Digital Forensics in Second Life

by

Anastassia Sergeevna Rakitianskaia

Submitted in partial fulfillment of the requirements for the degree
Master of Science (Computer Science)
in the Faculty of Engineering, Built Environment and Information Technology
University of Pretoria, Pretoria

September 2014

Publication data:

Anastassia Sergeevna Rakitianskaia. Digital Forensics in Second Life. Master's dissertation, University of Pretoria, Department of Computer Science, Pretoria, South Africa, September 2014.

Digital Forensics in Second Life

by

Anastassia Sergeevna Rakitianskaia
E-mail: arakitianskaia@cs.up.ac.za

Abstract

Computers and the internet have become an integral part of our lives. People have grown accustomed to feeling constantly connected to the outside world, and in the past couple of decades online social networks and three-dimensional online virtual worlds have gained great popularity. In addition to social connections, virtual worlds (such as Second Life, a popular virtual world) offer their users opportunities for both work and play, and let them take part in things that might have been impossible in real life. However, the human factor plays a big role in the formation of the virtual community. The feeling of false anonymity online might lead to a feeling of freedom from any laws that govern the real world, and possibly facilitate offensive behaviour.

The problem addressed by this study is the need to determine whether digital forensic techniques can be applied to an incident inside the Second Life environment (i.e. offensive behaviour between avatars, while logged in to Second Life), as well as to find possible sources of evidence accessible via the standard Second Life viewer. The former also requires a classification of various offenses committed in Second Life, in order to determine which actions are to be regarded as offences, and whether these actions occur inside or outside of the Second Life environment. In this dissertation the author's own classification of various real-life offences is provided, together with a mapping of these offences to their alternatives in Second Life. Second Life is analysed and explored from a forensic perspective.

A new digital forensic process model, derived from various existing models in the literature, has been developed by the author for this study. The model is designed to accommodate for the specifics of a virtual world environment. An exploratory experiment

has been undertaken by the author in order to investigate how inexperienced users perceived Second Life, as well as how they reacted to attacks from other users, to identify the possible sources of evidence, and suggest possible digital forensic techniques based on the gathered data.

Keywords: *digital forensics, forensic process, virtual worlds, Second Life, experiment*

Supervisors : Prof. M. S. Olivier
Mr A. K. Cooper
Department : Department of Computer Science
Degree : Master of Science

"The 'self-image' is the key to human personality and human behavior. Change the self image and you change the personality and the behavior."

Maxwell Maltz

"All life is an experiment. The more experiments you make the better"

Ralph Waldo Emerson

Acknowledgements

I would like to thank the following people for all the support given to me during my studies:

- My supervisor, Prof. MS Olivier, for professional guidance and patience;
- My co-supervisor, Mr AK Cooper, for forcing me to meet the deadlines and always coming up with interesting thoughts and ideas;
- Mr K Eloff, for the help in the organisation of the experiment for this research, and the aid in gaining access to the required research facilities;
- All the participants of the undertaken experiment, for aiding me in gathering valuable data for my research;
- My parents, for always being there for me, and encouraging me to do my best;
- My sister Anna, for being my role model and the best friend, and always making me smile;
- Pierre Rautenbach, for being himself, and never failing to make me laugh;
- Johan van Jaarsveld, for being funny, and being a loyal friend through and through;
- Liam Borgstrom, for lifting my spirits when I needed it most;
- The University of Pretoria, for giving me the opportinity to learn and become proficient in my field of study.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

> *People have always yearned for the impossible: magic, flight, time travel, immortality. Writers and artists fantasized about it and created fantastical worlds where people were born with wings or could become immortal. But what if one could learn to fly? What if there was a world where a person could do magic and did not age, get ill, or die? Where any person could, on a whim, become anyone they desire, and travel freely through thousands of realistic and magical worlds? And all of that - at no cost, physical or financial. Virtual worlds hold the answer to these impossible desires. Enter a virtual world and transform into someone you have always dreamed to be, fly, slay dragons, and travel across space. Create an avatar, giving life to an alternative personality which lives its own life, independent of the real world. But beware of the evil, brought by the inhabitants of this would-be paradise.[101]*

In the past two decades the internet has become an integral part of people's lives. People send e-mails and digital post-cards instead of writing letters and sending them by post, and most goods, such as clothes, books, or digital accessories, are available for online purchase at digital stores such as Amazon[1]. Smartphones and tablet PCs have also become popular in the past few years, bringing the internet to one's fingertips at any

[1] http://www.amazon.com

time. The internet has vastly expanded people's social circles and facilitated social interaction. Online social sites launched in 1985, with The WELL[2] as the pioneer [109], and SixDegrees.com (now non-existent) following suit in 1997. Online communities grew in popularity ever since [14]. Primal examples of currently popular social networks are Facebook[3] (launched in 2004), Twitter[4] (launched in 2006), and Tumblr[5] (launched in 2007) [14]. Three-dimensional (3D) gaming social spaces such as World of Warcraft[6] have also received acclaim, and in the past couple of decades popularity of 3D virtual worlds such as Second Life started catching up to the two-dimensional (2D) social networks (e.g. Habbo Hotel[7]), and web-based social networks (Twitter, Facebook). Virtual worlds offer opportunities for both work and play, and let one take part in things that might have been impossible in real life.

A Virtual World (VW) can be defined as "simulated persistent space based on the interaction by computer, inhabited by several users, who are represented by iconic images called avatars, who can communicate with each other and with the world in a synchronized way" [107]. However, that definition is focused on the technical aspects of virtual worlds, disregarding the psychological impact of the interaction with these environments on the users. The author believes that virtual worlds should be regarded as something much bigger than just another communication platform. Offering virtually limitless opportunities to their users, virtual worlds can become a platform for self-realisation, artistic freedom, business, or education. Second Life is one the most popular social virtual worlds to date, populated by millions of people from various countries and cultural backgrounds. It is an immersive environment which is made up of various inner islands, or "sims" (taken from the word "simulations") [129], some representing real life and some being implementations of imaginary locations and sceneries. All these sims function in a way similar to the real world: people can see each other and interact with each other

[2] http://www.well.com/

[3] http://www.facebook.com/

[4] http://twitter.com/

[5] http://tumblr.com/

[6] http://us.battle.net/wow/

[7] http://www.habbohotel.com/

via verbal as well as non-verbal communication. They can touch, pick up, and make use of objects, take photos and film videos, attend live concerts and participate in sporting events, as well as engage in various other activities. Some might consider it simply a game, but others take it as an alternative life with endless opportunities which are not available to them in real life. Over the years Second Life developed its own independent economy using the virtual currency Linden Dollars (L$) which can be purchased using real-world currencies, as well as exchanged into real currency. It becomes apparent that Second Life has grown to make a considerable impact on the lives of those members of the community who take the online world seriously [80]. With regards to virtual assets gaining real value, the popularity of Second Life raises security concerns regarding criminal activity inside the virtual world.

Second Life is populated by the same people that populate the real world, thus the human factor plays a big role in the formation of the virtual community. By creating virtual identities some people create personalities completely different to their own and prefer to behave in a way their real selves never could or never would. The feeling of false anonymity online might also lead to a feeling of freedom from any laws that govern the real world, including moral laws. Such a psychological impact might, in turn, facilitate offensive behaviour. This raises concerns as to whether Second Life is, in fact, as idyllic a world as one might think it to be. Sometimes avatars engage in "griefing" - malicious activities in order to harass other avatars and otherwise disturb their virtual world experience [38]. As was mentioned above, the residents are able to turn Linden Dollars into real currency, and that fact is bound to attract fraudsters and other offenders willing to obtain the in-world currency via illegal means. Second Life is also open about the adult-oriented areas of the environment, and such areas at times prove to be platforms for child pornography distribution [36]. Among others, these factors suggest that offenses in Second Life need to be studied and investigated, in order to find ways of preventing the perpetrators' activity in-world. Possible ways of carrying out a digital forensic investigation in a virtual world such as Second Life should also be explored.

The rest of the chapter is outlined as follows. Section 1.1 states the problem addressed by the dissertation. Section 1.2 lists the main objectives of this study. Section 1.3

summarises the original contributions of this work. Section 1.4 outlines the structure of the rest of this dissertation.

1.1 Problem Statement

The problem addressed by this study is the need to determine whether digital forensic techniques can be applied to an incident inside the Second Life environment (i.e. between avatars, while logged in to Second Life), as well as to find possible sources of evidence accessible via the standard Second Life viewer. The former also requires a classification of various offenses committed in Second Life, in order to determine which actions are to be regarded as offences, and whether these actions occur inside or outside of the Second Life environment. Offensive behaviour in virtual worlds has been researched before [4, 23, 45]; however, none of the studies considered a digital forensic process applied to an incident in a virtual world. The various offenses which are possible in the Second Life environment have not been studied in-depth, and such offences are rarely put together and formally classified.

In this dissertation the author presents a classification of a number of real-life offences according to their subject (e.g. an individual or an individual's property), and maps them to the virtual world of Second Life. Based on various conditions that need to be met for each offence to occur in real life the author derives a Second Life alternative to those real-life offences which are found to be applicable to a virtual world. The author also presents an original digital forensic process model, based on a number of existing digital process models. The model is designed to accomodate the digital nature of offences occuring in virtual worlds by adapting or eliminating steps of the existing models which are not applicable to "virtual" cases. A simple case of griefing in Second Life is simulated in an experiment, and critically analysed, in order to determine whether previously discussed forensic tecniques are applicable and effective when used by inexperienced Second Life residents.

1.2 Objectives

The primary objectives of this dissertation are summarised as follows:

- To provide an overview of the field of digital forensics, including the different branches created in the field, and a number of digital forensic process models. (Chapter 2)
- To adapt the existing digital forensic process models to a forensic investigation in a virtual world by creating a new derived model. (Chapter 2, Section 2.2.2, Chapter 7, Section 7.2)
- To provide an overview of virtual worlds, namely their characteristics and the security threats they pose. (Chapter 3)
- To provide an overview of Second Life, and show what makes it stand out among the rest of the virtual worlds available online. (Chapter 4)
- To map real-world offenses to Second Life and derive Second Life alternatives to those offenses. (Chapter 5)
- To present a classification of the offenses and determine which offenses are committed inside the virtual world, i.e. without the aid of any external devices or software. (Chapter 5, Section 5.3). The matter of criminal law is, however, outside of the scope of this dissertation and is not considered.
- To set up and conduct an exploratory experiment to find ways griefing can be committed and counteracted in Second Life by inexperienced users of the virtual world, as well as how to collect evidence of it from inside the standard Second Life viewer. (Chapter 6) The "inside" characteristic of virtual offences is a very important factor in this dissertation, since the victims of griefing, according to the literature, are mostly inexperienced users. Thus it is important to explore ways to gather evidence through the standard Second Life viewing software, seeing as it is the default Second Life software every new resident starts interacting with.

  The experiment was taken through the research ethics committee of the University of Pretoria and was approved by the committee.

- To describe possible sources of evidence for offenses committed inside Second Life. (Chapter 7, Section 7.1.1)
- To present some possible digital forensic techniques for investigation of offenses in Second Life.(Chapter 7, Section 7.1.2)

1.3 Contributions

This study made a number of novel contributions to the field of digital forensics. Real-world offenses were mapped to the Second Life environment, and Second Life alternatives to each were discovered. The offenses were also categorised according to the subject of the offence. The author developed a digital forensic model adapted specifically for investigations of offences occuring in virtual worlds. An experiment was carried out, showing possible ways of gathering evidence of griefing in Second Life. Possible sources of evidence, accessible from the standard Second Life viewer, as well as possible digital forensic techniques, were presented.

1.4 Dissertation Outline

The rest of the document is organised as follows. **Chapter 2** covers the field of digital forensics. It provides an overview of the field, discusses the digital forensic process, and looks at a number of different digital forensic process models presented in the literature. The chapter also presents the author's own digital forensic process model, based on the previously discussed models and adapted to a digital forensic process conducted in a virtual world. **Chapter 3** gives an overview of virtual worlds. It looks at a number of different types of virtual worlds, discusses the characteristics common to all of these types, as well as addresses some of the virtual worlds' security concerns. The figures presented in this chapter belong to the public domain and are listed on various help and overview resources of the respective virtual worlds[8], unless credited otherwise. **Chap-**

[8]e.g. "All About Faces - A Newbie Help Guide", found at http://b.whyville.net/smmk/help/newbie-aboutFaces

ter 4 provides an overview of Second Life. It discusses the history of its making and a number of its aspects which make it stand out among the rest of the virtual worlds available online, such as the fact that some Second Life residents regard their Second Life avatars as real second identities. The chapter also addresses the forensic relevance of Second Life as a means of committing offences such as fraud and identity theft. **Chapter 5** focuses on offensive behaviour of avatars in Second Life. It provides the author's mapping of real-life offenses to their alternatives in Second Life, as well as the classification of the offenses according to the subject of the offense. It also discusses people's real-life experiences of Second Life offenses. **Chapter 6** describes the researcher's experiment on griefing in Second Life. The experiment set-up and procedure is described in detail, and the participants' responses are studied and discussed. **Chapter 7** discusses digital forensics in Second Life. It gives an overview of possible sources of evidence of Second Life offenses, accessible through the standard Second Life viewer, as well as possible digital forensic techniques applicable in a forensic investigation in Second Life. It also discusses the preservation phase of the author's digital forensic process model as the most relevant to the process of evidence gathering. **Chapter 8** lists the conlusions of this work, as well as some possible topics for future research.

The appendices of this dissertation are as follows:

- **Appendix A** shows the informed consent form given to each experiment participant before the experiment commenced.
- **Appendix B** provides the questionnaire given to the experiment participants after they completed their tasks in the experiment.
- **Appendix C** provides the log of the public chat between the members of the experiment.

Chapter 2

Digital Forensics

This chapter provides a brief overview of the field of Digital Forensics. It explains what the field stemmed from and what it is used for, and discusses the work previously done in the field. It also gives an overview of the digital forensics process, discussing various digital forensic models available in the literature. Based on the models studied, the author presents a new digital forensic process model, adapted to the specifics of a digital forensic process carried out in a virtual world. Finally, a number of different branches of digital forensics are listed and given a brief overview of. The chapter is concluded with a summary of the topics covered and a brief discussion on the way they fit into the context of the current research.

2.1 Overview

Forensic science is a field of study centered around gathering and analysing evidence obtained primarily at a crime scene. Its principles are followed in an attempt to answer questions most commonly related to a crime or a civil action. Forensic science consists of gathering evidence, analysing it, and presenting the findings in court [72], which may determine or help determine the outcome of the investigation. In the old days the evidence considered reliable was physical evidence such as fingerprints, pieces of clothing, hairs, blood stains, among others. A way to find the criminal was to gather all the different pieces of physical evidence, together with information from various witnesses

and people who could have been involved in the crime, and to analyse it, in order to logically re-create the crime scene. The findings could then be presented in court. Based on whether the findings were consistent with the acusation or exculpatory to it, the accused would be either convicted or cleared of all charges.

The modern world can be justly called "digital world" due to the ever-increasing degree of dependency on digital processes, devices, and networks. Computers are a part of almost every household and every business, and take part even in our day-to-day activities. This digitalisation affected the existing study fields, which now make extensive use of digital devices, as well as created the need for foundation of totally new fields, such as Computer Science. Forensics was one of the study fields the horizons of which were broadened by the invention of computers and other digital devices. However, having been designed to be used by humans, the new digital aspect of human life was still affected by the human factor. Humans are not perfect, and even though forensic science has been empowered by digital technology it is still prone to human error, as well as misuse. There is always room for misuse of any technology unintentional, as well as intentionally malicious. Cyber crimes cannot be called "new"; they are just another realisation of the malicious, unlawful, and unethical intentions of criminals who found new opportunities in digital technology. Evidently, cybercrimes require investigation, and cybercriminals have to be pursued by the same laws as all the other criminals. Thus the field of digital forensics was born - a branch of the classic forensic science focused on gathering evidence from digital sources. At first it was used as a synonym for Computer Forensics [96], but nowadays the field has expanded and digital forensics became an independent term governing the forensic processes conducted on both computers and all the other digital devices that were invented in the 20th, as well as the 21st century. One of the definitions of computer forensics states that computer forensics consists of "[v]alid tools and techniques applied against computer networks, systems, peripherals, software, data, and/or users" [96], and is "the collection of techniques and tools used to find evidence in a computer" [18], whereas a definition of digital forensics covers a much broader spectrum of subjects [94]:

> "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation,

> and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations"

Computer forensics focuses on making use of specialised tools and techniques that would aid one in collection and investigation of evidence found on a computer, while the scope of digital forensics is much wider, allowing for investigation of all the various digital systems and devices available nowadays. Digital forensic scientists can obtain important information from CDs, DVDs, mp3-players, smartphones, tablets (and other handheld devices), as well as computers system files, such as log files, dynamic link libraries, registry files, catalog files, etc., and deleted files, temporary internet files, and browser's cache [19]. The evidence can also be concealed in databases on online servers as well as local machines, inside image and sound files, inside e-mail headers, and in packet data sent via a network from one machine to another, ranging from ethernet to the world wide web [19]. However, even this list of evidence sources cannot be called an exhaustive list of locations which digital evidence can be extracted from. Overall, digital forensics follows similar principles as the classic forensics, namely collecting evidence, analysing it by the means of specialized tools (in case of digital forensics it is specialised software), and then presenting the findings in court.

High dependency on the digital technologies does not allow for disregard of the vast amount of ways cyber criminals could affect systems and infrastructure, as well as private lives. Cyber attacks vary from simple irritations to serious threats to people's wellbeing. Thus it is highly important to address the security problems associated with various digital devices and systems, in order to develop reliable, fast, and cost-effective techniques and solutions that would allow for collection and preservation of as much evidence as possible, as well as an effective analysis of hidden, tampered, or encrypted data. The work that has been done in the field of digital forensics up till now and the work that is currently being undertaken by researchers is of utmost importance not only to the research community, but also to investigators and other forensic specialists, ensuring effective collection and analysis of evidence during ivestigations.

2.2 Digital Forensic Process

An important part of a digital forensic investigation is the process thereof, i.e. the approach and methodology used to conduct the investigation. It is crucial to make sure the process is followed accurately from the first step to the last. Omitting a certain step or conducting a part of a certain step inaccurately and thus incorrectly may result in a criminal escaping rightful conviction, or even an innocent being falsely accused based on unreliable evidence. The following sections consider and discuss some of the digital forensic process models found in the literature, as well as derive a simple model of a digital forensic process which would be applicable to a digital forensic investigation in a virtual world such as Second Life.

2.2.1 Previous Work

A digital forensic investigation, according to Kruse and Heiser [56], consists of three crucial steps, or three As:

- acquiring the evidence, as well as ensuring the evidence is not corrupted during the course of the investigation;
- authentication of the reliability of the collected data;
- analysing the evidence, as well as ensuring the validity of the data throughout the investigation.

Those steps are abstract in the sense that they do not depend on any specific technologies, making it usable in any kind of a digital forensic investigation. However, this model is a very high-level description of the process, which could make it difficult to apply in a real-life investigation.

The U.S. Department of Justice (DOJ) developed an abstract digital forensic process model incorporating four core phases, namely collection, examination, analysis, and reporting [92]. The collection phase implies searching for any available evidence, collection, and documentation of the findings. It is crucial to preserve the integrity of the evidence while at this phase of the investigation, as well as throughout the whole digital forensic

process. The examination phase involves inspecting the collected evidence and trying to make it accessible by revealing any information that may be encrypted or hidden on a digital device. Providing relevant documentation is also necessary at this phase. During the analysis phase the evidence undergoes examination once more; however, contrary to the examination phase, the goal of the evidence examination during the analysis phase is to determine the validity of the evidence and its significance to the current investigation, as well as to draw findings and certain conclusions about the investigated case. The reporting phase consists of writing a report with the outline of the conducted investigation process, and listing all the data that has been found during the investigation, as well as the results of the evidence analysis. One of the pros of this digital forensic process model is the fact that it can be applied to a digital forensic investigation in any environment, and to any digital devices, due to the fact that the model is not dependent on any specific technologies. However, the shortcoming of this model is in the fact that the specifications of the examination phase and the analysis phase are quite ambiguous. Neither of those phases are thoroughly defined and thought through, thus the processes involved in one phase can be confused with the other. It is a considerable drawback since, as mentioned earlier, it is of utmost importance that all the steps in the digital forensic process are followed to the letter.

Another digital forensic process was defined by the Digital Forensic Research Workshop (DFRWS). The DFRWS developed a framework that consists of "identification, preservation, collection, examination, analysis, presentation, and decision" [94]. Each of the seven phases is assigned specific tasks and processes that have to be undertaken during that phase.

The identification phase consists of the detection of the crime that has taken place, examination of any unusual events, inspection of possible criminal profiles available at that point, as well as monitoring of the affected system for any anomalous processes or data.

The preservation phase speaks for itself; it implies preserving the available evidence, and governs processes of imaging, i.e. creating perfect copies of the evidence, as well as case management and some other minor processes. The collection phase makes use of the existing technologies to collect the evidence from the digital device and reduce the

data to only the evidence relevant to the current case. This implies that the evidence has to be examined and proven authentic before undergoing the process of reduction. Preservation of validity and integrity of the evidence is crucial throughout the whole process. Processes of recovery of all the data that might have been made unavailable before this stage are also a part of the collection phase of this digital forensic process model.

The examination phase which follows the collection phase utilises the validation and filtering techniques [94] available to the investigators in order to sort the evidence provided by the collection phase and limit its already roughly filtered data to the valid evidence that is relevant to the case. This phase also involves going through the processes of extraction of any hidden, as well as all the encrypted and other purposefully obscured data, and revealing its contents to the investigators. Specialised techniques (such as pattern matching) are applied in the analysis of the available data to discover any similarities in the data, as well as to create a map of inter-related information, which would aid the investigators in drawing of important conclusions from the evidence.

The analysis phase follows the examination phase. Analysis governs processes such as data mining, statistically analysing the available data, and trying to place every occurred event (the evidence of which proves that it happened) onto the timeline to facilitate the process of picturing and "re-playing" the events of the investigated incident. It is crucial for this phase to be carried out as accurately and thoroughly as possible, since the conclusions drawn from the results of the analysis are the basis for the last step of the digital forensic investigation process model, namely the decision phase (discussed further in the text).

The presentation phase follows the analysis phase and is designed to document all the details of the investigation process and the results up to date. However, it is important to note that documentation has to be done throughout the entire forensic process. The presentation phase also involves giving an expert opinion on the results of the investigation, proving them to be valid, as well as statistically interpreting results. The forensic specialists might also recommend specific countermeasures to the investigated incident.

The decision phase is listed as the last step in the digital forensic process according to DFRWS. The model does not provide a description of the processes and techniques

involved in that phase. Nonetheless, based on the name of the phase one may conclude that it entails making the final decision about the outcome of the investigation. The results obtained from the forensic process could prove or disprove the occurence of the investigated events, as well as help determine the nature and severity of the incident. A final report on the results of the investigation is most likely to be presented in court to make the findings official.

Overall, the model developed by the DFRWS is a sound model, designed to be applicable to any kind of a digital forensic investigation due to the abstraction from any concrete technologies. However, one of the drawbacks of this model is the fact that collection and examination phases are somewhat similar, in the sense that same types of processes are assigned to both phases. That may complicate the investigation procedure, since the investigators would have to make a separate decision each time as to which parts of the process should be carried out in one phase and another, respectively. That could negatively affect the consistency of the investigation procedure, which may lead to poor results.

