchell, "How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs," *Pediatrics*, pp. peds.2007-0693, 2008.
- [12] J. Snyder and D. Carpenter, "MySpace.com – A Social Networking Site and Social Contract Theory " *Information System Education Journal*, vol. 5, pp. 1-11, 2007.
- [13] M. Karyda and L. Mitrou, "Internet Forensics: Legal and Technical Issues," presented at Workshop on Digital Forensics and Incident Analysis, International 2007.
- [14] R. R. Yager, "Intelligent social network modeling and analysis," presented at Intelligent System and Knowledge Engineering, 2008. ISKE 2008. 3rd International Conference on, 2008.
- [15] P. D. Dixon, "An overview of computer forensics," *Potentials, IEEE*, vol. 24, pp. 7-10, 2005.
- [16] H. Lee, T. Palmbach, and M. Miller, *Henry Lee's Crime Scene Handbook*: Academic Press, 2001.
- [17] H. Jones and J. H. Soltren, "Facebook: Threats to Privacy," 2005.
- [18] E. Casey, *Digital Evidence and Computer Crime*, 2nd ed: Elsevier Academic Press, 2004.
- [19] "Electronic Crime Scene Investigation: A Guide for First Responders.," U.S. Department of Justice July, 2001.
- [20] N. I. o. Justice, "Results from Tools and Technologice Working Group, Governors," presented at Summit on Cybercrime and Cyberterrorism, Princeton NJ, 2002.
- [21] B. Carrier and E. H. Spafford, "Getting Physical with the Investigation Process," *International Journal of Digital Evidence*, vol. 2, Fall 2003.
- [22] M. V. Baryamureeba and F. Tushabe, "The Enhanced Digital Investigation Process," presented at Digital Forensic Research Workshop Baltimore, MD, 2004.
- [23] S. Ó. Ciardhuáin, "An Extended Model of Cybercrime Investigations," *International Journal of Digital Evidence*, vol. 3, 2004.
- [24] M. Kohn, J. H. P. Eloff, and M. S. Olivier, "Framework for a Digital Forensic Investigation," presented at Proceedings of the ISSA 2006 from Insight to Foresight Conference, Sandton, South Africa, July 2006.