The following model presented by Reith *et al* [108] was inspired by the DFRWS model but is also similar to the US DOJ model [92], since it is an abstract model, independent of the technical details of the icident. It consists of the following nine steps:

- Identification
- Preparation
- Approach strategy
- Preservation
- Collection
- Examination
- Analysis
- Presentation

- Returning evidence.

The identification phase requires the investigators to identify the existing evidence and determine the type of the crime scene based on the available data. The preparation phase involves preparing the necessary tools for the investigation and search warrants, as well as overseeing the authorisation management so that the evidence is not tampered with or tainted by any unauthorised individuals.

Approach strategy speaks for itself; during this phase the investigators decide on the way they are to approach the investigation and on the strategies they are to implement during the collection and the analysis of the data, taking into account the impact on the bystanders and the technological details of the crime scene. The authors emphasize that "the goal of the strategy should be to maximize the collection of untainted evidence while minimizing impact to the victim" [108].

The preservation phase, similarly to all the models discussed previously, entails preserving and isolating all the physical and digital evidence, making sure that it is kept untouched and untainted, preserving its integrity. During the collection phase all the data is collected from the crime scene. The physical scene is recorded and all the digital evidence is duplicated according to accepted standards, using the appropriate tools and techniques.

The examination phase involves an in-depth systematic search of the collected data to identify the evidence that is related to the investigated crime, as well as identification and location of any other data that could potentially serve as evidence. The authors state that detailed documentation of the findings is essential at this point and should be carried on to the next phase, namely the analysis phase. This phase of the investigation deals with the data itself. It entails determining whether the evidence presented for analysis is valid and significant enough for conclusions to be based on it. This phase also involves reconstruction of bits of data and drawing of conclusions based on the evidence.

The presentation phase, following the analysis phase, requires the investigators to summarise and provide explanations for all the conclusions drawn from the evidence analysed in the previous phase. The authors specifically state that the documentation "should be written in a layperson's terms using abstracted terminology" [108]. However, the abstract terminology does not mean abstract explanations. On the contrary, the

authors emphasize the importance of addressing all the details of the evidence analysis.

Finally, returning evidence is the very last step of a forensic investigation process, according to Reith *et al.* It is a step that does not appear in any of the previously discussed models, and it entails ensuring that all the physical and digital property used during the course of the investigation is returned to its rightful owners, as well as deciding which part (if any) of the evidence should be removed and how it is to be done. From the structure of this model and the explanations the authors provide for each step, it is evident that the authors put a lot of effort into ensuring that most aspects of a digital forensic investigation are accounted for, and that the integrity of the evidence is preserved with all precautions.

Seeing as it is an abstract model, the model by Reith *et al* can be used in a variety of digital forensic investigations, involving different technologies and devices. It is abstract enough to be applied even to future technologies not available to us yet. Another advantage of the current model is that the forensic process is divided into nine steps, each of which is quite straightforward and easy to follow, contrary to models such as the model by Kruse and Heiser [56], where each of the steps consists of many different tasks, which could possibly lead to confusion and thus unreliable results. However, the abundance of steps in the abstract model could also be seen as a potential shortcoming. Since the model is abstract, when applied to a concrete case the investigators might need to more specifically define some of the steps of the forensic process to make them more applicable to the case at hand, e.g. by adding sub-steps or additional tasks. Seeing as it is quite a large model already, these actions might make it quite cumbersome and potentially confusing to use [108].

2.2.2 Derived Model

In the previous section various digital forensic process models available in the literature have been described and discussed. Some models offered detailed schemes, dividing the forensic process into a number of specific phases, while others provided a more abstract description of the forensic process, presenting a generalised set of steps. All the models have some advantages and drawbacks, and it is difficult to decide whether any one of them could be called “the best” or the most complete. The current study is

focused on digital forensic techniques as applied to Second Life, the online social virtual world. This makes it a very specific and unusual context, seeing as most digital forensic investigations, while focused on the digital data, still have some physical aspects to it. There are physical objects at the crime scene, e.g. a computer, a hard drive, or a mobile phone, and the investigators must work with those physical devices to collect the digital data from them. The current context, however, is purely digital; an offense is committed inside the virtual world, by a digital avatar against another digital avatar, and both the scene of the offence and all the evidence is computer-generated. Thus it is evident that the digital forensic process should be revised and adjusted to this specific context. Based on the models discussed in Section 2.2.1, an attempt will be made to derive an abstract digital forensic model which would be applicable to a digital forensic investigation of an offense committed inside a virtual world, specifically Second Life.

Seeing as each step of an abstract model encompasses two or three steps of a more detailed model, it is practical to apply a detailed model to the virtual world scenario to see which steps are not applicable in this context and can be omitted or modified, or which required steps are missing and need to be added. Let us look at the two most detailed models, namely the DFRWS model [94] and the Abstract model by Reith *et al* [108] (referred to as the Abstract model for the rest of the section).

Both start with the identification phase, during which the crime scene should be studied, the existing evidence identified, and the type of offense determined, based on the existing evidence. The DFRWS model also lists examination of any unusual events, studying of possible criminal profiles, and monitoring of the affected device for any anomalous processes or data as part of the identification phase. Looking at a virtual crime scene, we can see that most of the tasks of this phase are applicable in this case. One could study the crime scene from a screenshot or a video recording done either in-world or via screen monitoring software. The recorded crime scene could also be scanned for any unusual events. The process of looking for evidence of the offense also needs to be carried out, even though the type of evidence left in a virtual world might be different from the evidence found in a "standard" computer crime scene. The bystanders and the witnesses of the offense could be interviewed at this point, provided the offense was of a more "physical" nature which the people around the victim could see (e.g. the

victim avatar being pushed or insulted on public chat). A specific notion in this context would also be that, should any interviews be conducted in-world, the resulting data would inherently become digital evidence of the offence and would be accessible to the investigators for later analysis. The tasks of monitoring the affected device and studying of criminal profiles, included in the digital forensic process of the DFRWS model, would also require some alterations in the context of a "virtual" investigation. There would not be any affected devices *per se*, since Second Life residents do not own fully functional virtual computers or virtual CDs in-world. However, most residents own virtual items, either bought or built by themselves. Should any of those virtual items be relevant to the case at hand, the investigators could acquire them (with the owners' consent) and analyse them as digital evidence, since each virtual item contains metadata such as the item's previous owner, date of last access to the item, etc. Studying of criminal profiles would not be an easy task due to the vast amount of residents in Second Life. However, should a property of one or more avatars be present at the virtual crime scene, those avatars could be considered potential suspects, and could be located and personally interviewed. Their property could also be examined for any relevant evidence.

Two phases precede the preservation phase in the Abstract model, namely preparation and approach strategy. They are intended to prepare the investigators for the collection and preservation of the evidence data, as well as to make a decision on the strategy that is going to be followed for the rest of the investigation process. The preparation phase involves a number of preparatory steps, such as preparing the forensic tools and the relevant documentation, making a decision on the standards, policies, and procedures to be followed during the investigation, as well as guarding the crime scene so that no data is tampered with. All of these procedures are equally applicable in the context of a "virtual" investigation and in a more traditional, physical context. To be noted, however, is the fact that in the context of a "virtual" investigation the crime scene itself cannot be "guarded" *per se*, as it would be against the principle of unrestricted public areas in Second Life [61]. Thus this particular step would be excluded from the derived model. The approach strategy phase, however, is quite important in an investigation of an incident in a virtual world, for the investigators need to decide where to look for evidence and how to extract that evidence from the virtual world's system (details on

evidence gathering inside Second Life are discussed in Chapter 7).

The following phase is the preservation phase, during which the data is preserved in the state it was initially found, and duplicated to ensure integrity in a situation where the original evidence gets destroyed or tampered with. This also applies to the collection phase, which follows the preservation phase according to the Abstract model, since the collection phase in this model entails the duplication of the digital evidence data according to accepted standards. Evidently, this is a crucial phase in any digital forensic process, regardless of the nature of the evidence. In the context of a virtual world investigation, the evidence gathered from the virtual world needs to be preserved and maintained in the state it was initially found, for later use in the investigative procedures.

The collection phase in the DFRWS model is similar to the examination phase of the Abstract model. According to the DFRWS model, the collection phase consists of the collection of all the available evidence, and a rough sorting of the available data, for the sake of its reduction to evidence relevant to the current case. The latter task would also require an examination of the evidence. Another part of the collection phase in the DFRWS model is the recovery of the data that might have been lost after the offence had been committed, but before the investigation process could commence. The examination phase in the Abstract model involves the same process of sorting the available evidence according to its relevance to the current investigation, and it is specifically stated that an in-depth systematic search is necessary during the examination of the evidence [108]. Identification and location of any other potential evidence, as well as the documentation of the findings is listed as part of the examination phase. When applied to a virtual crime scene, it is evident that the search for the relevant evidence in the pool of data is necessary in this context. However, one might not acquire as much data from the virtual world's system as one would when traversing through data on a physical device, mainly because not all data of a virtual world is easily accessible and might require permission from the virtual world's owners and assistance from their personnel. The recovery of lost data is not applicable to an investigation in a virtual world, since it is a live system, i.e. everything happens in real time; thus one cannot freeze the system at any point in time to search through the sources of evidence for potential lost data. However, detailed documentation of the findings is an important task at this stage. Since the system is

live, some of the evidence might be lost if not properly documented, as the system is constantly updating.

The examination phase in the DFRWS model partially overlaps the examination phase of the Abstract model, since it repeats the process of limiting its already roughly filtered data to the evidence that is relevant to the case. The examination phase of the DFRWS model also entails extraction of any hidden and purposefully obscured data, to ensure the validity of the evidence used. Another task of the examination phase is the application of specialised techniques (such as pattern matching) to the evidence, in order to create a map of the avalable information, listing the relations and associations between different pieces of evidence. This map would then be carried over to the next phase of the digital forensic investigation and used in an in-depth analysis of the data. The Abstract model lists testing the validity of the data as part of the analysis phase, as opposed to the examination phase. In the context of a virtual crime scene, all the processes listed above are relevant. A perpetrator who committed fraud inside a virtual world might try to hide all personal information that was recorded in the system, which would have to be recovered. The available evidence needs to be refined and validated to make sure only relevant information is analysed later on. Pattern matching and other data sorting techniques are not necessarily a mandatory task, but, if applicable to the case, they could prove beneficial for simplification of evidence analysis.

Both models list analysis as the next phase in a digital forensic process. According to the Abstract model, this phase consists of reconstruction of bits of data and drawing of final conclusions from the available evidence, in addition to validating the evidence, as was mentioned above. The DFRWS model presents a much more detailed list of tasks for the analysis phase. It consists of data mining, statistical analysis of the available data, as well as attempts to picture the crime procedure by placing every occurred event onto the timeline. Since all of these tasks require investigators to work with the evidence already collected from the crime scene and possibly even duplicated to keep the original data untainted, the type of the analysed crime scene itself (i.e. physical or virtual) does not affect the investigation process at this stage. Thus it is fair to assume that all the abovementioned tasks are applicable to the evidence collected from a virtual crime scene.

The presentation phase is once again quite similar in both the Abstract and the

DFRWS models, with DFRWS model providing a more detailed list of tasks necessary to be completed during this phase. In both models the detailed documentation of the evidence analysis and drawn conclusions is listed as one of the tasks of the presentation phase. The DFRWS model also includes presentation of an expert testimony of the authenticity and validity of the data and the results, a statistical interpretation of the results, as well as presentation of a list of all the recommended countermeasures for the type of offense that had taken place. As was seen in the analysis phase, the tasks of the presentation phase do not depend on the crime scene itself, since they are based on the evidence data. Thus all of them are relevant to a digital forensic investigation process, regardless of whether the crime scene was a physical or a virtual space.

The last phase differs in the DFRWS model and the Abstract model. In the DFRWS model it is called the decision phase, and, as mentioned in Section 2.2.1, no explicit explanation is given as to which tasks are to be carried out during this phase. The author of the current study derived some conclusions based on the name that was given to the phase, but those are simply assumptions and speculations. However, the last phase of the Abstract model, namely the returning evidence phase, lists the following two tasks: returning all physical and digital property used during the investigation to its rightful owners, as well as deciding whether any part(s) of the evidence need to be removed and how it is to be done. In the context of a virtual crime scene these tasks are also applicable, since social virtual worlds such as Second Life allow their residents to own virtual content. However, should the investigators make use of evidence such as public chat logs, it is debatable whom the information content belongs to; however, the topic of information ownership is beyond the scope of this dissertation and will not be discussed any further. If any privately owned virtual content was used in the investigation, it would have to be returned to the owners (or have the investigators' access rights revoked). Any copies made during the investigation might possibly require to be destroyed, especially if the items contained private information. Overall, the question of removing evidence in the context of a "virtual" investigation is debatable, and must be addressed by the investigators in every specific case.

Finally, based on all the discussions above, the digital forensic process as applied to an offence committed in a virtual world, the author proposes a general, abstract model

consisting of the following six phases:

1. Identification
2. Collection
3. Preservation
4. Examination
5. Analysis
6. Presentation
7. Decision

The identification phase requires the investigators to study the scene of the incident and determine the type of offence that took place, based on the evidence available at the scene. If the incident was of a more "physical" nature (e.g. an avatar being pushed around, public disturbances or insults to a person via public messages which bystanders would be able to observe) it might be important to interview the avatars present at the scene of the offence. As witnesses of the offense, they might provide useful information which could be used as evidence. Another task which should be carried out during the identification phase is an examination of the scene of the incident for any unusual details, paying attention to any unusual events that might have taken place before or during the time the offense was committed. In the context of an investigation in a virtual world the "unusual" might be virtual objects with scripts attached to them, metadata that would appear unusual or simply worth investigating, items in the victims' or witnesses' posession that either have not been there before or have been altered somehow, private virtual items that have been altered or stolen, etc. The identification phase also includes studying the policies, terms, and conditions of the virtual world where the incident took place, identifying boundaries, defining strategies of collecting as much of the relevant data as possible without violating any of the aforementioned policies, and documenting the process.

The collection phase consists of collecting all the available evidence from the virtual world system, as well as from the possible interviewees. During this phase the investigators should also identify, locate, and collect any other data that could serve as evidence, as well as document all the findings up to this point. Contrary to most digital forensic process models, the current model, adapted to an investigation in a virtual world, lists the preservation phase after the collection phase. The main reason behind it is the fact that in a virtual incident the investigators work with a live system, as was mentioned earlier in the chapter, thus it is important to make sure all the evidence is extracted from the system and any other possible sources, before any work on the evidence begins. It can be argued that in a real-world investigation the forensic specialists also work with a live system, thus a virtual world investigation is no different from a real-world investigation in this regard. However, in a real-world context the physical crime scene can be enclosed and locked, rendering it inaccessible to unauthorised individuals. In a virtual world most areas are freely accessible to the public, and locking a virtual area (unless you are the owner of that specific section of virtual land) is against one of the core principles of virtual worlds, namely the freedom to travel anywhere in the boundaries of a virtual terrain [131]. The preservation phase involves keeping the evidence in its original state, as well as duplicating it so that the investigators could work with the duplicates instead of the original files, to preserve the integrity of the evidence.

The next phase is the examination phase. It involves sorting the data and reducing it to the evidence relevant to the incident (should any irrelevant data be present). When examining the evidence, the investigators should also attempt to extract any possible hidden or purposefully obscured data. The analysis phase which follows the examination phase, requires the investigators to determine the validity of the used data. After the data has been validated, various techniques for data analysis should be applied to it, e.g. data mining, pattern matching, or statistical analysis, among others. The last task for this phase is drawing conclusions from the evidence analysis. In the presentation phase the evidence analysis findings should be documented in detail. The results should be statistically interpreted, and the list of possible countermeasures for the investigated offence should be compiled at this stage. The latter step is very important, since finding the countermeasures for different offenses committed in virtual worlds might trigger some

security policy and access rights alterations in virtual world systems, making them a safer and a more enjoyable experience for all the users.

The last phase of this digital forensic process is the Decision phase. The only task that is assigned to this phase is determining which country's laws (or, perhaps, "virtual laws") are to be followed, should the offender be found and proven guilty by the evidence analysis. However, the topic of law is beyond the scope of this study and it will not be discussed further. Chapter 8 lists it as a possible topic for future research.

2.3 Types of Digital Forensics

Due to the rapid growth of the progress on the digital side of people's lives, and a vast variety of digital devices and techniques that have been invented over the years, it is evident that different devices or other sources of digital evidence would need different approaches and different forensic tools and techniques during a forensic investigation of an incident. It will also require specialists in different fields to work on each specific case. Thus, the technical aspect of digital forensic investigations is divided into a number of branches, each addressing a different type of digital devices involved. There is no standard framework created for the types of digital forensics, and in this study the author looks at the following branches: Computer Forensics, Multimedia Forensics, Network Forensics, Software Forensics, and Database Forensics. The author does not claim it to be an exhaustive list of the branches of the digital forensic science, as this is only a general overview of the field.

2.3.1 Computer Forensics

Computer forensics is the most generic branch of digital forensics. It is probably the most widely known, since all the other types mentioned here require some understanding of computer systems, as well as familiarity with terms such as "network" or "database". Computer forensics involves working with computers and other computer devices (such as portable HDDs) and extracting digital evidence from these devices. According to Fernandez *et al* [37], computer forensics "involves the investigation of computers *themselves* for evidence of criminal activity or activity that constitutes a violation of company pol-

icy". Nelson, Phillips, Enfinger & Steuart [87] state that computer forensics focuses on investigation of data collected from a computer's memory, hard disks, or other storage devices such as memory cards or CDs.

2.3.2 Multimedia Forensics

Multimedia forensics is a branch of digital forensics that focuses on multimedia data stored on a computer or any other digital device. Sometimes multimedia forensics is seen as part of computer forensics, and is not recognised as a standalone branch of digital forensics. Böhme *et al* [13] state that it is an erroneous opinion, as the two branches are not the same. Multimedia forensics is based on data captured from sensors, in image, video, or sound format [13]. Just as for any other type of digital evidence, one of the essential parts of working with multimedia evidence is that it is crucial to ensure the validity and authenticity of the multimedia data before presenting it for forensic analysis. Since the investigators working with multimedia data can only judge it on the state it was found in, not knowing what the original looked like and how it might have been tampered with, proving the integrity of the mutimedia evidence is one of the primary goals of multimedia forensics. Similarly to any other digital forensic investigations, the techniques used in multimedia forensics provide a means to validate, authenticate, and find the source of the multimedia data. Böhme *et al* [13] point out one principal difference between computer forensics and multimedia forensics. While in computer forensics the investigators work with digital evidence on a computer, or "computer objects that are created in a virtual world by computer events" [96], multimedia forensics focuses on digital evidence captured by a sensor. Contrary to the computer-generated evidence in computer forensics, the evidence in multimedia forensics holds a record of something that happened in reality, thus it cannot be recreated by machines and is linked to the outside world. Böhme *et al* also state that multimedia forensics has to be seen as empirical science. As mentioned above, the main goal of multimedia forensics is to authenticate and prove the integrity of the multimedia data. There are two main aims of multimedia forensics, namely manipulation detection and identification of source [13]. Manipulation detection involves the development of forensic tools for examination of multimedia data and detection of traces of malicious manipulation. Identification of source is a process

of finding the possible source device of the multimedia data [13]. With the ever-growing popularity of multimedia, multimedia forensics is in high demand and research is actively being done on this topic [6], [85], [98].

2.3.3 Network Forensics

Network forensics is a branch of digital forensics that works with networks of digital devices instead of the machines themselves. Stephenson [122] defines network forensics as the process of "capturing evidence passing over a computer network". According to Ranum [104] network forensics is "the capture, recording, and analysis of network events in order to discover the source of security attacks". Corey *et al* [28] provide an alternative term for network forensics, namely "reconstructive traffic analysis", and state that it consists of archiving network traffic and analysing subsets as necessary. Looking at computer networks, the network forensics investigation would normally be conducted on a local area network (LAN), a wide area network (WAN), the intranet, or the internet [122]. However, as seen from the definitions by Ranum and Corey ([104], [28]), computer networks are not the only type of networks considered by network forensics. Wireless networks such as cellphone networks (GPRS, 3G, 4G) or wireless sensor networks (WSNs) are also investigated by the network forensics specialists [83], [82]. The goal of network forensics is to analyse the network data and trace the source of the attack, in order to find the perpetrator(s) [97]. Garfinkel [41] lists two approaches to capturing of the data in network forensics, namely the "catch it as you can" approach and the "stop, look, and listen" approach. The "catch it as you can" approach implies capturing all the data packets going through a certain point in the network, and saving it to storage for future examination and analysis. This approach does not need a very fast processor and it guarantees that no packets are lost in the process of evidence collection. However, capturing *everything* requires a lot of storage space, and makes data analysis a very lengthy process due to the amounts of data to be sorted and filtered. It might also cause some privacy issues, since the captured traffic might contain private information which might be inappropriately disclosed during the course of the investigation. The "stop, look, and listen" approach implies examining all traffic going through the network but capturing only the packets relevant to the investigation. This entails some analysis to

be done "on the go" and therefore requires a faster processor. However, one of the advantages of this approach is that the computers can monitor much more information than they can capture, since memory is faster than the disk, thus with this approach busy networks can be monitored without the concern of disk space. Another advantage of this approach is the lack of any privacy concerns, since it reduces the risk of private information disclosure. The "stop, look, and listen" approach is used in a number of forensics tools such as the Network Flight Recorder [105] and SilentRunner[1].

2.3.4 Software Forensics

Software forensics is another branch of digital forensics, which is sometimes considered a part of computer forensics, even though its focus is much different than that of computer forensics. While computer forensics works with the evidence found on the storage media such as HDDs and CDs, software forensics is a science intended to identify authors of malicious computer software [118]. Gray *et al* [44] define software forensics as "authorship analysis of software source code". They also state that in the absence of source code the object code (usually created by compiling the source code) should undergo analysis or be decompiled into source code with some inevitable information loss. Software forensics can also be seen as a science combining digital forensics with forensics for handwriting and linguistical analysis [44], seeing as it involves analysing texts written in computer programming languages in order to find personal traits and styles of the authors of the code. Even though a programming language is much more structured and restricted than human language, it still allows for some degree of freedom. Some of the factors that aid authorship analysis are the author's choice of language, code formatting, comment style, or variable name choices [120]. Gray *et al* [44] list four aspects of authorship analysis which can be applied to the analysis of source code, namely author discrimination, author identification, author characterisation, and author intent determination. Author discrimination refers to deciding whether some pieces of code were written by a single author or a group of programmers. It usually involves a similarity comparison between a couple of different pieces of code, which enables the analysts to decide how

[1] http://www.accessdata.com/products/cyber-security/silent-runner

many authors wrote the code. Author identification is an aspect of authorship analysis which involves determining whether a particular author wrote a certain piece of code, by comparing it to other code examples done by the same author. The tested piece of code can also be compared to a number of different code examples by various authors in order to prove or disprove the authorship of any of these authors. The next aspect is author characterisation. The goal here is to determine some personal characteristics of the author, such as educational background and even personality, based on code written by this author. As mentioned above, choices of variable names, writing style in comments, and many other characteristics of a piece of code may disclose the personal traits of the author. The last aspect of authorship analysis applied in software analysis is author intent determination. The goal of this step is to determine whether the code was written with malicious intentions or the investigated incident was a result of an accidental error. Sometimes code that produces results harmful to one's computer or the data stored on the computer turns out to have been a result of a bug in the code or simple negligence to abide by rules of safe coding. Thus the software investigators should never discard this as a possibility and thoroughly check the code before accusing the author of intended malice.

2.3.5 Database Forensics

Database forensics is a very important branch of digital forensics, although not as extensively researched yet as some of other branches. As the name states, database forensics focuses on forensic investigations of databases. Fowler [39] defines database forensics as "the application of computer investigation and analysis techniques to gather database evidence suitable for presentation in a court of law". Database systems are much more complex than the raw data found on storage media or in device memory, but they are a rich source of evidence. One of the advantages of databases over raw data in a forensics investigation is that a database stores metadata of the data it contains, as well as offers links between individual data records via the available metadata [91]. Databases also allow for recovery of previously deleted rows and identification of the data pre- and post-transaction. Investigation of the contents of a database can also help prove or disprove a data security breach or determine the scope of a database intrusion [39].

Fruhwirt *et al* [40] state that the analysis of the structure in the database management system is a precondition for forensic analysis. Olivier [91] compares file system forensics with database forensics and applies five key aspects of file system forensics to database forensics, namely integrity, searchability, restoration (known as file carving in file system forensics), metadata extraction, and attribution, in order to flesh out a map of a forensic analysis of database systems. The former aspect concerns the integrity of the data which is brought for analysis. The investigators must take extra precautions and ensure the integrity of the data in a database, since databases offer additional possibilities for the perpetrator to conceal the evidence, such as data dictionary modification. Searchability refers to searching for relevant evidence among the large amounts of data captured for analysis. According to Olivier, "the best forensic tool [for extracting evidence] is the database itself" [91], due to the queries one can run on a database system. However, that approach raises integrity concerns, since modifications in the data dictionary, the relations between the data tables (in the case of a relational database), or column names might yield purposefully modified results instead of the real evidence contained in the database. Restoration is a process of recovering the data that was partially deleted or only partially extracted during the phase of data collection. This process is facilitated by database options such as a roll-back. Metadata extraction refers to the extraction of the metadata contained in the database for each row, e.g. unique hashcode or date. This process happens "automatically", since a piece of data is extracted from the database with all the information contained in the same row. Finally, attribution refers to determining of the authorship of the actions performed on the data in the database. If detailed logs are available, they can be used in an attempt to determine the authorship. Alternatively, the available metadata can be analysed in order to determine who was authorised to perform those actions. In both cases, it is a possibility that the perpetrator was able to modify the information in such a way as to obscure their person.

2.4 Conclusions

Digital forensics is a branch of forensic science, a field of study which attempts to answer questions most commonly related to a crime or a civil action. Digital forensics was de-

veloped to accomodate the digital evolution of our time, and to provide security against attackers making use of the available technologies. Crime committed via digital means such as a computer or a mobile device is referred to as cybercrime. Forensic investigations of cybercrime generally follow a predefined process, known as the digital forensic process, which is used to structurise the investigation in order to retain the integrity of evidence and obtain reliable and sound results. However, there is no standard digital forensic process model which would be accepted and followed universally. Various researchers have developed their own digital forensic process models, a number of which are compared in this chapter, as well as discussed with regards to their advantages and disadvantages. Applying these models to a digital forensic investigation in a virtual world, it is evident that some of the "standard" steps of a digital forensic process are not applicable to such an investigation, due to some significant differences between a tangible environment containing digital devices, and a purely computer-generated environment. Some of these differences include the absence of any physical evidence in virtual worlds, or the inability of the investigators to "freeze" the virtual world for the duration of the investigation process, due to it being a live and constantly updating system. Adhering to the specifics of a digital forensic investigation in a virtual world, the author derived a specialised digital forensic process model, based on the previously discussed models, which consists of six steps, namely Identification, Collection, Preservation, Examination, Analysis, Presentation, and Decision. Contrary to the previously discussed models, all the tasks allocated to the phases in the author's model are applicable to an investigation conducted inside a virtual world. The chapter is concluded with an overview and a brief discussion of some of the existing branches of digital forensics, namely Computer Forensics, Multimedia Forensics, Network Forensics, Software Forensics, and Database Forensics.

The following chapter covers the topic of virtual worlds.

Chapter 3

Virtual Worlds

In the past couple of decades, online social spaces have become very popular, and are being used by millions of people all over the world. Although virtual worlds *per se* have existed ever since 1978 as Multi-User Dungeons, or MUDs [111], online 3D virtual worlds such as ActiveWorlds and Second Life only came onto the digital scene during the last twenty years. This chapter provides an overview of Virtual Worlds (VWs). Section 3.1 derives a definition of the term "virtual world", based on a number of definitions available in the literature. Section 3.2 discusses characteristics common to all types of online virtual worlds. Section 3.3 addresses some security concerns arising with regards to virtual worlds. Section 3.4 concludes the chapter.

3.1 Defining "Virtual Worlds"

Before any discussion on virtual worlds can be commenced, the term "virtual world" must be clearly defined and agreed upon. There is no universal definition of this term in the literature, and academics use various definitions in their studies. This section presents an overview and a discussion of a number of different definitions of virtual worlds, and offers the author's own definition, applicable to the current study, derived from the definitions previously discussed.

According to Shroeder [116], virtual worlds are persistent environments populated by people and focused on social interaction. Shroeder also remarks that virtual worlds allow

users to "experience others as being there with them". Koster [54] states that "a virtual world is a spatially based depiction of a persistent virtual environment, which can be experienced by numerous participants at once, who are represented within the space by avatars". Castronova [21] defines virtual worlds as "crafted places inside computers that are designed to accommodate large numbers of people", while Bell [11] provides a more detailed and precise definition which states that a virtual world is "a synchronous, persistent network of people, represented as avatars, facilitated by networked computers". Having mentioned various aspects of the virtual worlds, none of the above definitions mention the aspect of immersion. According to Nechvatal [86] and Brown and Cairns [16], immersion is a state of mind where the person's consciousness of the surroundings is diminished and they feel as if they are present in an environment other than their own (often artificial). A familiar example of immersion could be getting lost in the narrative of a novel or feeling part of a film you are watching on television. It is a very important aspect of any social virtual world such as Second Life, as it makes the users feel as if they are really a part of the artificial world. The term "virtual world" is sometimes considered a synonym for the term "virtual reality", but that assumption is not always correct. Let us consider and compare some definitions of "virtual reality" and "virtual world" available in the literature. Schroeder [116] defines virtual reality as:

> "a computer generated display that allows or compels the user (or users) to have a sense of being present in an environment other than the one they are actually in, and to interact with that environment."

Virtual reality is also given a definition by Dunnet *et al* [35]:

> "Virtual reality applications, often called artificial realities or virtual worlds, are entirely computer generated environments. These environments attempt to model the behaviour and effects of a real world by employing realistic computer-generated images and animation techniques, for interaction with a human operator, or operators. Interaction devices allow 3D manipulation of the environment, and feedback where appropriate."

Brooks [15] states that "a virtual reality experience is any in which the user is effectively immersed in a responsive virtual world." In all the definitions virtual reality is described

as immersive and responsive to a user (or users), but none of the authors mention the interaction between the users in such an environment, which is an essential characteristic of any virtual world. Schroeder [116] explains the difference between the two terms as follows: "The difference between virtual realities [...] as against virtual worlds is that the latter term has been applied to persistent online social spaces".

Combining the definition given by Bell [11] and the concept of immersion, a virtual world is defined in this study as an immersive environment which consists of a synchronous, persistent network of people, represented as avatars, facilitated by networked computers.

3.2 Characteristics of Virtual Worlds

Many virtual worlds have been created up to date. Most well-known among them seem to be the online gaming worlds, such as World of Warcraft or EverQuest[1], as well as virtual worlds created mainly for social interaction, such as Second Life[2] or ActiveWorlds[3]. Other virtual worlds have been created for educational purposes, e.g. WhyVille[4], made for children and teens, aged 10-16, in order to get "hands-on" experience with science projects.

Made for different purposes and in different styles, all these online virtual spaces are virtual worlds, with certain characteristics common to all of them. In the following section a number of those characteristics is listed and discussed with regards to the virtual worlds mentioned above.

3.2.1 Environment type

The environment type is one of the most important things in a virtual world, since it is something that conveys the style and overall feel of the virtual world. It is something

[1] http://everquest.station.sony.com/

[2] http://secondlife.com/

[3] http://activeworlds.com/

[4] http://www.whyville.net/

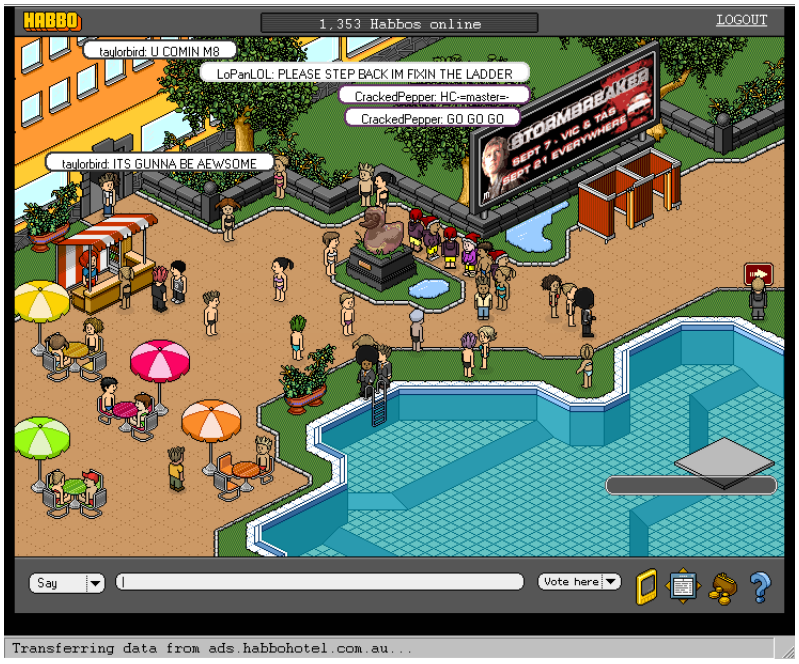

Figure 3.1: Habbo Hotel 2D Interface.

that first meets the user's eye, and is a crucial factor in the user's decision on whether the virtual world suits their needs or not.

Online virtual environments could be categorised into 2D and 3D environments. 2D environments are not as immersive as 3D environments, seeing as the world around an avatar is not made to look realistic. It is usually done as a top-view, cartoon-style or pixel-art still background, with avatars moving around it but not *in* it, since the third dimension - depth - is missing (see Figure 3.1). Avatars are usually animated in such a way that they can move around the area and interact with the objects (e.g. sit on a couch), and the surrounding area is usually divided into blocks (e.g. "lobby" and "guest rooms" in Habbo Hotel). But the main focus of such 2D environments is usually on the social aspects of it. An in-built public chat is always available to the users who are in the same block, and private messaging facilities are available regardless of either the sender's or the recipient's location. Section 3.2.3 covers the types of communication in virtual worlds in more detail. 3D environments provide more realistic virtual worlds, with an avatar represented as a 3D model of a custom character (the character choice varies from world to world) moving around in a life-like environment. An avatar is usually

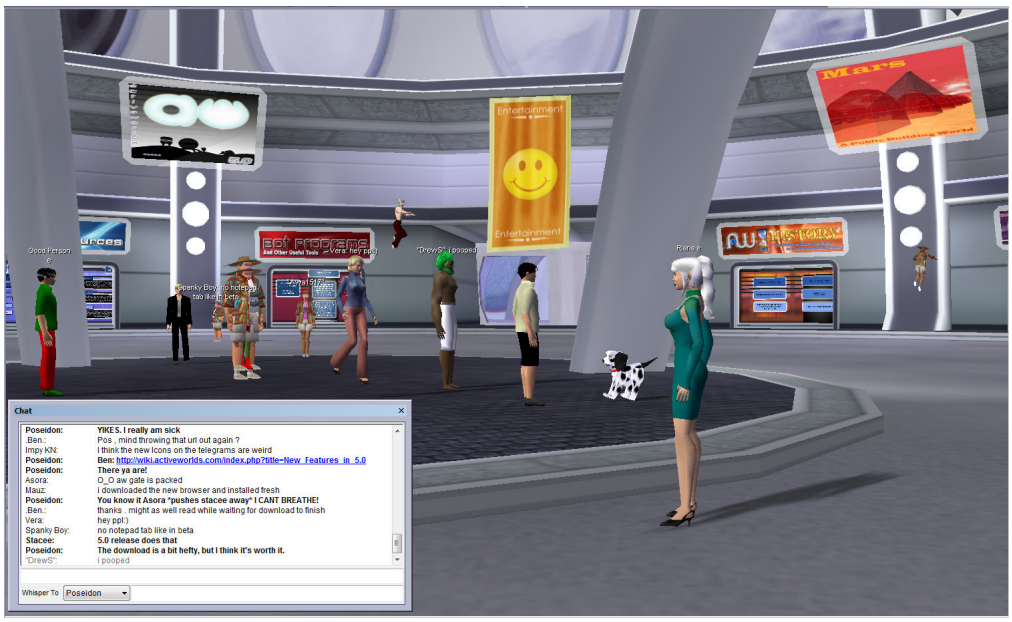

Figure 3.2: ActiveWorlds 3D Interface.

able to interact with most objects in the surrounding areas, e.g. read notice boards, sit on benches, touch items on the ground. An avatar can also usually enter buildings (provided they are not constrained by private property boundaries), and interact with the objects inside them. Section 3.2.4 provides more information on interactivity in 3D virtual worlds. 3D environments are less obviously divided into areas, since the whole terrain of an area is free for avatars to enter and interact with. Just like in real life, people can group in any part of the room or an outside area and have a chat.

3D environments are becoming more and more popular among the developers of the virtual worlds for a number of reasons. Firstly, it provides a much bigger sense of presence in the environment than a 2D world does, since the user can usually rotate 360° in the surrounding environment, as they would in real life (see Figure 3.2) [100]. The user can also switch between first-person and third-person view. In first-person view one cannot see their own avatar, but, like with oneself in real life, only sees their hands and feet and the surrounding area. That would also increase the user's field of vision, which, according to Prothero and Hoffmann [100], increases their sense of presence. Another reason 3D environments are preferred by the developers of the virtual

worlds is the visual clarity and quality they provide, referred to by Haugtvedt *et al* [46] as "vividness". Their study was focused on the way virtual aspects affect consumer behaviour, and they conclude that 3D environments stimulate sensory experiences of the users thus making them more enthusiastic about and involved with what they see on the computer screen. For the current study it is safe to assume that such behaviour applies not only to consumer products, but also to the general experience of a user in a virtual world. For example, having a "real" garden to take a walk in will surely provide a more satisfactory experience than having a static picture of a garden in the background with one's avatar moving around it.

Having different types of environments available in various virtual worlds, it is essential to note that there is no "perfect" environment, since different environments are suitable for different purposes; environments that work well for social virtual worlds might not work as well for the educational or gaming-oriented environments, and vice versa. When assessing the environment in a virtual world, the first thing to look at is the main focus and purpose of the virtual world. Even though 3D evironments are generally ranked higher than 2D environments, at times an overly complicated 3D environment can confuse the user and thus become counter-productive [26].

3.2.2 Persistence and Shared Space

Persistence refers to the aspect of virtual world environments which probably contributes the most to the feeling of a virtual world being "real", and not just a computer-generated space. Persistence is the continued existence of the virtual world regardless of whether a user is logged in or not. Ongoing processes, such as changes in the displayed weather or time of day, continue even when there are no users logged in to see it [20]. This is a very important characteristic of online virtual worlds, especially those with an economy of their own, such as Second Life. Advertising one's product(s) around the virtual areas would be worthless had those advertisements not been available for everyone to see when their owner was offline. If a user owns property/land in a virtual world or is involved in a lengthy process (e.g. building), it is essential that they are able to log off and be sure that the their objects' ownership and any of their unfinished processes remain intact.

Another fundamental characteristic of any virtual world is the availability of a variety

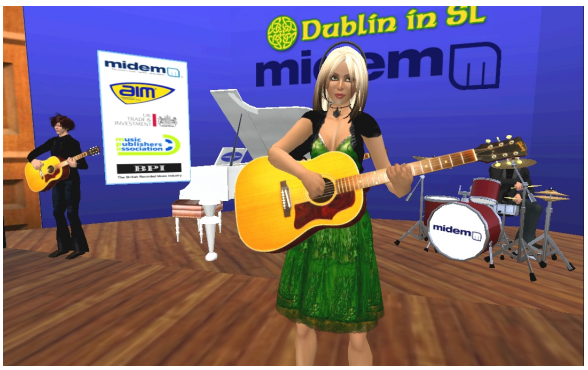

Figure 3.3: Live performance in Second Life.[5]

of virtual areas shared among a big number of concurrently logged-in users [21], [54]. From the start virtual worlds were mostly meant for socialising and gaming, thus shared space was one of the first features in such online systems. For virtual worlds focused on specific tasks and themes (e.g. Whyville, made for children's education) network traffic might not be a problem, and providing high-end servers with a big capacity would not be a necessity, since there are not as many registered users as there are in bigger-scale virtual worlds such as Second Life or World of Warcraft. Nonetheless, every virtual world should have the capacity to hold a significant number of concurrent connections. More popular virtual worlds such as ActiveWorlds offer concurrent object building, live public chats, live in-world concerts, and more. Naturally, such advanced tasks require high-end servers and a fast internet connection, provided by the owners of such massively multi-user virtual worlds.

3.2.3 Community

Every virtual world gathers a number of people together in the same environment. That in itself makes them a part of an online community, even if if there is no interaction between them. However, seeing as social interaction is a major part of the notion of a virtual world, communicating with the people around oneself is encouraged and aided in various ways. Chat functionality in a virtual world is usually the first thing that

[5]Midem International Music Festival Simulcast Into Second Life by Sitearm Madonna, http://www.fengshuichat.com/sitearm/midem_2008_images.htm

one notices when looking at the user interface, and by default the messages one sends through are public, i.e. visible to everyone in the area around the user. This encourages communication and facilitates making acquaintances with stangers, since after greeting everyone in the "room" there is bound to be at least one greeting in response, which might eventually lead to a conversation. On a more advanced level of communication there are a lot of choices available to the users. In Second Life open communities are available to general public, created for people who share certain interests, e.g. religious communities such as Thai Buddhist Temple: Golden Green, or fantasy communities like Wizard's Alley & Hogwarts: Sunset Harbor [129]. One can find communities for role-playing, sight-seeing, and even psychological rehabilitation. Creation of such communities is encouraged, as any two users, regardless of membership plan type (free or premium), can form a group, and later expand that group to as many members as they wish, since there are no restrictions on group size [129]. The creator of the group is given a choice as to the way their group is run, e.g. they can choose to run it as a democracy, or become the sole leader and dictator. Communities are also supported by the system itself, as group members are given special privileges with regards to each other. For example, if they purchase land as a group they enjoy the benefits and special offers available to group land owners [129].

Community building is a part of any virtual world, regardless of the world's focus and goals, since social interaction is what makes virtual worlds different from other virtual environments (see Section 3.1). Joining a virtual world, especially a densely populated one such as Second Life, is a good way to make friends online, meet people that share one's interests, spend time doing fun activities with other people, and develop one's communication skills.

3.2.4 Interactivity

Interactivity plays a big role in virtual worlds. It is one of the features that makes virtual worlds very different from other online spaces such as websites or blogs. On a website one can only see and traverse through the information already put in place by the website developers, but one cannot usually add anything new to the existing product. It may be argued that websites such as Facebook provide dynamic interaction, seeing as one can

post status updates and comments in real time. However, Facebook and other similar online services only allow the users to interact with each other by the means of the service; the service itself does not contain tangible objects a user can examine, lift up, or wear. In a virtual world, not only do users see what is around them and use it to their needs, but they can also create content and alter the appearance of the areas around them. They are given freedom to interact with everything around them; users can "sit" on any object (provided it is not locked by the owner of the object), touch non-player characters (NPCs), e.g. pat computer-generated animals, play with balls, or even sing on stage. They are also given the ability to "touch" objects. Depending on the type of the object the touch action would yield different results; "touching" a microphone on stage would trigger a menu where the user could state which song he/she would be singing, and "touching" a fellow dancer on the dance floor would trigger a menu with types of dance animations available. Building new content also plays a big role in the world of Second Life. New users might just play with building tools, creating simple shapes and objects, but the extensive building tools built into the Second Life interface are very powerful. Those who are willing to take time to study them and practice can learn to build beautiful and complicated objects, varied from an ornamented chair to a house or even an estate. Those who regard Second Life as something more serious than simply a way to spend free time, can build the house of their dreams, or even make money from their building skills. Having created a useful or simply good-looking objects, one can sell them at the Second Life marketplace and earn Linden Dollars. Group building is also available in Second Life. As a group, users can create more complicated objects and make use of each other's strengths in different areas of building. However, collaborative building requires the users to grant each other modify rights to different objects in the project being built, and later group ownership [129].

Extensive interactivity might raise some security concerns regarding interaction with owned content. Those concerns cannot be called groundless, for it is possible to find ways to tamper with someone else's content, although it will take time and effort. Second Life's system offers owned content protection by letting the owner set any of his/her object's modification property to "no modify" [59]. It means that no one except the owner himself is allowed to edit the object and alter its appearance, shape, or placement. To

(a) World of Warcraft

(b) Second Life[6]

(c) Whyville

Figure 3.4: Avatars in different virtual worlds.

prevent anyone from deleting an object the owner can set another of its properties to "no delete". However, there are public objects in areas of Second Life dedicated to building, for novice users to practice on.

3.2.5 User Avatars

One of the first things a user is asked to do upon registering in a virtual world is creating an avatar. An avatar is a character which other users are able to see and communicate with, and which is controlled by the owner to move around the virtual areas and interact with virtual objects. According to Meadows [76] an avatar is "an interactive, social representation of a user". The author states that an avatar is an interactive entity because it is used to interact with the virtual world and fellow users, and a social entity because without a social setting where people need a way to represent themselves on screen, an avatar is redundant. Neustaedter and Fedorovskaya [88] talk about the avatar as a synthetic body used to represent user's virtual identity. An avatar is always customisable to the user's needs, but the range of customisable options varies from world to world. In World of Warcraft users create a full-body character for themselves, and are able to choose between ten different races, while in Whyville users are represented on screen as floating faces, so the face is the part of the avatar that the newbies aim to

[6] "Female Human Avatar" by HyacintheLuynes - Own work. Licensed under Creative Commons Attribution-Share Alike 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Female_Human_Avatar.jpg #mediaviewer/File:Female_Human_Avatar.jpg

customise and make their own [50].

In Second Life one of the things a user is first judged on is their avatar appearance, so the customisation options for one's avatar are close to endless. One is able to customise almost every part of one's avatar, including facial features such as nose length or eye size (in the case of a humanoid avatar). New users enter Second Life with one of the default avatars (all of them humans), and almost all of them would change the default appearance at some point. Neustaedter and Fedorovskaya [88] noted an interesting social phenomenon regarding the default avatars in Second Life: most Second Life residents who had spent some time in-world assume the users with default avatars are newly registered residents who are typically still lost in the vast virtual world and are not sure of how to act and where to go. These experienced users usually fall into two categories: those who avoid residents with default avatars for the fear of having to become their mentors in the SL world, and those who are, on the contrary, inclined to make contact with such residents because they enjoy the teaching process. This shows how much social pressure is placed on the new users in Second Life, and just how important one's avatar is from the very first moments inside the virtual world.

That brings us back to the notion of a virtual identity and the fact that the user's avatar is a representation of their identity in a virtual world. Both definitions of the notion of an avatar given above ([76], [88]) imply that avatar creation involves the user's personality and the identity they want to portray in the virtual world. An identity is one's mental model of oneself [43], and it "emerges in the process of interaction" [34], i.e. through interactions with other people and presenting oneself to the social community. Having different types of online identities causes people to perceive virtual worlds very differently. Some people use virtual worlds simply to meet new people and engage in some interesting online activities. They regard it more as a game than anything else. Others take virtual worlds much more seriously, regarding their participation in an online world as a continuation of their real life. In Second Life some people start new businesses, get employed and earn their real-life income through online activities. Undoubtedly, people's regard of the value of their virtual presence affects the way they represent themselves to other people in the virtual world, and thus affects the appearance of their avatar.

Neustaedter and Fedorovskaya [88] list four different types of Second Life users,

namely *Realistics*, *Ideals*, *Fantasies*, and *Roleplayers*. Realistics regard their virtual world activities as a continuation of their real life. These people take their "virtual lives" seriously and might involve themselves in something "real", such as online money-making (e.g. starting a business inside Second Life). Their online identity is constant, and is the same as their real-world identity. Even their avatars tend to resemble their real-world appearance as much as possible. The Ideals regard their virtual identity as an idealised version of their real-life indentity. They register in virtual worlds to create virtual identities that resemble the way they would like to see themselves. Their online identities are mostly the same as their real-life identities, with corrections of the aspects they do not like about themselves. The same applies to the Ideals' avatars: while retaining their real-life appearance, the avatar is given features they lack or want to have in real life. Contrary to the Ideals and the Realistics, the Fantasies and the Roleplayers take on a different role as virtual identities. While Realistics and Ideals tend to stick with one identity in both virtual and real worlds, Fantasies and Roleplayers take on a completely different identity when entering a virtual world. Fantasies clearly separate virtual and real lives, and usually create avatars that look different from their real-life appearance. Nonetheless, Fantasies are continuous in their virtual identity, and are able to establish and maintain long-term relationships. On the contrary, Roleplayers do not maintain any continuity in their virtual identity, for they come into a virtual world to experience things they are not able to experience in real life. They try out different ideas, often changing their avatar, as well as the virtual identity, for each one. Some Roleplayers have alternative avatars for different fantasy virtual lives they lead, and some have one primary virtual identity, while taking on secondary identities to try out different things. Similarly to the Fantasies, Roleplayers create avatars that do not resemble their real-life selves. Nonetheless, in every role they play online, Roleplayers strive to achieve as realistic a gameplay as possible, sharing that trait with the Realistics.

As we can see, user avatars play an important role in the users' perception and experience of the virtual world they enter. Since a virtual world is always a social space, whether it is a structured virtual world focused on a specific task such as gaming (e.g. World of Warcraft) or an unstructured online space such as Second Life, the user is always given a choice of the avatar they use and is given the means to change the avatar

at their convenience.

3.3 Virtual Worlds and Security

The fact that virtual world communities have grown so popular and have become so big, makes them an easy tool for people with malicious intentions. One may encounter rudeness, harassment, and other offensive behaviour in online social spaces. Being examples of 3D Internet [129], they allow for a bigger variety of offences to take place than other online spaces such as forums or chat rooms, where offensive behaviour is limited to text (insults and profanities) and indirect communication (e.g. spam). Section 3.2.4 briefly touched on one of the security concerns related to the owned content in Second Life, but that is not the only concern with regards to security in virtual worldss. As was mentioned in Section 3.2.5, the avatars you see inside the virtual world do not always resemble their owners' real life identities. While that does not necesarily imply that the users have malicious intentions towards the people around them, some people do use their avatars as a means to purposefully hide their real identity, considering that "on the Internet, nobody knows you're a dog" [121]. That could create a feeling of permissiveness which could lead to offensive behaviour and might even result in crime perpetration [48]. One may encounter racism, discrimination, insults, as well as other offenses such as fraud or money laundering, since in-game currency can be exchanged for real-world currency in virtual worlds such as Second Life. One can find many other examples of civil and criminal offenses within online social worlds, which proves the need for some legal actions to be taken against the perpetrators. People disrupting other users' experience of the virtual world (also called "griefers". More about griefing in Chapter 5), or spammers can simply be banned from accessing the virtual world. However, if a more substantial offenses are committed, such as child pornography distribution or fraud, a digital forensic investigation should take place, in order to find and prosecute the offender. The question regarding which country's laws are to be followed should the perpetrator be found (seeing as a virtual world could be seen as "no man's land") is beyond the scope of the current research, and is considered a possible topic for future research.

3.4 Conclusions

The phenomenon of virtual vorlds is one of the core notions this dissertation is based upon; thus it is important to address the topic in more detail. This chapter discussed and compared various definitions of the term "virtual world" available in the literature, as well as explored the ways the term is related to similar terms, such as "virtual environment" and "virtual reality". Terms "virtual reality" and "virtual world" are sometimes used interchangeably; however, that is not entirely correct. "Virtual world" is a specific type of virtual environment, focused on social interaction between its users, whereas "virtual reality" is a more broad term which does not imply any specific characteristics apart from the fact that it is a computer-generated evironment. The chapter also discussed a number of characteristics common to different types of virtual worlds, namely GUI/environment types, persistence, shared space, community building, interactivity, and the presence of custom user avatars. Finally, the chapter briefly addressed the security concerns that arise with regards to the great popularity of online virtual worlds. It is evident that, being a social environment, any online virtual world is affected by the human factor, thus opening a possibility for people with malicious intentions to misuse the environment to their advantage, be it money gain, harassment, or simple disturbance of other users' experience of the virtual world. The author sees the topic of security and offence in virtual worlds as very important, requiring more attention from the research community than it currently attracts.

The following chapter presents an overview of Second Life, the social virtual world this dissertation is mostly focused on, and discusses the factors that make it stand out among other onine virtual worlds.

Chapter 4

Second Life

Second Life (SL) is an online virtual community populated by millions of people from various countries and cultural backgrounds. It is an immersive environment which is made up of various standalone terrains, also called "islands", some modelled on real life and some being implementations of imaginary locations and sceneries. All these inner "islands" offer users freedom similar to the real world. People can see each other and interact with each other via verbal as well as non-verbal communication, touch, pick up, and make use of objects, take photos and film videos, attend live concerts and participate in sporting events, as well as engage in various other activities. Some might consider Second Life simply a game, but others take it as seriously as an alternative life with endless opportunities not available to them in real life. Over the years Second Life has also developed its own independent economy using virtual currency Linden Dollars (L$) which could be purchased using real-world currencies, as well as exchanged into real currency. It becomes prominent that Second Life has grown to make considerable impact on the lives of those members of the community who take their virtual identities seriously.

This chapter presents an overview of the world of Second Life, briefly explaining its history, and focusing on four of its aspects, namely: Second Life as a game, as a social platform, as an economy, as well as an alternative life. Each aspect is given an overview of and discussed. The chapter is concluded with an introduction to possible offensive activity in the Second Life environment. This chapter serves as an introduction

to the environment which the following chapters, as well as the author's experiment (Chapter 6), are based on.

4.1 History of Second Life

Linden Lab was founded by Philip Rosedale (a.k.a. Philip Linden) in 1999. His initial idea was to create a vast digital space which the user would be able to navigate freely [73] [126]. Up until 2001 there was no concrete direction to the development of Linden Lab. 2001 brought in an idea of using the created digital space, spread almost seamlessly over multiple servers, for a hardware-research company focused on haptic technology. The users would be able to access virtual environments, real-time telepresence devices and teleoperation devices, as well as work with them. This called for the creation of the virtual space where people would be able to create items in real-time and test them. A prototype called "the Rig" was created to bring Rosedale's idea to life [126]. The new virtual world was called Linden World. At that stage functionality such as flying and building was incorporated into the Linden World. The world even had weather, to make it look more realistic and immersive. The avatars were made out of primitives, and were called "Primitars". One could shoot and throw grenades onto the terrain and the surrounding objects. The objects exploded into tiny pieces when hit by a grenade, and the terrain changed its shape. In fact, the only way to change the shape of the terrain was to throw a bunch of grenades onto it. The early Linden World also had a primitive eco system of snakes and birds; snakes ate the birds, thus getting bigger and spawning smaller snakes, and the birds fed on rocks. The users could control the population by the use of their guns. Overall, Linden World of 2001 looked like a primitive shooter game.

For a while the Linden World project struggled to acquire any funds, as the idea of haptic technology development did not appeal to any sponsors. Later Mitch Kapor decided to give Philip Rosedale a chance and invested in the project, and a couple of other investors followed Kapor's example. In a meeting with the investors where Philip Rosedale and Cory Ondrejka presented the virtual world, the investors' attention was captured by the Linden World itself rather than the idea of haptic technology development in it [126]. Linden Lab offered collaborative seamless real-time content creation,

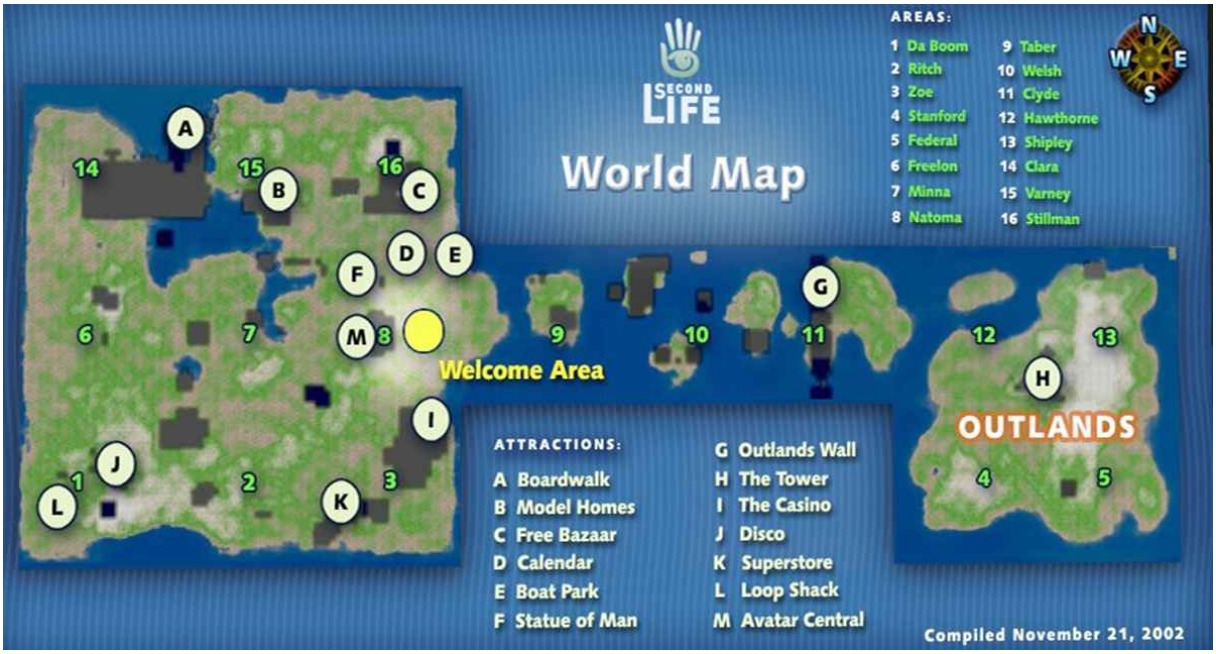

Figure 4.1: Second Life World Map (2002)

which was something unheard-of before and had much potential.

From this point on Linden World began to be developed as a game which multiple users would be able to access at the same time, and which would allow for user interaction and real-time content creation. In March 2002 Linden World was renamed into "Second Life", and opened its doors to the first Resident: Steller Sunshine [73]. In November 2002 the final beta-testing was finished and Second Life was officially open to the public. The world consisted of 16 regions, the first being called "Da Boom" [73], and the rest carrying names of various streets in San Francisco, since Linden Lab was founded on the Linden street in San Francisco (see Figure 4.1).

At first Second Life suffered from the "tragedy of the commons", i.e. from over-utilization of resources by the residents [24], which brought the necessity of establishing a basic economic system. That is when the Linden Dollar (L$) was first introduced [126]. According to the initial system of taxes, before building something, the user had to pay a weekly fee to the Linden Labs. The amount one had to pay depended on the amount of primitives created in-world. A more complex system of taxes was introduced later. Shortly after the introduction of the rudimentary economic system some Second Life

residents started attempting to evade taxes. An uprising against the taxes took place in a section of the Second Life world called Americana [8]. In October 2003 Second Life 1.1 was launched. The terms of use contained certain measures to oppose and suppress tax evasion, thus preventing riots similar to Americana in the future. As we can see, illicit activity in Second Life began as soon as money was introduced to the system, making illegal ways of financial gain accessible. Thus the strategy of offence prevention had been a relevant topic for quite some time. The new release also brought in many improvements on the technical side of the virtual world, such as defined textures and animated hair, which improved the appearance of Second Life to a great extent. Up to version 1.5 the world of Second Life had been undergoing visual improvements and bug fixes, letting the users enjoy a virtual world which was getting closer and closer to representing real life. The year 2005 brought in such additions as Teen Second Life, the separate virtual world for teens, as well as free teleportation between the regions inside Second Life [73]. Free basic accounts received a weekly L$ stipend. Lindex Exchange, which allowed the exchange Linden Dollars and US Dollars and vice versa, was also introduced in 2005. There were major outbursts of public disturbances inside the virtual world, which sometimes caused the whole Second Life system to collapse and stay disabled for days, but with the introduction on more robust rules applying to newly registering residents, such incidents became much less frequent and less destructive.

In 2006, a Second Life resident Anshe Chung was featured on the cover of the U.S. magazine BusinessWorld as the person who had become a millionaire due to business in Second Life. This caused a “gold rush”, with hundreds of new users registering in Second Life over a short period of time, to make what they considered “easy money”. It also caused Linden Labs to announce that free basic accounts would no longer receive weekly stipends, due to sheer numbers of newcomers [126]. 2007 brought a major change in the structure of Second Life. Linden Lab announced the deprecation of all gambling activity in the virtual world, which was quite a blow to the managers of the gambling sites because they were quite popular among the residents. In the same year the first official Second Life Viewer was launched [126].

The following years, up until today, the world of Second Life underwent significant improvement in appearance (Figure 2), as well as on the technical side. Various ad-

ditional functionality was implemented, the users were given more freedom in content creation (e.g. adding scripts to ones objects), and the economy of the world grew more complex and more functional.

As seen from the history of Second Life, the more complex the world grew, the more serious issues needed to be attended to and resolved. If "The Rig" started out as a simple game, Second Life required law enforcement to limit offensive behaviour and misuse of the system, as well as financial strategies to regulate Linden Dollar exchange and usage. The following sections address the different aspects of Second Life, namely Second Life as a game, as an economy, as a social network, and as an alternative life.

4.2 Second Life as a Game

When the term "online virtual world" is used, the first thing that comes to mind is an online environment such as World of Warcraft or Everquest: a Massively Multiplayer Online Role-Playing Game (MMORPG) where people from all over the world create characters, develop their skills, fight monsters and go on quests for treasure and gold. World of Warcraft (WoW) and many other similar online games are set up in an environment where fantasy creatures such as dwarves, elves, and dragons participate in quests and work together to earn awards and experience points, which, in turn, help the characters gain levels and with it new powers and possibilities [103]. The world of WoW has a built-in database of available characters, a pre-set storyline and quests, as well as a limited amount of objects one can buy, pick up, or win. The players are required to gain levels in order to get access to more items and progress in the game [7]. Based on these characteristics one can clearly see that World of Warcraft and similar online games belong to the category of structured MMORPGs where players have specific goals to be met in order to develop their character and obtain more powerful items [103]. In contrast, Second Life, though also dependent on character creation and development, is an example of a more complex online virtual world, and can be categorised as an unstructured MMORPG. The users are able to create any character they desire, from human to a walking tree, since the character creation is based on basic shapes which are modified by the user, instead of a built-in database of pre-set characters. The gameplay

does not follow any set storyline. The world of Second Life imitates real life, thus an avatar can travel through various inner "islands" visiting virtual countries, cafeterias, dancing floors, and various other places of interest with complete freedom. The players also have freedom with regards to virtual items; the environment mainly provides virtual landscapes and a basic set of islands (also called "sims"), while the rest of the development is done by the players themselves. The development and improvement of one's avatar in Second Life is at one's discretion; its role in the virtual world has more of a social nature (as discussed in Chapter 3), as compared to MMORPGs, since the system of levels is absent in Second Life, so the players are not dependent on level-gaining to progress in the gameplay and acquire items. Overall, characters in Second Life do not have any specific game-related skills (such as agility or strength), thus "developing" a character takes on a different meaning. It usually entails settling in the Second Life world: buying or building a house, finding favourite entertainment areas, making virtual acquaintances, and maybe even finding work. The only places in Second Life where standard online gaming principles (such as health, strength, or quests) are applicable are gaming sims, built specifically for Second Life users to participate in RPGs and other kinds of online games. One can take damage, use weapons, and even die in such gaming worlds, although dying does not disturb the gameplay: the avatar is just teleported to the location set by the user as "home" [69].

Overall, one of the main reasons millions of people join online gaming communities is not only to participate in the games, but also to take part in social interactions with the fellow players. Thus, even when seen as a gaming platform, one of the greatest appeals of the Second Life world is the vast space and freedom it offers for social communication with other users. The next section will discuss social aspects of Second Life and what it offers its users as a social platform.

4.3 Second Life as a Social Network

Social aspects play a huge role in the world of Second Life. Whether people join the Second Life community to play games, run a business, or build themselves a house, there is always desire to interact with fellow Second Life users [57]. People often register in the

virtual world to meet new people [78]. Having freedom to visit a large number of sims with themes varying from Renaissance towns or virtual Paris to Halloween and Tolkiens Middle-Earth, the residents of the Second Life world are presented with opportunities to meet people who share the same interests and to feel accepted by other people, as well as be a part of a large community. Second Life is also used as a means of interaction with one's existing friends. The virtual world strives to make communication as realistic as possible, and sometimes people might prefer chatting to their friends inside Second Life than making use of the faceless communication via IM and telephone lines. Skype offers video call functionality for the users to see the people they talk to; however, it does not allow them to take walks or participate in events together, while Second Life offers these opportunities to its users.

The avatars of the people engaged in a conversation might not represent their real-life appearance at all (as was discussed in Chapter 3), but this does not pose any problems when the communication takes place between two people who know each other in real life or for a long time virtually. However, as mentioned in Section 3.2.5 of Chapter 3, this fact pose a potential threat when meeting new people inside Second Life, seeing as the person behind an avatar might not be the person he/she acts as, and this can be used for malicious purposes such as establishing false trust and grooming.

Social events in Second Life make it a unique social platform different from other online social spaces such as Facebook or Twitter. Second Life residents are able to engage in virtual activities such as clubbing, sports, and live concerts, visit art galleries, and even attend virtual lectures. The availability of such activities to the users makes Second Life experience very appealing, especially to disabled people who cannot participate in some of these activities due to their physical condition. As was discussed in Section 3.2.3 of Chapter 3, community building is one of the focus areas of the world of Second Life, and the system offers countless opportunities for communication, group activities, and collaborations.

4.4 Second Life as an Economy

Having undeniable appeal as an online game and a social network, Second Life is nonetheless more than "just a game" or another version of Facebook, due to its considerable impact on the lives of the users who take their Second Life experience seriously. The residents of Second Life are able to not only spend their money to buy various items but also earn money through selling their in-world creations or working for in-world employers. They can also purchase, create, and sell land, thus expanding the money-making opportunities. Due to the fact that virtual financial profit gains one profit in real life, there is a possibility that offenses such as fraud or blackmail may be targeted at owners of considerable sums of Linden Dollars.

All the abovementioned financial opportunities represent the basic four factors of production of an economic system, namely land, labour, capital, and entrepreneurship [24]. It is necessary to look at each of these factors in detail to see how the laws and principles of a real-world economy apply to the world of Second Life.

In real life, land consists of sources of nature, original and irreplaceable. Therefore a real economy always faces a problem of choice: utilising a piece of land for building or for growing crops; using the land as a source of building material or making it a road which would aid in transportation of building materials. Regardless of the choices, the result is often final, i.e. the land becomes unusable for anything else [24]. Looking at the land capital available to the users of Second Life, one can clearly see that the "virtual" aspect of the land plays a huge role in the difference between the land production factor in real life and in Second Life. A piece of land in Second Life can be cleared out completely at any time, provided the user is the owner of the land or the land's owner unlocked the edit mode for the land to other users. When cleared, the land can be used for anything; the user can build a house or plan out a garden, open a shop or even sell the land to other users as is. The main difference between virtual land and real land is the fact that using virtual land does not affect the land terrain in any way, thus making it re-usable and suitable for any kind of purpose. The problem of choice never arises in Second Life. The only choice one has to make is deciding what is to be built on the piece of land, and whether to take down the buildings already present on the land (provided the land had been sold together with everything on it).

Human labour as a production factor does not differ as much in real life as compared to its Second Life counterpart. The work of human beings is an essential part of any economy, since it is humans who make any economic system functional. In the real world the work of humans provides goods and services to the community, and gets financially rewarded by the government or the employers.[12]. The human labour in Second Life works in a similar way: user avatars get employed by virtual businesses or private employers, spend a certain amount of time performing certain tasks (e.g. modelling in a virtual design studio), and get financial reward for the hours they spent at the workplace. The only difference between real life and Second Life is the currency used to pay out employees' salaries. Second Life employers reward their employees with Linden Dollars instead of real-world currency. It does not make too drastic a difference overall, due to the possibility of exchanging Linden Dollars for US Dollars. However, one drawback to earning money virtually is the fact that most exchange points only offer L$ to US$ exchange, and exchanging it afterwards to one's country's currency would inevitably yield a certain loss. With regards to the problem of unemployment, while it is present in every real-life economy, unemployment is not encountered in the world of Second Life. The two fundamental problems of economics, namely scarcity of resources and unlimited wants [12], are not as acute in the virtual economy, seeing as any object can be created at will and in unlimited amounts, hence making the goods and services provided by the human labour beneficial rather than vital. Second Life's initial release in 2002 was not meant to make use of any virtual currency or develop a virtual economy, so the financial opportunities, while being a very important aspect of Second Life, do not affect the flow and the "life" of the virtual world.

Chisholm & McCarty [24] define capital as "produced means of production". In the real world, it consists of goods produced for storage and used for creation of other goods and services. For example, a road is considered a capital good, since roads are used for transportation of consumer goods (food, clothing), as well as for numerous public transport services (buses, taxis). In addition to general capital goods like roads and buildings, other types of capital in a real-life economy are human capital and financial capital. Development of the human capital mainly involves education. Educated people can perform higher quality work thus adding to the country's physical capital, as well

as labour [12]. Financial capital is the money provided to businesses to create capital goods, thus supporting the economic system. Looking at the capital of the virtual economy of Second Life, we can see that the capital system is much simpler than its real life model. The capital of Second Life is mostly physical. Buildings are created to be used by various employers, shops, and other services; new sims are created to provide more freedom for the Second Life residents, thus enhancing their experience of the virtual world. Human capital of Second Life benefits both virtual and real worlds, since all educational programmes in-world also benefit the person's education in real life, thus adding to the human capital of the country the person is from. Financial capital of Second Life works just like its real life model: businesses are supplied with Linden Dollars to set up their in-world business, which in turn provides goods and services for the Second Life community.

The last production factor mentioned above is entrepreneurship. In the context of real life, the term governs the activity of entrepreneurs – people who are able to identify profitable opportunities in the market and are willing to take the risk of realising their creative business ideas [24]. Entrepreneurs are the driving force behind the economic development in any country since they are not afraid to think outside the box and put their creativity to life. Second Life's economic development had been made possible, as well as succcessful, through efforts of the entrepreneurs among the development team. The year 2003 brought the major change into the virtual world which affected the whole development process thereafter. At the end of 2003 the Linden Dollar was introduced, which put a start to what Second Life is now – a huge international virtual economy [73]. Since the notion of a virtual economy was not widely known back then, it required some innovative thinking and entrepreneurial qualities from the developers for the economic system to be introduced into Second Life.

As mentioned above, the introduction of the Linden Dollar into the world of Second Life marked the start of the development of the virtual world into a virtual economy. Inside the virtual world the currency exhibits the three characteristics needed for a commodity to be accepted as money: commodity as a medium of exchange, as a store of value, and as a unit of account [12].

The residents of Second Life use Linden Dollars to purchase various virtual goods

and services, i.e. they exchange their Linden Dollars to obtain those goods. In the same manner the providers of various goods and services obtain Linden Dollars in exchange for providing their products to the public. Similarly to real life, the existence of Linden Dollar as the medium of exchange helps avoid the double coincidence of wants. Linden Dollar easily maintains its value due to the fact that it is a virtual currency which is impossible to physically destroy. One cannot physically see or touch the virtual currency, but there is assurance that one can exchange the "invisible money" for things of value inside Second Life, as well as in real life. It is possible to order an item in a shop in Second Life and have the physical object delivered to your doorstep. Thus Linden Dollars serve as a store of value to their holders. The virtual currency is also considered a unit of account: it is divisible while still maintaining the same value [12]. That voids the need to calculate how much of a certain product must be sold to gain another product [24]. Thus we can see that Linden Dollar is a stable virtual currency. In addition to being a legitimate currency inside the world of Second Life, Linden Dollar has real-world value, as was mentioned above. This aspect of the Linden Dollar makes it a "meaningful currency". According to Yamaguchi [136], a "meaningful currency" is a virtual currency that can be exchanged to real-world currency at a certain exchange rate.

Another substantial proof that Second Life has evolved into a real economy is the constantly growing number of real-world businesses (such as Dell) which create their offices and branches in the world of Second Life, as well as businesses which have been established in-world [115]. Both the real-world and the in-world businesses offer work opportunities to Second Life residents, thus contributing to the cash flow of the virtual economy. Real-world diplomatic embassies have also established their presence in Second Life, offering their services to the public through their virtual offices. In 2007, the embassy of the Maldives opened a branch on the Diplomatic Island in Second Life [33], followed by Sweden, Serbia, Estonia, and a number of other countries. Most embassies only function as each country's representation in the virtual world, while the embassy of the Maldives is operated by virtual staff who help Second Life residents with visas and other diplomatic matters relevant to the real world [33].

The fact that Second Life has grown to be a fully functional economy, providing people with employment and financial profits proves that it has an impact on the real

world and is sometimes taken much more seriously than virtual worlds focused solely on entertainment. In fact, as discussed in Chapter 3, some users take on different personas when entering virtual worlds, and with their avatars live completely differently from the way they lead their real lives. The following section addresses the topic of Second Life as a platform for creating a full alternative life, and the possible dangers with regards to this phenomenon.

4.5 Second Life as an Alternative Life

An important but often overlooked aspect of Second Life is its psychological effect on the residents. People can create avatars which resemble their real life appearance, but they can also design their Second Life appearance in such a way as to embody their fantasies and dreams, to look the way they have always wanted to look. The personalities might also change with the change of appearance (Section 3.2.5 of Chapter 3 presented a more detailed discussion on this topic). Sometimes people get very attached to their virtual personalities, and start leading a genuine alternative life inside the Second Life world, parallel to their life in the real world. They make friends, build their dream home, travel around the Second Life sims, work for in-world employers. Second Life becomes not only a place to socialise, play, or make money, but a place where a person can experience as much freedom as real life could never offer. They can embody their personal dreams and desires, some of which might not have been possible in ordinary life, feel at ease with the people around them even if they were very shy in real life, due to the virtual aspect of communication, find people who share their interests, as well as build virtual relationships. One can fall in love in Second Life and even get married in-world, creating a virtual family. If this virtual family does not work out, in-world divorce is also something that is being done on a regular basis [66]. Even something as personal as religion made its way into Second Life. One can find Catholic cathedrals and other Christian churches, Muslim places of worship (Virtual Hajj [31]), and even a new religion, First Church of Rosedale, created in-world and being a parody of the real-world religions [68]. To its members, Philip Linden is God and Torley Linden is his prophet. It was started by Samantha Poindexter [90].

Boundaries between the virtual world and the real world become blurred, since a person involved so deeply in their Second Life existence might start mixing up real life and virtual life or feel that their activities and relationships in the virtual life gain priority over their real life alternatives. According to The Guardian [81] a couple got divorced in real life when the wife found her husband flirting and talking affectionately with a woman in Second Life. Thus, indulging in a Second Life alter-ego's life might negatively affect one's real life affairs. This raises a question of escapism versus psychological pathology: should one's "second life" be considered a way of relaxation, or as a means of running away from reality? Second Life residents' psychological connection with their avatars plays a big role in this. There is a drastic difference between thinking of Second Life as just another way to connect with people from all over the world or make some financial profit, and considering one's avatar an alter-ego, another identity, as important as one's real self. The latter case is highly likely to be a cause of a dissociative identity disorder (DID) which implies having multiple distinct personalities [42]. Each one displays its own unique behaviour depending on the situation one finds oneself in. These personalities usually appear involuntarily and spontaneously [55], [52]. If a person suffering from dissociative identity disorder registers in the Second Life world, they might use their avatar(s) to embody one or multiple of their alternative identities. It might be dangerous, since the person people meet inside the virtual world would not be their "real" identity, but one of their alter selves. Alternatively, embodying one's multiple identities in online avatars might lead to decrease of alter ego outbursts in real life. Second Life users struggling with DID have organised a support group named "DID Friendship Circle", providing a learning environment and support for people with DID and other personality disorders [130]. Garvey [42] states that experiencing disorders such as DID would be considered undesirable, but channeling them into various avatars in Second Life is "considered normal, liberating, and even transcendent", providing an "out-of-body" experience for the dissociative disorder patients. Thus it can be assumed that Second Life can be used as a means to relieve DID sufferers from the anxiety the disorder causes them in real life.

Another psychological disorder which might encourage the person affected by it to register in the world of Second Life is one of the anxiety disorders, namely the social phobia. A phobia is "a disruptive fear of a particular object or situation that is out of

proportion to any danger posed" [55]. A person with social phobia has an unrealistic and severe fear of being among unfamiliar people and being scrutinised by them [55]. Even though in Second Life most avatars surrounding a user are, in fact, unfamiliar people, a person with social phobia might feel less anxious among them than among real people. In Second Life no one can judge the person's anxiety levels by the avatar's appearance, thus displays of anxiety such as blushing or sweating, even if present in real life, would not give one's psychological state away, and might make one feel more at ease among strangers.

Another important fact to be considered is the following: when an owner of a Second Life avatar dies in real life, what is to become of their avatar? Such a question occurs to many Second Life users, especially to those who are closely connected with their alternative virtual personas. According to the official Second Life policy [65] [61], the will document of a resident can specify the legal (real-life) name of the person whom they want to inherit their avatar in case of their death. To put it in action, the person mentioned in the will has to send Linden Lab their identity document, the death certificate of the deceased, and any other legal documents requested by Linden Lab. One can see it as purely something related to the law, but it is a possibility that by making someone inherit their Second Life alter-ego after their death, a person might feel that they are prolonging their life on Earth even after death, practically achieving immortality.

Based on the characteristics and aspects of Second Life mentioned above one can clearly see that the virtual world has become something much bigger than a simple online game or a social network. It is a place for entertainment, a social space, an independent economy, as well as a true second life for any person willing to indulge in the virtual world's offers and possibilities. However, it is also evident that in most aspects of Second Life there is room for malicious and unlawful behaviour, which creates a necessity for forensic investigations to be done on the activity in the virtual world.

4.6 Conclusions

This chapter provided a detailed exploration of Second Life, the virtual world which this dissertation's goals are focused on. The history of the making of Second Life was studied,

listing the highlights of its development throughout the years 1999 – 2006, which could be called the crucial development years of the virtual world, even though its development continues up to this day. The chapter also examined the world of Second Life from four perspectives, namely as a game, as a social network, as an economy, and as an alternative life. Compared to well-established online games such as World of Warcraft, one can see that Second Life is very different in its structure. In fact, it has no particular structure, since there is no plot line users have to follow, and no skills or levels to be upgraded over time. Second Life is also a vast social network, where people can communicate via standard communication platforms like chat and private messaging, as well in more advanced ways such as dancing together or attending concerts. However, Second Life is not just a platform for entertainment and community-building. The virtual world is also a standalone independent economy with its own currency, bureau de change, and in-world business. This chapter explored the similarities and differences between a real-world economy system and the Second Life economy. Lastly, the chapter explored the psychological side of the world of Second Life, addressing topics such as mental disorders and death of users behind the Second Life avatars. These topics need to be addressed, since some residents take their online identities as seriously as their real identities, thus developing alter egos, which might negatively affect their lives in the real world.

The following chapter provides an overview of offensive behaviour in Second Life and presents the author's classification of offenses that may occur inside the virtual world.

Chapter 5

Crime in Second Life

Computers and easy access to the internet have become an essential part of everyday life in the modern/post-modern community. The internet has not only become a gateway to instant communication and information sharing, but also to the rest of the population that is registered on various online social networks. The fact that the Internet is so widely available does, however, make it an easy tool for people with malicious intentions. As in the physical world, the human factor plays an important role. As was briefly mentioned in Chapter 3, one may encounter rudeness, harassment, and other offensive behaviour in online social networks, especially in virtual worlds such as Second Life, since they allow for an even bigger variety of offences to take place. As explained in Chapter 4, the Second Life residents interact with each other on a more "physical" level, via their avatars' actions such as dancing, waving, or hugging [113], thus offences such as assault or robbery suddenly become possible in a seemingly harmless virtual world. Criminal activity in online virtual worlds has not yet been extensively studied: there is no standard classification for the offences one may encounter in these virtual worlds, nor have the means by which the offences are committed or ways to collect evidence of it been studied in depth.

This chapter provides an overview of various real life and cyber offences and presents the author's classification of the common offences together with their equivalents for virtual worlds (specifically Second Life). Section 5.1 consists of a brief discussion of the definitions of the legal terms used in this study, as well as the specification of the scope

of the study. Section 5.3 presents a table which combines a number of common law offences (based on the South African law) together with their equivalents in the Second Life environment. The table demonstrates the author's classification of the offences based on their targets (e.g. person, property, etc). The section also provides a discussion on the offences which can be committed inside the Second Life environment, by the means of the SL Viewer interface, without the aid of any external programs or spyware. Section 5.4 presents the results of a discussion on offences in Second Life with a focus group, held in October 2011 at the University of Pretoria, and provides an overview of real-life experiences of some of the offences discussed in Section 5.3. Section 5.5 concludes the chapter.

5.1 Defining "crime"

The terms "crime", "criminal activity", and "offence" have been mentioned so far with regards to security concerns arising in Second Life and other virtual worlds. Crime can be defined as an act which is considered by statute or common law to be public wrong, and is punishable in the court [1]. It is also defined as an action that is against the law, a wicked or forbidden act [123]. It is clear that these definitions are applicable to actions which are punishable according to criminal law and are subject to punishment, such as a jail sentence. "Offence" is defined in the Oxford English dictionary as "a breach of a law or rule; an illegal act" [95]. While the definition is similar to the definitions of the term "crime", the author considers "offence" a more general term governing not only severe acts with severe consequences, but also less serious misconduct against the public or an individual, such as breaching of a contract or offensive behaviour online. The term "offence" is also considered more applicable to malevolent behaviour in Second Life. "Criminal activity" implies the use of the term "crime", thus in this study the term "offensive behaviour" is preferred. A "criminal" is an individual who is guilty of or convicted for an offence, or a person who commits crime for a living [102], whereas an offender is an individual who engages in attacking and aggressive actions and acts against the law [123]. Similarly to the reasons for choosing the term "offence" over "crime", the term "offender" is preferred over "criminal" in this study. It may be argued

that an action might be condsidered offensive or unethical even though it is not against the law. Similarly, an action might be ethical, albeit illegal. Some actions which are considered offensive or criminal in real life do not always have the same impact in virtual worlds. Murder is part of the list of the most severe crimes, but it does not bear the same weight if put in the context of a virtual world. Killing off someone's avatar in a virtual world does not cause the person behind the avatar any physical harm, so can it really be considered murder? Evidently, in the context of virtual worlds the line between a simple irritation and an actual offence is not clearly defined and requires clarification. However, the topic of ethics and whether a legal act can be considered an offence based on its psychological impact is beyond the scope of this dissertation, and is considered a possible topic for future research.

5.2 Rules of Play

During the early stages of development of Second Life its creators realised just how big their virtual world was becoming, and just how deeply the residents grew to be involved with their virtual lives. They also realised that the big number of residents would inevitably lead to disputes and player-to-player problems, similarly to real life. Back in 2004 Robin Harper, Senior Vice President of Community and Marketing at Linden Lab, already expressed concerns about the escalating growth of the world of Second Life, and the need of a dispute resolution system, which would be more complex and "urgent", i.e. available at any time for any resident's use immediately after a dispute occurs [53]. Up until today a centralised dispute resolution system has not been put in place by Linden Lab. However, every Second Life resident is bound by the rules of a tight end-user license agreement (EULA), which lists a number of categories of anti-social behaviour prohibited in Second Life, also known as "The Big Six" [60]. The first category is intolerance, which focuses on acts of aggression or humiliation towards any resident on the grounds of their opinions or life choices (e.g. sexual orientation). It includes defamation, the use of demeaning language, racism and sexism, among others. The second category is harassment. Seeing as there is a vast amount of opportunities for harassment in Second Life, Linden Lab does not provide an exhaustive list of offences in this category, but

only mentions a couple of examples, such as offensively coarse or threatening behaviour, undesired sexual advances, or requests for sexual favours. Any other actions which result in annoyance or alarm also fall under "The Big Six". The next listed category is assault, which contains straight-forward and concrete examples, such as shooting, pushing, or shoving another resident in a Safe Area, i.e. an area where fighting and physical attacks on fellow residents are prohibited (most areas in Second Life are considered Safe Areas, except those built especially for games that involve fighting). Making use of scripted objects which would affect another resident's experience of Second Life (e.g. by stopping them from moving) is also listed as an example of assault. The fourth category of "The Big Six" is disclosure, which concerns residents' privacy. It includes sharing other people's private information, such as gender, race, age, etc., without their consent, as well as disclosure of their real-life location beyond what is included in their public profile. The category also includes remote monitoring of conversations, posting online and otherwise sharing chat logs without the consent of their participants. The next listed category concerns the adult content in Second Life. Adult content is allowed, but is limited to private islands and the adult continent "Zindra" [129]. No explicitly mature content is allowed on Mainland or even the land marked as "Moderate". Finally, the last category of "The Big Six" is disturbing the peace. It includes disrupting scheduled events, creating self-spawning items or otherwise intentionally slowing Second Life servers down, continuously posting unwanted advertisements or creating scripted sounds that follow residents and spoil their Second Life experience.

The above mentioned anti-social acts are considered significant offences and, if reported to Linden Lab, will result in the suspension of the perpetrator's account. If, having committed one or more of the abovementioned offences, the offender continues to engage in actions belonging to "The Big Six", they are banished from Second Life, and their account deleted. However, even the tight EULA might not always stop the perpetrators from malicious behaviour. The following section addresses the real-life offences, based on South African law, and their Second Life alternatives.

5.3 Categorisation of offences

The table presented here (Table 5.1) is the author's classification of a list of offences based on the South African common law [117]. The categorisation is based on the annual crime statistics of the South African Police Service (SAPS) [117].The first column of the table is titled "RL Offense" which stands for "Real Life Offence". This column lists all the offences which occur in real life, grouped according to the category they belong to.

The second column of the table, titled "Pre-conditions", lists the conditions necessary for a certain offence to be committed; e.g. one must be able to receive money from a person to commit fraud or kill a person to commit murder. It is important to note that a pre-condition is not used to define the offence, but is only listed as a basic principle which needs to be present/possible for the offence to occur.

The next column of the table is titled "SL Equivalent", which stands for "Second Life Equivalent". The author derived an equivalent of each of the real-world offences listed in Table 5.1 as applied to the Second Life environment. Some of these offences are not applicable to Second Life at all, e.g. poisoning, since an avatar is not able to consume any substance. However, most of the listed offences are possible in the virtual world, even though some of them can be committed via means much different from real life. The "SL Equivalent" column also provides a brief description of the specifics of the Second Life context of each of the offences listed there, in case the offence differs significantly from its real world origin.

The fourth column of the table, titled "Can occur Inside SL", states whether each offence applicable to Second Life can be committed inside the virtual world, or only "outside" the environment. Committing an offence "inside" the virtual world implies engaging in offensive actions by the means of one's avatar and the Second Life viewer of choice, whereas malicious activity "outside" Second Life involves performing an offensive act by the means of an external program or platform (except any Second Life viewing software). This categorisation is of utmost importance to this study, since the focus of the research is on the offences committed inside the Second Life environment, and the ways of their investigation. The reason this dissertation focuses on the offences committed "inside" Second Life is the fact that the goal of the current study is to explore the ways inexperienced users of Second Life experience offensive behaviour, and the ways

to gather evidence of those offences through the Second Life viewer itself. As discussed later in this chapter, inexperienced users are the ones who would be more likely to fall victims to offences such as griefing or harassment, and it is important to explore ways to gather evidence through the standard Second Life viewing software, seeing as it is the default software every new resident starts interacting with Second Life through. Offenses committed via other Second Life viewers, as well as via different means altogether, and the respective investigative techniques such as analysis of external logs or databases, are outside the scope of the current study and are possible topics for future research.

The following sections provide a detailed discussion on a number of offences belonging to different categories from Table 5.1 and more likely to be encountered inside the Second life environment, leaving the rest of the listed offences for future work.

Table 5.1: Real Life vs. Second Life offences.

RL Offense	**Pre-conditions**	**SL Equivalent**	**Can occur Inside SL**
OFFENSES AGAINST THE PERSON			
Abduction	Possibility to forcibly take the person somewhere	Teleporting someone to another sim other than which they were originally in without their consent	Yes
Account Hacking	Possibility to obtain login information	Account Hacking	Yes
Assault	Possibility to physically attack a person	Griefing (Only restricting movement / pushing / touching, since no physical harm can be done)	Yes

Continued on next page

Table 5.1 – *Continued from previous page*

RL Offense	**Pre-conditions**	**SL Equivalent**	**Can occur Inside SL**
Bestiality	Possibility to have sex	Only possible if one of the avatars is in a shape of an animal	Yes
Bullying	Possibility to pester, attack, or threaten the person	Griefing	Yes
Crimen injuria[1]	Possibility to invade the privacy of the person	Crimen Injuria	Yes
Culpable homicide	Possibility to physically kill a person	Deleting an avatar	No[2]
Defamation	Possibility to share false information about the person with others via various means such as spoken or printed words	Defamation	Yes
Exposing an infant	Possibility of death / physical harm, presence of infants	n/a	n/a
Extortion	Possibility to threaten the person	Extortion	Yes

Continued on next page

[1] A crime under South African common law, defined as the act of "unlawfully, intentionally and seriously impairing the dignity of another." [25]

[2] An avatar cannot be killed except in designated fighting areas [69], and the deletion of an avatar from the Second Life database would occur outside of the Second Life viewer.

Table 5.1 – *Continued from previous page*

RL Offense	**Pre-conditions**	**SL Equivalent**	**Can occur Inside SL**
Identity Theft	Possibility to obtain private information	Identity Theft	Yes
Impersonation	Possibility to obtain private information	Impersonation	Yes
Incest	Possibility to have sex	Incest	Yes
Kidnapping	Possibility of taking a person somewhere and restricting their movement	Teleporting someone to another sim other than which they were originally in without their consent and restricting their movement	Yes
Murder	Possibility to physically kill a person	Deleting an avatar	No
Paedophilia	Possibility to have sex	Paedophilia	Yes
Poisoning	Possibility to make the person eat/drink something	n/a	n/a
Rape	Possibility to have sex	Virtual Rape	Yes
Robbery	Possibility to attack / threaten to attack a person	Virtual Mugging (Forcing the victim to give you something of value via restricting their movement / pushing / touching)	Yes

Continued on next page

Table 5.1 – *Continued from previous page*

RL Offense	**Pre-conditions**	**SL Equivalent**	**Can occur Inside SL**
Stalking	Possibility of following a person, pestering them	Cyberstalking	Yes
OFFENSES AGAINST THE PUBLIC			
Contempt of court	Presence of court	n/a	n/a
Defeating or obstructing the course of justice	Presence of an institution with the authority to administrate justice and address legal disputes between parties (e.g. court)	n/a	n/a
High treason	Presence of a government or some other authoritative group, possibility to affect its decisions	Forcibly making Linden Lab change its constitution. Communication inside SL could facilitate the process of organisation of a hostile takeover of Linden Lab.	Yes
Inciting public disorder	Possibility to contact / advertise to a large number of people	Griefing	Yes
Public indecency	Possibility to act in a highly crowded place	Public Indecency	Yes

Continued on next page

Table 5.1 – *Continued from previous page*

RL Offense	**Pre-conditions**	**SL Equivalent**	**Can occur Inside SL**
Public violence	Possibility to act in a highly crowded place, possibility to gather a group of people	Public violence	Yes
Sedition	Presence of a government or some other authoritative group, possibility to gather a group of people	Defy, challenge, or resist the authority of Linden Lab.	Yes
Violating a corpse	Presence of a corpse	n/a	n/a
Violating a grave	Presence of a grave / graveyard	Violating a virtual grave	Yes
PROPERTY-RELATED OFFENSES			
Arson	Possibility of fire damage	n/a (only fire animations)	n/a
Burglary	Possibility of entering a private building	Burglary	Yes
Malicious damage/ vandalism of property	Possibility of alteration / damage to property	Damage / vandalism of property	Yes
Receiving stolen property	Possibility of receiving items from another person	Receiving stolen property	Yes
Stock theft	Possibility of stealing animals	Stock theft	No

Continued on next page

Table 5.1 – *Continued from previous page*

RL Offense	**Pre-conditions**	**SL Equivalent**	**Can occur Inside SL**
Theft of motor vehicle and motorcycle	Possibility of entering a vehicle and operating it	Theft of motor vehicle and motorcycle	Yes
Theft out of or from motor vehicle	Possibility of entering a vehicle and taking something out of it	n/a	n/a
Trespass of real property	Possibility of trespassing of property	Trespass of virtual property	Yes
MONEY-RELATED OFFENSES			
Assisting gambling	Possibility of advertisement	Assisting gambling	Yes
Betting	Possibility of communicating the betting rules to a person and receiving money	Betting	Yes
Embezzlement	Possibility to receive money from a person	Embezzlement	Yes
Fraud	Possibility to receive money from a person	Fraud	Yes
Gambling Equipment Violations	Possibility of selling, possessing, or transporting items / equipment used for gambling purposes	Gambling Equipment Violations	Yes
Money Laundering	Possibility to receive money and obscure its source	Money Laundering	Yes

Continued on next page

Table 5.1 – *Continued from previous page*

RL Offense	**Pre-conditions**	**SL Equivalent**	**Can occur Inside SL**
Prostitution	Presence of brothels, possibility of sex	Prostitution	Yes
Shoplifting	Possibility of stealing items from a shop	Virtual Shoplifting	Yes
OTHER OFFENSES			
Discrimination (based on a certain characteristic)	Possibility of restriction of opportunities to people with a certain characteristic	Discrimination	Yes
Forgery and uttering	Presence of official certificates or other documents	n/a	n/a
Gold Farming	Possibility to obtain virtual currency / goods and trade it for real money, presence of a number of people employed to earn money / gold in-world	Gold Farming	No
Perjury	Presence of a certain course of justice (e.g. court)	n/a	n/a
Pornography distribution	Possibility of distributing information / items to other people	Pornography distribution	Yes

Continued on next page

Table 5.1 – *Continued from previous page*

RL Offense	**Pre-conditions**	**SL Equivalent**	**Can occur Inside SL**
Sports Tampering	Presence of sporting events	Virtual Sports Tampering	Yes
Spam	Possibility for information sharing	Spam	Yes

5.3.1 Griefing

Griefing belongs to the category of "Offenses against the person", according to Table 5.1. Griefing involves malicious actions which are aimed at a specific person, or sometimes a group of people, in order to disrupt their virtual world experience, harass them, damage or steal their virtual persona, etc [38]. Griefers usually do it out of boredom, to assert their power, or simply "because they can" [23], which is upsetting and disturbing, but generally harmless. However, sometimes the purpose of such actions is much more serious. By the means of harassment or identity theft an offender might attempt to get the victim's money or virtual property, and offences such as defamation or bullying might cause trouble in the victim's real life. But regardless of the purpose, any offensive behaviour towards any Second Life resident must be stopped and, if possible, prevented.

In Table 5.1 griefing is listed as the Second Life alternative to assault, bullying, and inciting public disorder. Assault is one of the "Big Six" offences of Second Life's community standards, and it is a term for an attack on another person. Assault is mostly associated with physical attacks, or, as applied to the Second Life environment, attacks on an avatar by another avatar such as pushing them around or blocking their way. In gaming-oriented virtual worlds (e.g. World of Warcraft) actions like repeated killing of a certain character (even though killing is allowed) are seen as griefing [38]. Jim Rossingol [112] defines a griefer as "a player with malign intentions" and explains that "[t]hey will hurt, humiliate and dishevel the average gamer through ending and breaking the rules of online games" . However, it must be noted that the term "griefing" is used both for

"physical" attacks such as killing an avatar, as well as general offensive, disruptive, and anti-social behaviour. Typical examples would be a DOS (denial of service) attack on the servers of Linden Lab which would temporarily cause a number of sims to crash, harassing actions towards other players, insulting and obscene chat messages, etc. Mulligan and Patrovsky [84] define griefing in virtual worlds as "purposefully engaging in activities to disrupt the gaming experience of other players" . In a similar fashion, Warner and Raiter [128] define the concept as the "intentional harassment of other players" and note that "the game structure is used in unintended ways to cause distress for other players". Foo and Koivisto [38], two game theorists who research antisocial behavior in massively multi-player online role-playing games (MMORPGs), characterize it as a type of play style and refer to it as grief play. As we can see, griefing is seen as an umbrella term governing the virtual world alternatives of both assault and harassment. Chesney *et al* [23] put griefing in the same category as harassment and bullying, or in this case cyberbullying. Cyberbullying is bullying via the means of digital media such as computers, mobile phones, tablets, etc. It has been described as "[a]n aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself" [119]. Chesney *et al* note that griefing in Second Life is very similar, but not quite the same as bullying in real life, for two reasons. Firstly, the bully is not physically present in the virtual world, which might make the attacks feel less threatening. Secondly, the victim of griefing would generally not know the identity of the offender, seeing as millions of people all over the world use Second Life. Griefing also differs from bullying in the fact that the victim can escape griefing attacks at any time by either teleporting to another area, disconnecting from Second Life, or entering Second Life via another avatar. However, the necessity to "escape" would nonetheless be disrupting and lead to annoyance and dissatisfaction with the gaming experience. They might also encourage the griefer, since their aggressive actions would cause the victim to deny him/herself some parts of the virtual world or in-world activities, thus essentially "losing the game" [23]. Foo and Koivisto [38] mention three aspects of a griefer's actions, based on a definition by Mulligan [84], namely: a griefer's actions are intentional, spoil the victim(s) gaming experience, and are done for the perpetrator's enjoyment. Thus we can see that the intention is the key factor behind

griefing. However, the authors make a point of the fact that not every act of griefing is intentional. In general, the players would feel griefed if an action of another player caused them frustration or annoyance, even if the player abided by the game's rules . In their work Foo and Koivisto refer to MMORPGs and provide examples of unintentional griefing as camping, i.e. standing in a position where a valuable item is expected to appear, to be the first to collect it, thus denying other players a chance. In the world of Second Life which is not focused on gaining experience and money, an example of such unintentional griefing could be building an item in a public practice area, in the spot where another person wanted to build their object(s). The person who was denied the location would naturally be disappointed and might get annoyed with the "griefer"; however, the person who "stole" their spot did not break any rules of Second Life, and might have used the building location completely unintentionally, unaware of the other player. Foo and Koivisto propose a special term for such unintentional griefing, namely "greed play". It is more subtle than grief play, but might still cause annoyance, be seen as selfish, and disturb other people's gaming experience. Foo and Koivisto also propose three other categories of griefing, namely harassment, power imposition, and scamming. Harassment is a type of offence which involves actions aimed to threaten or otherwise disturb the victim (or victims). Harassment griefing does not benefit the griefer in any way apart from the enjoyment of seeing the victim suffer. The authors mention slurs, space intrusion, and spam as examples of harassment griefing. One may unintentionally offend another, but if one does not stop the offensive action(s) after being asked to do so, it can be rightfully considered an act of griefing. The "power imposition" category of grief play refers to griefers who demonstrate their power to fellow players in a way that is harassing, disturbing, or humiliating. In Second Life griefers might attack newbies who are not yet completely familiar with the environment and threaten them, claiming to be people of authority. A Second Life user Fr43k Paine mentions "fake police", or other demonstration of fake power, used as a means to "rob" newbies or make them do what the griefer says [93]. Chesney *et al* [23] mention that some griefers try to assert their knowledge of Second Life over the newbies who lack it, and exploit the fact that the newbies do not know how to defend themselves from the attacks. The third category of grief play is scamming. Scamming refers to a fraudulent or deceptive act or

operation [32]. According to the author's crime categorisation in Table 5.1, fraud belongs to the category of money-related offences. However, this section only considers the anti-social and harassing aspects of griefing, which involve the victim's person and not thier possessions. Money-related offences such as fraud will be discussed in Section 5.3.3. Sometimes griefers unite and act as a group. That gives them a sense of belonging and the feeling of power over their victims, since a person subjected to a group attack is more likely to subdue, or surrender and log out of the virtual world out of frustration, which is then seen as a victory [38].

Griefing also belongs to the category of "Offenses against the public", as seen in Table 5.1, since a lot of griefing attacks in Second Life are aimed at everyone in the area where the attack is being launched. Most well-known examples would be the Second Life Liberation Army (SLLA) group which launched an attack against the clothing store, American Apparel. They shot "white balls" which obscured areas of the screen temporarily, and interfered with people's ability to see merchandise and to shop. Sometimes these effects actually pushed customers out of the store [99]. The reasons behind the attack were that of liberation nature, as the group members tried to demand voting rights from Linden Lab by the means of griefing. However, the residents shopping at American Apparel at that moment, who did not know about the "liberation movement", were involved in the attack and much disturbed in their in-world experience. One of the members of the focus group the author took part in (discussed in Section 5.4) mentioned that when he was walking in a Second Life area the area was suddenly filled with self-copying scripted items which looked like boxes with an image of dancing Hitler on them. The outburst of scripted objects obscured the way and slowed down the system's performance. Most probably that was a variation of the infamous CopyBot, a third-party software which copies other people's objects without permission and with no quantity limit [47]. A similar griefing attack was launched on Second Life's famous persona Anshe Chung [124], when a griefer group "Room101" disturbed her live interview with CNET by a cloud of animated flying penises which interrupted the live talk for about 15 minutes [23].

Griefing is one of the most commonly encountered offence in Second Life, as well as an offence with probably the biggest variety of causes, variations, and ways of imple-

mentation. It is evident that, as griefing becomes more and more common in the Second Life community, Linden Lab will need to consider some law authority for those griefers who cause serious harm. Some Second Life residents are starting to take responsibility and organise into groups to find griefers, report them to Linden Lab, and ban them from certain areas in Second Life [23]. Ideas on possible investigative techiques of offensive behaviour in Second Life are discussed in Chapter 7.

5.3.2 Property-related offences

Virtual property is becoming an important topic, as the popularity and the scale of the virtual worlds continues to grow. Second Life presents virtual property and content creation as one of the main features of the virtual world; according to their Terms of Service (ToS), any resident creating and submitting content in Second Life owns intellectual property rights (called a "User Content Licence" [61]) to anything that they create or submit to the service, as well as to any user-created items that they buy off another resident. It is specifically stated in the ToS that "the term 'Buy' or 'Purchase' means to receive a User Content License in exchange for Linden dollars or other consideration in accordance with the Terms of Service" [61]. Everything in a virtual world is created by programming, i.e. via the writing of code which runs on a server and creates scripts and all the virtual items. Since code is seen more like an idea rather than personal property, it is governed by intellectual property rights [3]. However, virtual worlds such as Second Life have brought a different kind of code to the scene; code which is designed to act more like chattel property than just an idea [3]. If one creates a unique item it is regarded as personal property, which no other user can enjoy and make use of unless the owner personally grants them access to it. This has been raising some concerns as to whether intellectual property rights are enough to protect the virtual property from theft, vandalism, unauthorised access, and other property damage. According to Adrian [3] [4], virtual goods must be regarded as personal property rather than an idea, categorised as intellectual property. Virtual property fits the five aspects of chattel property: the ability to possess, use, enjoy, transfer, and exclude others from it [114]. Second Life residents possess the items they create or buy, are able to use them as they wish, and enjoy the benefits those items grant them. Residents can easily transfer the goods to

other people by selling them, or transfer the goods "physically" by moving the items on the virtual land (except if the owned item is in itself virtual land which cannot be moved). Property owners can also deny some residents access to or even the ability to see their items by concealing them inside the boundaries of a private virtual land, whereas intellectual property rights only govern adaptation, distribution, display, reproduction, and performance [137]. The absence of property rights makes it very difficult to appeal to court if an offender defaces one's house or damages a virtual item by attaching a malicious script to it. In 2007 a griefer group called "Patriotic Nigras" defaced the headquarters of a politician John Edwards [17]. Their actions have been reported numerous times, but, being a big and ever-changing group of individuals, it was hard to track and ban everyone's accounts. In addition to property vandalism, virtual property can be practically stolen if the offender either copies the victim's objects without their consent (e.g. via CopyBot) or tricks them into giving their objects to them as part of a fraudulent trade, not giving anything in return and disappearing afterwards. Such actions call for the virtual world authorities to review their current "hands-off" approach (avoiding involvement in any resident disputes) and install some form of criminal law to protect their residents from attacks.

5.3.3 Money-related offences

The two most commonly encountered offences which involve illegal acquisition of money are fraud and money laundering, both of which involve obtaining money via illicit means. Fraud is defined as "deception deliberately practiced" [5]. In the context of Second Life, fraud would be deception of a Second Life user into giving the perpetrator money either when purchasing goods or for safekeeping, or simply tricking them into clicking a link which leads them to a fraudulent webpage, and providing their bank account details. According to Lee [64], the offenders in Second Life would often "take advantage of the social engineering and target specific weaknesses that exploit the gullibility of users". Chesney *et al* [23] also mention naive inexperienced users of Second Life who could become "easy prey". If a fraudster was to pretend to be an experienced user, they could convince a newbie that a certain action would earn them virtual currency, in reality stealing their personal details (such as login information) and using it for their

own profit. The users of the Firestorm Second Life viewer were recently tempted by a fraudster who messaged Second Life residents, making it look like a message from Second Life developers themselves, offering instant 1000 L$ to anyone who clicks on a certain link and registers there [127]. Another scam was being circulated in 2012 in the Second Life environment: residents would receive private messages offering good deals on the Second Life Marketplace, with links to a login page. The login page looked exactly like the original Marketplace webpage, but it was fake, and by having people sign in there the fraudsters received their login details. Later they used that information to wipe out the accounts of the people who fell for the scam [29]. Fraudulent actions do not necessarily involve actual goods or money. A person might make a deal with another to create a certain unique item, sell it, and share the profit equally between the two developers. However, when the item is created, one of the involved parties would copy it to their inventory and disappear, putting it up for sale as an individual before their fellow developer has the time to, thus gaining all the profit for themselves. The main reason for fraud is money making, although gaining some valuable information (such as ways to create specific items) without paying for it could also be a reason to involve oneself in fraudulent activities.

Money laundering is hiding the source of money obtained via illegal means [110]. This is one of the big financial problems of the real life economies [75], and, seeing as the world has become "digitalised", money laundering found its way into virtual economies as well. Being the biggest virtual economy at present, Second Life is probably the most likely platform for online money laundering. A Second Life resident may use an actual credit or debit card to purchase Linden Dollars, later redeeming those credits for actual money with another resident in another country and in that country's unit of currency. Should a money launderer take advantage of this and purchase Linden Dollars with a stolen card, the money would be difficult to trace back to the original buyer. Seeing as the money is redeemed from Second Life, it also obscures the original source of the money, only tracing it to the virtual persona. To further obfuscate the illicit source of the money, the money launderer could also register a number of different Second Life accounts, all with fake information in their profiles, transferring Linden Dollars between them as if those avatars were different people, and later redeeming the money as real-life

currency from one of the fake accounts. The Linden Dollar transactions are only logged for up to 32 days, while older logs are discarded [58], which could also be advatageous to money launderers if the transfers between a number of fake accounts happen over a period of time longer than the 32-day limit. And, seeing as there are thousands of people all over the globe participating in virtual worlds such as Second Life, the in-world money transfers would be very difficult to track.

5.3.4 Other offences

Among other offences, child pornography and virtual paedophilia are two serious concerns in Second Life. Virtual sex is legal in Second Life, but to protect minors adultery is only allowed on a specialised island called Zindra [134]. However, this does not stop the paedophiles, and they find new ways of realising their fantasies. An example of that is sexual ageplay; the act of simulating child sexual abuse by two consenting adults' Second Life avatars, one of which takes the form of a child [106].

According to a report on Sky News [36], an undercover investigative journalist reported on sexual ageplay at a Second Life location called Wonderland. It was described as a "virtual paedophile ring", with houses filled with perverse images, embedded videos of child pornography, sex toys, etc [36]. Despite the evidence, Linden Lab responded to the report negatively, stating that there was "no firm evidence of wrongdoing" [125]. The reports led to international police investigations of ageplay in Second Life, and Wonderland in particular [71], which resulted in the demolishment of the Wonderland island. The investigator also reported that after it was demolished "the usual individuals were still turning up, unsure of what had happened" [36]. However, in a minute or two a virtual note was circulated among the avatars present in the area with a list of close to fifty other "child-play" areas. The list was passed to England and Wales' Child Exploitation and Online Protection police unit[3] (CEOP) in Virtual Barcelona and the case was left for further investigation by the police officials. However, the problem still exists, and nothing can guarantee that paedophiles would not find themselves shelter in virtual worlds such as Second Life. However, online paedophilia is a concern not only from a

[3]http://ceop.police.uk

virtual world perspective. Since any online action is invoked by a human in real life, it is evident that online paedophilia has a real-world aspect and might lead to harm of children in real life. Online child sexual exploitation is listed as one of the key threats in the "Threat Assessment of Child Sexual Exploitation and Abuse" published by CEOP [22]. Reeves [106] also mentions the real life aspect of sexual ageplay, and discusses four hypotheses addressed by the research community which make a connection between sexual fantasies (or sexual ageplay, in the current context) and real-world child sexual abuse:

- real child abuse images may be disguised as fantasy images;
- fantasy images are found alongside collections of real child abuse images and so are indicative of risk of offending;
- fantasy images can be used as a grooming mechanism with children;
- viewing fantasy images of child sexual abuse may reinforce inappropriate feelings towards children.

The first proposition is dismissed by Reeves, due to the fact that sexual ageplay in Second Life is a purely online activity. It is a sexual fantasy invoked by two avatars interacting directly with each other, without the use of any external images or videos. With regards to the second proposition there are no direct research findings which would prove or disprove it. However, the correlation between sexual ageplay and possession of real abuse images is indirectly evidenced by police investigations into Second Life activity of sex offenders, which often involved their engagement in virtual prostitution rings [106]. Reeves mentions that fantasy images are sometimes used by paedophiles as a "safe" alternative to real child abuse. Johnson and Rogers [49] pose a question as to whether such sexual fantasies should be regarded as problematic, with the absence of evidence to prove the correlation between possession of fantasy images and the increased probability of the people in possession to engage in real child sexual abuse.

The third hypothesis is analysed by Reeves from the real-life perspective. Reeves [106] and Wilson [135] argue that entering sexual ageplay in Second Life while with a child in real life could potentially be used to "normalise the behaviours" of a child,

which would constitute a real-life offence and would be prosecuted by the laws of the country the incident took place in. However, addressing sexual ageplay from the virtual world perspective, Reeves dismisses the possibility of the in-world activity to be used as a grooming mechanism, since no children are involved in the act. With regards to the last proposition, Reeves points to the lack of any clear findings on the topic, and to the criticism by some authors (e.g. Malamuth and Huppin [70]) of the methodological quality of the research conducted in the field.

Generally, it is argued that if sexual ageplay can be demonstrated to cause harm or promote child sexual abuse, it ought to be regulated [2]. However, the research findings in this field are too scarce to provide any reliable evidence to this relationship. Nonetheless, researchers pose a question as to whether it is ethical to engage in sexual ageplay, seeing as it can potentially be used to promote child abuse [2] [135].

Since 2008 Second Life installed age restriction mechanisms which require the user to submit real-life identity papers such as passports or provide proof of payment by credit card. This greatly reduces the risks of minors being able to access adult areas and thus helps them avoid potential paedophiles. However, no security mechanisms are completely safe. Guinchard [45] mentions a possiblity of a child stealing a credit card from an adult, and Meek-Prieto [77] talks about the use of motion-sensing technology where children could be used to mimic movements that would appear on the screen as those of an adult avatar's without the other avatars' knowledge.

Even if a Second Life resident is involved in paedophilia or child pornography distribution, Linden Lab would not suspend their account or ban them from the virtual world unless they are found guilty of one of the acts mentioned in the list of the "Big Six" crimes [23]. However, it is evident that if these offences become more common in the Second Life community Linden Lab will need to consider some law authority for sex offenders.

5.4 Second Life offences examples based on real life experiences

The current study uses information gathered from a focus group discussion on Second Life offences, held in October 2011 at the University of Pretoria, South Africa. It was led by Mr. K. Eloff, a lecturer in the field of Information Science (Multimedia) specializing in Human-Computer Interaction, as well as Virtual Environments. A group of students enrolled for Mr. Eloff's module on Virtual Environments were gathered to discuss various possibilities of offensive behaviour in Second Life. The attendees were given the table presented above (see Table 5.1) and asked to find examples of the offences listed in the table based on their real-life experiences. This was done in order to gain some insight into the types of offences encountered by inexperienced users of Second Life and their views on the possible ways of defending against such offences, as well as ways of tracking the perpetrators.

Two examples of online harassment, or "griefing" (see Section 5.3.1), were reported. One was an example from the World of Warcraft, a massively multiplayer online role-playing game (MMORPG) similar to Second Life in its environment's characteristics. It involved high-level players spoiling the playing experience of lower-level players. The experienced players took part in easy missions meant for lower-level players, already knowing where to look for valuable items due to their experience. They quickly seized all the valuables before the less experienced players could get to them, thus abusing their advantage over the low-level players. The other example reported by the focus group involved a user being harassed in Second Life while changing her avatar's clothes in Second Life. A stranger pushed her avatar around, which caused the camera to constantly change its angle, making it difficult to see the avatar. In Second Life an avatar becomes immobile (while still being visible to the outside world) when its owner enters editing mode, to change clothes or other attributes of the avatar's appearance. The griefer took advantage of that fact and disturbed the user's online experience. Another example of griefing is unwanted deletion of a user's objects in Second Life. The author found that it was impossible to completely delete someone's objects in Second Life due to the backups existing on the server. However, it was argued that in case a person

forgot to set the properties of the object they were working on to "no modify" and "no delete" it was possible for any stranger to delete the object without the owner's consent.

As part of the category of offences against the person, the focus group addressed the possibility of kidnapping and impersonation. The Second Life environment allows for the teleportation of a user to a certain place in-world, so it was generally considered a realistic threat. One example was reported which involved a Second Life user warning the people around her not to follow a group leader, since, according to her, it was "a trap". A user conducted a virtual tour inside Second Life and at a certain point invited the tour attendees to follow him by teleporting to some location. A stranger standing nearby saw their conversation and started warning the group against following the tour guide. Thus the tour guide concluded that such things as "traps", or virtual kidnapping, had indeed taken place in the world of Second Life. Logging off was considered the easiest solution in case of kidnapping, since an avatar disappeared from the virtual world when its owner logged off and quit the Second Life viewer. Impersonation was also discussed by the focus group members, and argued to be one of the more frequent offences in Second Life. Each Second Life user has a unique username, as well as a non-unique display name which they can set to anything they like. When other people see an avatar in Second Life, both the display name and the username are visible above the avatar's head, or, in case the owner has not set a display name, only the username is visible [67]. An impersonator could create an avatar with a very similar username, as well as the same display name, as another avatar, which would make it easy to mistake the impostor for the original avatar. Likewise, an impersonator could make their avatar's appearance almost identical to another user's avatar, with similar results. An example was reported by the focus group: a person would log in to Second Life and see people discussing something they did, but did not remember doing. Such a situation would most probably be caused by someone impersonating the user.

The focus group also addressed money-related offences such as mugging, theft, and fraud. The author learned that it was not possible to forcibly take any item from an avatar by another avatar since the victim could always teleport to another area. Two types of theft were considered in the focus group discussion. The perpetrator could either hack into a Second Life user's account and steal their possessions (items, money, etc),

or take another user's objects if the victim forgot to set its "no copy" property value to "true". It is debatable whether that should be considered theft, since a stranger would not know if the original owner had meant the object to be available to the public or not, but it is generally considered unethical to copy someone else's objects without their explicit permission. It would most likely be considered theft if the user who copied the object attempted to earn money by selling or renting it. Fraud was also considered in the context of Second Life. According to the members of the focus group, fraud would usually involve false advertising. A fraudster would advertise an item, and after buying it the victim would see that the item was not at all what it was advertised as. Due to the information about the last owner of the object available in the object's metadata such fraudsters would be fairly easy to track, although it would be difficult to prove them guilty, unless each transaction was accompanied by the buyer taking an in-world screenshot of the item and the seller, as well as citing the description of the item(s) as evidence, for future use. The issue of false trust was also considered in conjunction with fraud. If a person were to establish false trust with another person in Second Life, the perpetrator could convince the victim to lend him/her money, and disappear with it, effectively committing embezzlement.

Lastly, as an offence belonging to the category of property-related offences, vandalism was addressed by the focus group. It was considered possible, although difficult to commit in Second Life. If a user did not want anything on their property which they did not put there themselves the user could just set the value of the "no dropping" property of their sim to "true", and disable any stranger from leaving unwanted things on their land. The author found that one could only have an object defaced if one did not lock the object. It was argued that if one created a plane with a texture and put it in front of an object the original would effectively be defaced, provided the plane had an offensive texture. Using a CopyBot [9] to flood someone else's sim with unwanted objects would also be considered an example of vandalism.

As a result of the discussion above, the focus group expressed some ideas on digital evidence sources, as well as possible evidence-gathering techniques applicable to the Second Life environment. Chapter 7 addresses those and other ideas about digital forensics in Second Life, and presents a discussion of each of the suggested techniques.

5.5 Conclusions

This chapter covered various types of offensive behaviour in Second Life. Section 5.1 defined the notion of "crime" and established the terminology used in this study with regards to criminal offences. Section 5.2 provided an overview of the "Big Six": the six categories of offences listed in the Code of Conduct of Second Life, namely intolerance, harassment, assault, disclosure, adultery, and disturbing the peace. Comitting offences belonging to the "Big Six" might lead to one's account being suspended, or, with repeated misconduct, the offender could be banned from Second Life. In Section 5.3 the author presented a classification of various real-life offences based on the South African common law (see Table 5.1), and a mapping of these offences to their Second Life equivalents. It is important to note that not all real-life offences are applicable to the Second Life environment, due to various differences between the real and virtual worlds. The table of offences is organised into five categories, according to each offence's target, namely "Offences against the person", "Offences against the public", "Property-related offences", "Money-related offences", and "Other offences". The latter category includes all the offences which do not fit into the previous four categories. Section 5.3 was divided into four subsections, namely Griefing (5.3.1), Property-related Offences (5.3.2), Money-related Offences (5.3.3), and Other Offences (5.3.4). Each of the subsections discussed a selection of Second Life offences mentioned in Table 5.1 in more detail. Finally,the chapter was concluded by a discussion of users' real-life experiences, held in a focus group organised by the author and led by Mr. K. Eloff (Section 5.4). The following chapter will focus on the exploratory experiment run by the author, exploring griefing in Second Life.

Chapter 6

Experiment: Griefing

Previous chapters provided an overview of Digital Forensics, as well as the field of Virtual Worlds, with a focus on Second Life. Theoretical discussions of various offenses in Second Life, and possible ways they could be committed have also been presented, providing sufficient background information as well as a general overview of the topic of this dissertation and the research ideas of the author. The current chapter presents an experiment conducted on the second of May 2012 at the University of Pretoria, South Africa. The goal of the experiment was the exploration of a number of the author's ideas which resulted from the work discussed in the previous chapters. In the experiment the author attempted to apply the theories and ideas developed through her research to a small real-life scenario, where a small group of people were gathered inside the Second Life virtual world, and asked to imitate offensive behaviour. The main goals of the experiment were to explore the ways griefing can be committed inside Second Life, to identify possible ways of gathering evidence by the avatars observing the offensive actions (not involved in the incidents themselves), and to measure the usability level of such evidence gathered "on the go".

In the following sections the experiment is described in detail. Section 6.1 presents the theory behind the experiment, Section 6.2 describes the experiment setup, Section 6.3 focuses on the experiment procedure, and Section 6.4 presents and discusses the results of the experiment. Section 6.5 concludes the chapter.

6.1 Theory

As was mentioned earlier in this dissertation, this is an exploratory study. The author did not start the experiment with any set frameworks or expected results in mind, but, having provided initial technical training to the experiment participants, wanted to study the different approaches of the participants to the given tasks, as well as their findings at the end of the experiment. The focus of this study is not on the statistical results such as the number of different ways the participants managed to gather evidence of the griefing attacks, but rather on the participants' experiences in Second Life, as well as their comments and opinions on what happened to them during the running of the experiment. Thus, as opposed to the majority of studies conducted in the field of Computer Science, the current research experiment falls under the qualitative research category.

Qualitative researh is a method of enquiry focused on in-depth exloration and interpretation of the social aspects of human behaviour in certain circumstances or situations, as well as the reasons that govern this behaviour. Qualitative studies explore the *why* and *how* of the studied social setting, instead of *what*,*where*, and *when* [30]. The methods and techniques of qualitative research help researchers study the things that cannot be measured, such as people's individual views or reactions to interaction with people around them, which sometimes is more important for the success of a study than providing numbers and statistics. There are a number of methodolocial approaches to qualitative research, such as grounded theory, ethnographic research, phenomenology, and various other approaches [30]. In the current study the author made use of phenomenology: explored a specific phenomenon, namely griefing attacks inside the Second Life environment, and looked at the participants' personal experiences of this phenomenon. Various methods of data collection are employed by researchers to conduct qualitative studies, namely participant observation, field notes, interviews, and a number of other methods [30]. The methods employed in the current study were participant observation, field notes, and a questionnaire. The participants were gathered in a computer lab, with the author observing their actions and taking notes. At the end of the experiment all participants were asked to fill in a brief questionnaire. Section 6.3 addresses the methodology of the experiment in more detail.

Having its focus on an in-depth interpretation, qualitative research methods yield the

best results if applied to a small group of people as opposed to a big sample. A small group chosen on the base of a specific criteria produces outputs that can be analyzed with no technical difficulties. Thus the number of the participants for the current study is also quite small, seeing as analysing a large quantity of qualitative material would be extremely time-consuming and could in the end become counter-productive and cause confusion. Having a small number of participants also aids team work. The participants can see each other, talk to each other and easily share ideas and get help. Such a setting resembles a focus group [27], lacking only the interviewer to lead the group by asking questions. In this experiment the researchers investigated how inexperienced users of Second Life viewed the virtual world, as well as the ways the standard Second Life Viewer software could be used by the same inexperienced users for malicious purposes such as griefing attempts. The experiment participants had only been introduced to Second Life a week prior to the day the experiment took place; thus they were only familiar with the standard actions and controls available in the Second Life environment. However, one of the participants was an experienced user who provided some insight into the Second Life world and helped other participants with technical difficulties.

The current study does not claim to represent any specific audience and should not be used for statistical purposes. The author does, however, encourage a quantitative study to be conducted on the topic, which would allow for a more extensive research, rendering statistically sound results.

6.2 Experiment Setup

Before the experiment was conducted, the proposal of the concept of the experiment and the experiment's techinical details were presented to the University of Pretoria EBIT Ethics Committee for approval. The proposal was examined and the experiment was approved by the committee. Appendix D lists the letter of approval received by the author.

The main purpose of the experiment was to explore the different ways that inexperienced Second Life users could perform griefing attacks, as well as to look at the possible ways of gathering evidence of these attacks via the standard Second Life viewer.

The reason griefing was chosen among all the other possible offences that take place in Second Life (see Table 5.1 in Chapter 5) is the fact that it is one of the most common offences encountered in online social spaces, as well as one of the easiest to reproduce in experimental conditions. However, due to the fact that there is a big variety of ways to perform griefing attacks, testing all of the variations of this offence in one experiment would not be feasible. Thus the participants were limited to the "physical" aspects of the offence, i.e. constraining other avatars' actions by restricting their movement in various possible ways, and disturbing their activity in-world.

The group of participants was divided into three sub-groups: "perpetrators","targets", and "investigators". The "perpetrators" were asked to engage their avatars in griefing attacks on the "targets", through the following actions: pushing "target" avatars, flying into them, "physically" obstructing their movement and activities, and creating objects in their way which would obstruct them. Being new to Second Life, the griefers were expected to figure out ways of disturbing the activities of the "targets" on their own. Seeing as most griefers are newbies [62], it is a relevant aspect to explore, in order to see the potential ways for a griefer to learn how to grief. The experienced participant in the group was also a part of the "perpetrators", essentially playing the "leader" role in the group of griefers. Group identity and ritualisation are regarded as common in griefer culture [10], [38], and having a similar dynamic in the author's experiment aided in replicating a more realistic setting of a griefing attack in a laboratory environment. The "target" avatars were asked to engage in building, using the primitive shapes available in the "Build" menu of the Second Life envorinment. They were also asked to explore the environment and find different ways to "fight off" the attacks from the "perpetrator" group. The "investigators" were the most independent of the three sub-groups: they were asked to observe all the avatars around them (including "perpetrator" avatars, "target" avatars, and other "investigator" avatars) and explore the possibilities for gathering evidence of the attacks on the "targets". At the start of the experiment the author suggested potential ways of evidence gathering, such as screenshots and video recordings; however, for the rest of the experiment the "investigators" worked on their own.

The experiment was conducted in a small computer laboratory with close to twenty-five seats, arranged in three rows. The computers were running Windows 7, and the

experiment participants explored Second Life through the standard Second Life Viewer, version 3.3.0.251182.

6.3 Procedure

Seeing as most of the participants were inexperienced in Second Life, and some of them would have been interacting with Second Life for the first time, the participants were offered a training session prior to the day of the experiment. During the training session the participants were guided through the process of registration and creating an account on the Second Life website [1], downloading and installing the standard Second Life viewer, as well as navigating inside the virtual world. The participants were asked to gather in one area in Second Life and explore the environment via interacting with the user interface of the viewer, as well as the virtual environment itself. Some of the participants explored the building tools of the Second Life viewer, others tried changing their avatar's appearance and chatting to other participants. The roles were explained to all the participants and some of them, designated to be "investigators", were asked to explore a bit more of Second Life in their own time before the day of the experiment.

The experiment was held on the second of May 2012, at the University of Pretoria, South Africa. The participants were not allocated specific seats and chose seats individually. They were allowed to sit next to each other and converse during the experiment, sharing their experiences with the rest of the group. They were also asked to sign informed consent forms before the experiment commenced (a sample form is provided in Appendix A). Just before the start of the experiment the overall procedure and participants' roles were explained once again, and each of the participants' computers was connected to the internet via a specified proxy. A number of technical difficulties were encountered at the start of the experiment. Having registered on the Second Life website and launched the Second Life viewer, some of the participants could not log in to the virtual world because the viewer did not accept their login information. This was due to an issue with the proxy used, and those participants who experienced difficulties were connected to the Internet using private credentials of the author and another fel-

[1] www.secondlife.com

low researcher. Mr K. Eloff, the experienced participant in the group, found a neutral ground for the experiment, where the participants would not be disturbed (and would not disturb Second Life residents not involved in the experiment) and the experiment would not be interfered with. It was a practice area, namely the parcel called "UMAD? Public Sandbox", which is located on a parcel called "Cool Story Bro". When all the participants were successfully logged into Second Life, Mr Eloff sent everyone a personal invitation to teleport to the public sandbox, and everyone was gathered together in a rather empty virtual space, with only the ground and the sky. "UMAD? Public Sandbox" is a practice area, thus no buildings remain there for more than five hours, and are returned to their owners' inventories when that time period expires. A recording was started through a computer screen recording program in order to capture the activity of the group of participants during the course of the experiment. However, due to the computer's memory constraints, the recording failed after an hour, and the existing video file turned out to be corrupted, rendering it unusable for the experiment analysis.

At the start of the experiment the "target" avatars were given a task to attempt to build a house using primitive shapes available to them in the "Build" menu in the Second Life viewer. The "perpetrators" were asked to begin their attacks, and the "investigators" were left to explore and gather evidence of what they saw. At first the participants had trouble identifying each other, which hindered the process slightly, seeing as the "investigators" were not sure whom to look out for, and the "perpetrators" did not know whether they are attacking the "targets" or their fellow griefers. However, through public chat visible to everyone in the area, as well as private messaging, the experiment participants familiarised themselves with the avatars of their fellow participants. The "targets" commenced their building tasks, aided by Mr Eloff when they experienced difficulties, and the "perpetrators" tried different ways of disrupting their activities. Due to lack of experience, the "perpetrators" had to spend some time figuring out how to attack the avatars around them. The "investigators" seemed to mostly use the snapshot tool from the Second Life viewer to gather evidence of the attacks. During the course of the experiment two of the participants had to leave, leaving only one "victim" to the "perpetrator" group. One of the participants changed their role and became part of the "victims". The offenders tried different ways of hindering the "victims", e.g. walking

on user-created objects. The "perpetrator" group also discovered the "no modify" and "no move" options on the objects created by others, which prevented them from deleting those objects. At one stage during the experiment a stranger avatar called "Loser Mode" joined the sandbox, stayed there for a while, and asked the group of participants on public chat about what they were busy with. One of the participants answered and said that it was an experiment. After that "Loser Mode" left. The experiment had been running for about two hours. At the end of the experiment every participant was given a brief questionnaire to complete (those who left earlier were asked to fill in the questionnaire just before leaving the premises). After completion the participants gave the questionnaires back to the author. One of the participants who played the role of an "investigator" also gave the author her personal detailed notes on her experiences and observations.

6.4 Results

The questionnaire given to the participants after they completed the experiment was focused on the participants' experiences and findings in-world, as well as their interactions with the Second Life viewer (see Appendix B for the sample quesionnaire). The author tried to see how inexperienced users perceived the virtual world, as well as the user interface (UI) of the Second Life viewer, seeing as a newbie attacked by a griefer would need to "fight off" the offender by using the actions and options available to them in the viewer. The questionnaire also contained questions with regards to the participants' opinions on the technical setup of the experiment, as well as allowed them to offer suggestions for improvement of possible future experiments.

Some participants found the navigation inside Second Life mildly difficult. They had to spend some time familiarising themselves with the camera controls, movement controls, object interaction, etc. "We were all not familiar enough with the environment", "More building training needed beforehand, as well as more camera control training" were some of the responses with regards to the environment interaction. The Second Life viewer navigation received similar responses from some of the participants. They only found it mildly easy, saying that they "did not know the interface (with all its menus)

well enough". One of the participants stated that "most of [them] were still familiarising [them]selves with the interface". However, not everyone had trouble navigating in Second Life. Some participants stated that they found both the environment and the interface navigation easy, and had no complaints or suggestions on the technical side. That clearly illustrates the fact that each person is different and perceives the virtual world differently. Even in this experiment's small group of participants the opinions differ significantly. The fact that a number of participants found the environment navigation and the interface navigation slightly challenging shows that newly registered residents might have trouble defending themselves against possible griefer attacks, not knowing which options of the interface to use to teleport away or even simply run away. However, seeing as the literature review showed that most griefers are newbies themselves, the complicated interface and environment navigation might hinder them in their actions, preventing them from finding ways to perform sophisticated attacks. That might possibly be one of the reasons the griefers often organise into groups and attack together; discussing it among themselves or finding an experienced griefer to be their leader, they figure out more complicated ways to disturb other people's Second Life activities.

Seeing as Second Life is a public space, even a deserted space like the "UMAD? Public Sandbox", used for the experiment, is open to everyone, and avatars not involved in the experiment could enter the sandbox at any time. The experiment questionnaire contained a question about the participants' encounters with stranger avatars, which received a couple of responses. As was mentioned in Section 6.3, a stranger called "Loser Mode" entered the sandbox and asked the participants on public chat about what they were doing. One of the participants commented on that encounter saying that "Loser Mode was just curious as to what our group of avatars was doing because there were primitive objects lying everywhere and we were all building" (see Figure 6.1). But, according to the participants' responses, Loser Mode was not the only stranger entering the sandbox during the running of the experiment. One of the participants mentioned an avatar called "JMMBC Okelli", saying "JMMBC Okelli flirted with my avatar. He was unaware that we were busy with a task!". As seen in Appendix C, JMMBC Okelli talked to one of the participants named Aladrinn, calling her "a beautiful lady". When planning the experiment, the researchers were concerned about the way people not involved in

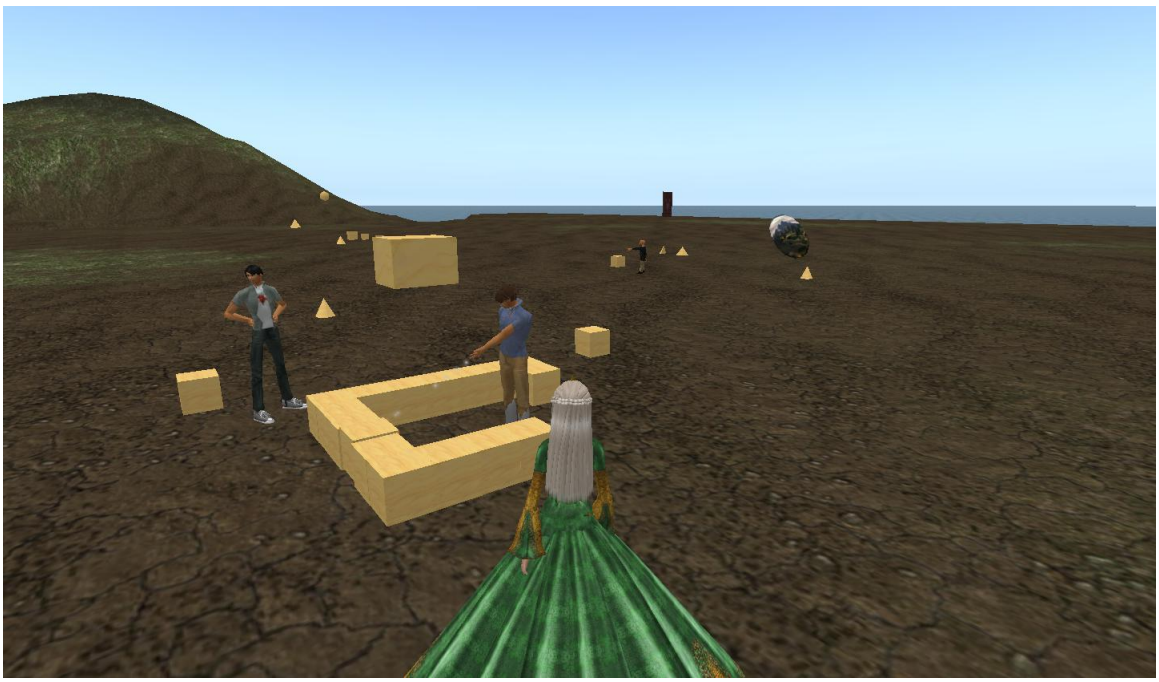

Figure 6.1: Experiment participants building in Second Life.

the experiment would react to a group of avatars attacking another group of avatars. That was the reason Mr. Eloff found the training ground "UMAD? Public Sandbox", which was unlikely to be visited by strangers. However, the strangers that did visit the group of participants did not hinder the experiment in any way, and were even friendly. Sometimes people online are seen as aggressive by default, due to the mostly fictional indentities and false feeling of permissiveness on the internet. However, even though that phenomenon does occur in the online world, most people are curious and willing to learn about the events and people around them. This might serve as indirect evidence of the fact that griefers in virtual worlds are more likely to be people with some or other psychilogical issues. Finding no rest in the real world, they would vent their insecurities and discontent in seemingly anonymous virtual environments.

Among the "interesting findings in-world" (see Appendix B) the participants mentioned a number of things. One of the participants' responses was the following: "I didnt crush when some avatar rolled an object over me. I think I am a strong guy". This shows that the user already learnt to relate to his virtual self, and was glad to see how his avatar

was able to undertake something that would never be possible in real life. Even in such short a time a person can get emotionally engaged with their avatar, so it comes as no surprise that some people start to really *live* in Second Life, as oposed to playing it as a game (refer to Section 4.5 of Chapter 4). Some participants listed building and environment navigation as examples of interesting findings. The participants engaged in building found that if an object is created as temporary it can disappear even if it is set to "no move" and "no modify". Thus residents new to Second Life must make sure that all objects they create are permanent. It is also a loophole which could be exploited by fraudsters in Second Life. If a new user decides to buy an object from someone, and they sell them a temporary object, the fraudster would receive the money and leave the buyer with an object that would disappear after a while. Another aspect of building that was discovered by experiment participants was the fact that even if the object is enabled for moving and modifying, it can be locked, so that other people couldnt edit it, thus protecting it from potential griefers. One of the participants also noted the following with regards to other people interacting with one's objects:

> "If you build an object and people / avatars interact with it by sitting on it (for instance), you can still continue modifying the object regardless of them interacting with it. However, their interaction disrupts the building process in that it is irritating and one cannot see a holistic view of one's object (because the people block your view)."

In fact, at one point during the experiment there was a "pile" of avatars on one participant's object, the purple cylinder (see Figure 6.2). The participant noted it in their findings: "I noticed that another user was able to climb up an object together with other users. In effect, you can "pile up" on an object". If a group of griefers disrupted one's building process by sitting on one of the objects it would not affect the building process as such; however, it would obscure the view of the object and thus make it inconvenient to build accurately. An offender could also build their object on top of one's object, thus obscuring the view. However, that could easily be avoided by moving the object away from the obstruction, as was noted by one of the participants. A more sophisticated way of disturbing someone's building is to fly high up in the air while "touching" someone else's object, and modifying it from a distance, as was listed in the findings of another

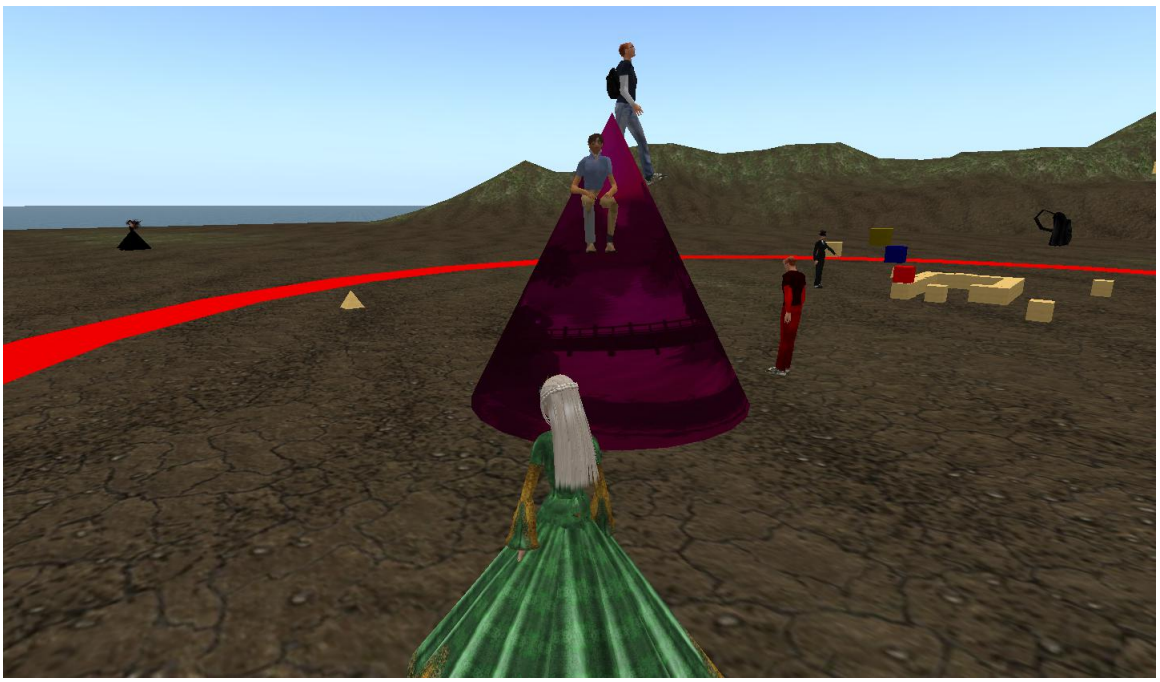

Figure 6.2: Avatars piling up on an object.

experiment participant. If the avatar who's object it was did not notice the offender touch the object and fly up, they would have trouble identifying the source of the disturbance. Finally, the third way of disturbing someone's building, as was discovered by the "perpetrator" group of participants, is to create small unnoticeable objects in-between someone else's objects. Building a complex structure in Second Life requires linking a couple of primitive objects. If there is an object in-between two objects that are to be linked the link would not be established. Thus creating unnoticeable disturbances on the ground might delay the building and frustrate the owner of the built structure.

In addition to the building, the participants also stated that they made use of the extra options (chat, user profile information, object information, etc.) available to them in the Second Life viewer, some to a lesser, some to a greater extent. All the participants worked with the "Basic" set of menu options, as it is a default setting for newly registered users. With regards to the chat function available in the Second Life viewer, one of the participants remarked that "having all [participants] in the same lab means people didn't use in-game communication tools unless asked". Nonetheless, they communicated

through both public chat and private chat, as was noted by one of the "investigators". This participant saved the chat log, which can be seen in Appendix C.

In addition to the chat log, this "investigator" participant gathered other information which could be useful as evidence, such as screenshots (Figures 6.1 and 6.2 were taken from the collection of screenshots taken by this participant), users' personal information available in their profiles (such as their screen names), offender avatars' appearances, as well as ownership of objects. While in a real griefing scenario the offenders might easily change their appearance not to be recognised later on, their screen names would not change, as it is their login name and it cannot be changed after registration in Second Life [129]. Finding the owner of an object through the object profile might be a very useful aspect of a digital forensic investigation in Second Life, especially with regards to fraud and illegally copied objects; the victim could attempt to trace the offender through the use of object profile information and all the data of the owner that is available there. Another piece of evidence that was mentioned by the participants was a screenshot of the abuse form in Second Life. It might be used as additional proof that someone committed an offence, if the screenshot is taken after the abuse form is filled in. It might also be useful as the proof of sending an abuse form to Linden Labs.

6.5 Conclusions

This chapter provided an overview of the experiment conducteds by the author on the second of May 2012 at the University of Pretoria, South Africa, in order to explore how inexperienced Second Life users perceived the virtual world, and reacted to griefing attacks. The experiment was also focused on the possible ways of gathering evidence of the griefing attacks from inside Second Life, using the standard Second Life viewer software. From the experiment results it is evident that the users' inexperience had constrained them to more basic attacks and defensive techniques. It is important for new users to familiarise themselves with both the environment navigation and the Second Life viewer they are using. It can help boost one's confidence in Second Life and combat the feeling of helplessness before experienced users, thus preventing some attacks the offenders usually aim at newcomers. It will also ensure that the user knows how to

react to an attack should they fall victim to any kind of griefing. The experiment also showed that potential griefers, inexperienced in Second Life, would not be able to effectively grief, since they would need to familiarise themselves with the environment and the user interface before they could cause any significant disturbance. Section 6.1 of this chapter provided an overview of the theory behind the decisions made by the researchers with regards to the experiment setup. Section 6.2 described the way the experiment was set up, namely the location, the software used, and the nature of the roles the participants played in the experiment. Section 6.3 described the experiment procedure, and mentioned the events and difficulties that occured during the running of the experiment. Section 6.4 presented the results of the experiment, which were gathered from the researchers' notes, the questionnaires given to the participants at the end of the experiment, as well as some additional files given to the researchers by the group of participants who played the roles of "investigators". The following chapter is focused on digital forensic techniques suggested by the author, which would be applicable to the Second Life environment.

Chapter 7

Digital Forensics in Second Life

In Chapter 2 the author presented and discussed their original digital forensic model, designed for a digital forensic investigation inside a virtual world, and Chapter 6 presented the experiment undertaken by the author in order to explore the possible ways of gathering evidence of offensive behaviour in Second Life. This chapter expands the discussion in the field of digital forensics in Second Life, providing a more detailed and more Second Life-specific overview of the digital forensic process model discussed in Chapter 2. The author focuses on two phases of the model, namely Collection and Preservation. These phases are considered the most relevant to the topic of evidence gathering, since in order to be used in an investigation the evidence has to be collected and preserved in its original state, ensuring its integrity. The author also provides a discussion on possible evidence gathering techniques, based on the information gathered from the experiment, as well as some ideas from the literature.

This chapter is organised as follows. Section 7.1 addresses the Collection phase of the digital forensic process model developed by the author, discussing the evidence gathering techniques applicable in the Second Life environment. Section 7.2 provides the overview of the Preservation phase, seeing as this phase differs the most from its "standard" computer forensics alternative. Section 7.3 concludes the chapter.

7.1 Collection

The Collection phase of the author's digital forensic process model (introduced in Chapter 2) consists of collecting all the available evidence from the virtual world system, as well as any other data that could serve as evidence. It is one of the most important phases in the process, since no evidence analysis can occur without prior data gathering. A number of well-known evidence gathering techniques such as analysis of removable devices (DVDs, flash drives, external HDDs), a scan for hidden files, or a search for deleted files, are commonly used in standard digital forensic investigations (e.g. computer forensics). However, not all of them are applicable to the Second Life environment. This section addresses the possible digital forensic techniques which could be utilised in a digital forensic process in Second Life, as well as mentions possible sources of evidence in the virtual world. However, the current study is focused on the activity inside the Second Life environment, thus the discussion only considers the possible sources of evidence and evidence gathering techniques which are available to a user logged in to Second Life through the standard Second Life viewer.

7.1.1 Sources of evidence

Before any evidence is gathered for analysis, the possible sources of evidence must be determined by the investigators. A number of sources are considered by the author. Screenshots of an incident (also referred to as "snapshots" [61]) are one of the most conspicuous sources of evidence of an in-world attack, available to Second Life residents in the standard Second Life viewer. The snapshot tool is easy to use, and the user can receive immediate results just by clicking the snapshot button. The tool can be really effective in cases such as defacing of an in-world object (e.g. a corporate building) since snapshots of the defaced object can be used as evidence of the attack. However, the snapshot tool is not a very efficient way of gathering evidence in the case of a violent griefing attack (e.g. an attack that involves pushing or "caging" - restricting an avatar's movement by creating a "cage" around them [132]), since the victim is typically only concerned with finding a way to escape the attack, and not gathering evidence against the offender(s). Nonetheless, should there be any witnesses to the attack, they could use

the snapshot tool to capture a still image of the surrounding area, as well as the avatars present in that area.

Another possible source of evidence in Second Life is video recordings, also called "machinima", which could be used in the same way as snapshots. Machinima is available to any Second Life resident; however, not all areas of Second Life are machinima-friendly [133]. Out of concern for intellectual property protection Linden Lab gives each landowner a choice whether to allow machinima on their property or not. If an attack occurs on a sim where machinima is not allowed neither the victim nor the witnesses would be able to record a video of the incident.

Objects possessed by the victim of the investigated offence could also serve as possible evidence. For example, if a perpetrator sexualy harassed the victim, they might have sent them objects and notecards with offensive messages inside. If the investigators receive those objects from the victim, they could analyse the metadata of those objects. The standard Second Life viewer is built to always show the initial creator of an object under the object's properties, thus it might be possible to find the creator based on the object's metadata.

The last source of evidence considered by the author in this study is chat logs. Public chat logs include all the conversations held by the avatars present in one sim, and private chat logs only contain private conversations between any two avatars. Any user can turn chat logging on or off. Choosing to turn the logging on lets the user save all the conversations they had - publicly and privately - in automatically generated log files, and store them in a designated folder on their computer. During a digital forensic investigation the investigators could receive chat logs relevant to the case from the witnesses of the incident, should they have any logs saved on their computers, and use them as evidence of the investigated offence. It is stated in Second Life's Terms of Service that no chat logs are allowed to be used without the consent of the parties involved [61], but by giving the investigators the log files the chat participants would have already granted their permission to use the chat logs for investigative purposes.

7.1.2 Techniques

Having considered possible in-world sources of evidence, some of the ways of gathering that evidence need to be looked at. Based on a discussion with a focus group (see Chapter 5, Section 5.4), the results of the experiment discussed in Chapter 6, as well as the results of research on the topic of offenses in virtual worlds, the author proposes three digital forensic techniques that would be applicable to Second Life, namely "virtual police", "private investigators", and "honeypots", in addition to more conventional ways of gathering evidence, such as interviewing the witnesses.

Virtual Police

"Virtual police" is a forensic technique which involves appointing people as police officers inside Second Life. These virtual policemen would serve the same purpose as policemen in real life, namely keeping order and making sure all avatars abide by the "laws", i.e. Second Life's Terms of Service. The avatars of virtual policemen could resemble real-life police by wearing police uniforms. However, seeing as police uniform differs from country to country, each "virtual country" could host its own group of virtual policemen, dressed according to that country's standards. "Virtual police" would not necessarily need to be present on all Second Life's islands at once, and at all times. That would not be a feasible solution, considering the number of people it would require, as well as the difference in time zones between different countries. However, "virtual police" would need to be prominent enough in the virtual world, so that potential offenders would realise they are putting themselves at risk of suspension or even banishment from Second Life should they violate the Second Life's code of conduct.

The author considers the "virtual police" technique to already be partially implemented in the world of Second Life. Moderator avatars (who are head managers of Linden Labs in real life), also referred to as "Lindens", visit various sims in Second Life from time to time, to answer questions and help other Second Life users. As administrators, their appearance on the scene is likely to make potential offenders restrain themselves from engaging in any anti-social activities. Linden officials are perceived by general public to be monitoring the Second Life areas even when their avatars are not present in those areas [51]. This aspect meets one of the abovementioned requirements

of "virtual police". However, even though the users assume the presence of a higher authority, Linded Lab does not assume such a monitoring position in Second Life and prefers the avatars to sort out all problems between themselves [61]. This is a drawback of the current Second Life "virtual police", since the potential offenders may ignore the Second Life rules even with Lindens around them. An in-world independent organisation, "The Green Lanterns", is also a realisation of the idea of "virtual police". It is a group of volunteer avatars who walk around the Second Life environment dressed in a uniform of the members of the Green Lantern Corps from the old comics about Green Lantern [62]. "The Green Lanterns" help new residents adjust to Second Life, report griefing, educate Second Life residents on security measures, and even provide security patrols during live events. A possible way of making "Green Lanterns" more prominent in Second Life could be promoting them in public areas and providing them with Linden Labs' support, e.g. building a "Green Lantern" police booth in most public areas of Second Life, to make potential griefers and other offenders feel constantly watched and assessed on their behaviour, thus potentially reducing the risk of attacks.

Private Investigators

A possible way to conduct an in-world investigation is to employ a "private investigator" - an individual with a standard, average appearance who would investigate suspicious areas of Second Life, and gather evidence of what they found. Such private investigators could also gather evidence of griefing attacks via snapshots and machinima, as discussed in Section 7.1.1, and provide this evidence to the relevant authorities. Once again, the author found that this technique has already been used before, during the ageplay investigation in the Wonderland incident (refer to Chapter 5, Section 5.3.4). During the author's discussion on criminal activity in Second Life with the focus group (Chapter 5, Section 5.4), the following procedure was proposed: if a person was suspected to be an offender, the private investigator could offer them a "gift", namely an object with a script attached to it. The script would serve as a GPS-tracking device, showing the investigator the location of the person in possession of the object, thus making it easy to track them. Evidently, a user experienced in Second Life would check what scripts the "gift" contained, and as a result would possibly dispose of it. Thus the proposed technique

would only be effective if the offender was an inexperienced Second Life resident. One concern that arised in conjunction with the proposed method was the privacy of an individual who would bes given the GPS-tracking object. It is not clear whether it is legal to track a person's location without the person's consent.

Honeypots

The author also proposes a forensic technique which involves creating a "honeypot" for potential perpetrators. The term "honeypot" had been used before in other branches of Computer Science. Mokube and Adams [79] define a honeypot as "a security resource whose value lies in being probed, attacked, or compromised". However, in this study a "honeypot" refers to a setting inside the Second Life environment, engineered specifically for the purpose of creating an illusion of an easy target for potential offenders. As was discussed in the previous chapters, new residents often fall victims to attacks. Due to being unfamiliar with the environment and the interface, new users easily believe anything more experienced users tell them, as well as are easily disrupted and confused. Taking that into consideration, the following application of the "honeypot" technique was considered: an investigator (an experienced Second Life resident) would disguise themselves as a newly registered user and spend time at one of the Introductory islands in Second Life. To make the setting more convincing, the investigator could ask questions on public chat and create an impression of being completely lost in the environment. Being an "easy target", the investigator could provoke potential perpetrators to take advantage of the "newbie", thus allowing the investigator to learn of the possible dangers for the new residents, and to think of the ways to prevent them. No implementation of this technique has yet been found in the world of Second Life. It is also not clear whether "honeypots" are a useful technique, seeing as the people involved in it would have to spend a lot of time inside Second Life with no guarantee of an encounter with an offender.

7.1.3 Some evidence gathering issues

Despite the use of advanced technology and software, digital forensic investigations hardly happen without hindrances and errors. The gathered evidence is not always easy

to collect, and at times even the slightest error might prove disastrous in this process. After the evidence has been collected, its integrity is also not a given. The evidence must undergo checks and tamper analysis before it can be analysed in conjunction with the investigated incident itself. This section addresses the issues digital forensic investigators face during the evidence gathering process.

One of the issues is the security concern arising in conjunction with Second Life snapshots and machinima. Being digital image files and video files, respectively, there is a possiblitity of the snapshots and video recordings being tampered with before they are collected by the investigators. Authenticity checks and tamper detection techniques have to be undertaken before the snapshots and the video recordings could be considered as reliable evidence. Another concern with regards to evidence gathering in Second Life is the so-called "bystander effect". According to Latané and Darley [63], the "bystander effect" refers to the likelihood of an individual to intervene in a public emergency situation, depending on the number of other bystanders known or thought to be co-witnesses to the incident. The research shows that a person is less likely to interfere if there are a lot of people co-witnessing the event [63]. A recent study by King, Warren, and Palmer [51] investigated the "bystander effect" in an online setting, using Second Life as a research platform. The authors attempted to test the validity of the "bystander effect" in a group of Second Life avatars witnessing an out-of-ordinary situation. An avatar named Thomas behaved in a deliberately provocative, disruptive, and sexually aggressive manner in front of a group of avatars, with one of the authors being a part of the group. At first Thomas did not harass any individuals specifically, and the observers did not attempt to stop him. Their comments suggested that the offensive behaviour was seen as "an amusing or juvenile anomaly" [51] rather than an offence ought to be stopped and reported as a violation of Second Life's Code of Conduct. However, as Thomas began attacking individuals, the group's response to his behaviour changed. The bystanders started mentioning "the authorities" who would come and evict him. However, none of the witnesses or the "victims" directly confronted Thomas, or tried to report him to Linden Labs themselves. The group of attacked individuals expected Thomas to be stopped by someone "in charge" instead of taking the matter into their own hands. Thus the authors prove that the "bystander effect" is as common in online communities of vir-

tual worlds as it is in real life, and not all victims / witnesses of offensive behaviour are willing to actively defend themselves from the perpetrators. This raises concerns with regards to gathering of evidence of such offences. Potential sources of evidence have been mentioned in Section 7.1.1, including snapshots and machinima. The latter can theoretically be collected from the witnesses or the victim(s) of the offence who recorded the events via the snapshot and machinima tools in the Second Life viewer. However, the presence of the "bystander effect" might mean that neither the victim(s) nor the witnesses collected any evidence of the offence, waiting for Second Life authorities to stop the perpetrator(s) instead.

7.2 Preservation

Section 7.1 discussed the Collection phase of the author's digital forensic process model. The next phase in the model is the preservation phase. Having investigated possible sources of evidence and collected the evidence from the Second Life system, the investigators would need to preserve the evidence in its original state, as well as validate it to prove its integrity, before the process of data analysis could be commenced. In addition to keeping the evidence in its original state, the preservation phase involves the duplication of the evidence, in order to work with the duplicates instead of the original files, to ensure the evidence integrity. This poses a question as to the way the duplication of evidence should be performed. Is the creation of exact copies of all evidence files enough to ensure the integrity of the data, or does the state of the location of the incident (in this case a virtual island) at the time it took place need to be captured as well? The topic of archiving of virtual worlds started receiving attention in the research community in the recent years [74], [89]. McDonough and Olendorf [74] attempted to archive certain regions of Second Life in order to identify the issues that arise with regards to archiving online user-created content. To achieve this, the authors followed a four-stage process. Firstly, they created a manifest which listed all the region's content, as well as provided general descriptive metadata of the objects in that region via the use of automated probes monitoring the region. Secondly, all the owners of the user-created content in that region were contacted with a request for permission of the archiving of

their creations. After permissions weres obtained, the authors proceeded to archiving the geometrical data of all the objects, along with their associated textures, via the CopyBot technology. CopyBot was briefly mentioned in Chapter 5, in conjunction with unauthorised copying of other people's objects. However, the study by McDonough and Olendorf shows that this software is a very useful tool for research purposes. CopyBot is a text-based Second Life client that allows one to download all the data of any chosen object (including detailed metadata such as ownership, shape, and other details) to their local computer. After copying all the available objects, the authors attempted to obtain additional metadata of all the region's content according to the OAIS reference model [74]. The model specifies five different types of information that can be obtained, namely descriptive information, context information, fixity information, representation information, and provenance information. Descriptive information lets the users find the needed objects in the archive. Context information consists of the links between specific objects and the environment they were present in. Fixity information (including authentication mechanisms and authentication keys) allows a user to assert the validity of the data and confirm that no unauthorised changes have been made to the archived content. Representation information is the digital information that can be converted into a format more understandable to the human eye (e.g. from bits to images or character data). Finally, provenance information is the history of the archived content. Having obtained all that information, the authors stored it in an XML file, which is easy to analyse and transfer. Finally, the authors archived the information that is impossible to collect via digital means, e.g. the way the current region is perceived by a human eye, its important properties, aspects, and events associated with it. Despite having archived quite a large part of each chosen region, a number of issues arose with regards to archiving of Second Life. The primary issue was the intellectual property present on the archived regions, which could not be archived without the owners' consent. Unfortunately, on average only 10% of all the owners contacted with regards to their property have responded to the authors' request and gave their permission for archiving of their content [74]. Some respondents denied the authors due to security concerns. Another issue encountered by the authors was the fact that the probe, which the initial region manifest's creation was based on, could get stuck at certain fluctuations of the region's terrain, as well as had a

limited radius of operation. Thus there was a possibility that some objects could get lost. The authors state that the overall process of archiving Second Life regions might take a long time, rendering it useless in need of urgent archiving of a region where an offence has been committed. However, should the research community find a more feasible way of archiving of Second Life regions, the process could prove to be an essential part of the preservation phase of any digital forensic process in Second Life, seeing as it would be one of the most reliable ways to ensure the data does not get lost or rendered invalid by unauthorised changes.

7.3 Conclusions

This chapter addressed the topic of performing digital forensics in Second Life and discussed the ways of evidence collection and possible sources of evidence. It is evident that digital forensic techniques, as applied to virtual worlds, have not yet been extensively studied or developed, and a lot of questions still arise with regards to technical challenges and privacy concerns of the forensic techniques presented in this chapter. However, it is the author's belief that the field of digital forensics has a lot of growth potential in the context of virtual world incidents, and various possibilities still exist for future research and development on this topic. The chapter focused on two phases of the digital forensic process model developed by the author (presented in Chapter 2), namely the collection phase and the presevation phase. The collection phase involves collecting the available evidence after identifying its possible sources. Section 7.1.1 discussed this topic and listed snaphots, machinima, objects in Second Life residents' possession, and public chat logs as possible evidence sources. Section 7.1.2 discussed the three digital forensic techniques suggested by the author, namely "virtual police", "private investigators", and "honeypots", as well as addressed the pros and cons of each. "Virtual police" is a technique involving certain individuals playing the same role as the real-life police, i.e. monitoring the environment and ensuring that no one breaks the rules (or Second Life's Terms of Service, in the current context). "Private investigators" are individuals sent to investigate problematic areas of Second Life without drawing attention to themselves, and blending with the crowd. Should any incident happen on site, the private investi-

gators would report it to the respective authorities. Finally, "honeypots" are artifically engineered settings in the Second Life environment that would attract potential perpetrators and provoke them to show their intentions. Section 7.1.3 addressed some issues that arise in conjunction with some of the evidence gathering techniques and evidence sources discussed in the previous sections, such as intellectual property concerns and the "bystander effect", where people are reluctant to intervene in a public emergency situation if they are part of a crowd. Section 7.2 focused on the preservation phase of the digital forensic model developed by the author, and presented a discussion on the possible archiving of Second Life regions where the investigated offences take place. Some issues, arising with regards to region archiving, were also addressed in this section. The following chapter concludes the current study and presents an overview of the results of the dissertation, as well as lists possible topics for future research.

Chapter 8

Conclusions

This chapter provides a summary of the conclusions of the current study, and lists a number of possible topics for future research. Section 8.1 lists the conclusions and shows how each objective of the study was met. Section 8.2 provides a list of possible topics for future research arising from this study.

8.1 Summary of Conclusions

One of the objectives of this work was to provide an overview of the field of Digital Forensics, including the different branches created in the field, and a number of digital forensic models available in the literature. Chapter 2 addressed this topic, providing a general overview of the field and its origins. It also discussed the different branches created in the field, namely Computer Forensics, Multimedia Forensics, Network Forensics, Software Forensics, and Database Forensics. A number of existing digital forensic models have been given an overview of and compared in terms of ther structure and the tasks associated with each phase of these models. The discussion on the existing digital forensic process models showed that there was no standard model for a digital forensic process, and not all aspects of the currently existing models were applicable to a digital forensic process conducted in a virtual world. Fulfilling another objective of the dissertation, the author developed a new digital forensic process model based on two detailed models, namely the DFRW model [94] and the Abstract model by Reith *et al* [108]. The

author examined each phase of those models and considered whether the tasks forming the phase were applicable to an investigation in a virtual world. As a result, the author presented an abstract model designed to be applicable to digital forensic investigations in virtual worlds.

The phases of the author's model are as follows: identification, collection, preservation, examination, analysis, presentation, and decision. The identification phase involves studying the crime scene and determining the type of crime that took place, based on the evidence available at the crime scene. The collection phase consists of collecting all the available evidence from the virtual world system, as well as from the possible interviewees. During this phase the investigators should also identify, locate, and collect any other data that could serve as evidence, as well as document all the findings up to this point. The preservation phase involves keeping the evidence in its original state, as well as duplicating it so that the investigators could work with the duplicates instead of the original files, to preserve the integrity of the evidence. The examination phase consists of sorting the data and reducing it to only the evidence relevant to the incident (in case there is irrelevant data present). The analysis phase requires the investigators to determine the validity of the used data, as well as perform forensic analysis on the validated data. Various applicable techniques for data analysis should be applied during this phase, e.g. data mining, pattern matching, or statistical analysis. During the presentation phase the resulting findings should be documented in detail, and the results should be statistically interpreted. Finally, the decision phase requires making a decision as to which country's laws (or, perhaps, "virtual laws") are to be followed, should the offender be found and proven guilty by the evidence analysis. Section 8.2 addresses this as one of the topics for future research.

Providing an overview of virtual worlds was also one of the objectives of this study. Chapter 3 discussed the definitions of the terms "virtual environment", "virtual reality", and "virtual world", as well as the differences between them. The author showed that there was no standard definition of the notion of "virtual world", and presented their own definition, based on the definitions from the literature. The author defines the term "virtual world" as an immersive environment which consists of a synchronous, persistent network of people, represented as avatars, facilitated by networked computers. The

chapter also listed and discussed the characteristics common to various types of virtual worlds, as well as the security threats posed by the virtual worlds. Another objective of the dissertation was to provide an overview of Second Life, and show what makes it stand out among the rest of the virtual worlds available online. Chapter 4 discussed the history of the making of Second Life, and looked at four aspects of Second Life, namely Second Life as a game, as a social network, as an economy, and as an alternative life. The chapter showed how differently various Second Life residents see the virtual world, and what a diverse community Second Life has developed, which making the virtual world unique and interesting.

Another objective of this work was to map real-world offences to Second Life and derive Second Life alternatives of those offences. Chapter 5 presented a list of real-life offences, based on South African law, together with their alternatives in Second Life. Some Second Life alternatives of real-life offences are quite different in the Second Life context, due to the fact that some actions (e.g. poisoning) are not applicable in virtual worlds. Mapping some offences to the Second Life environment proved to be challenging. It is a debatable topic whether some offences retain their severity when applied to a virtual world context; killing an avatar inside a virtual world where the owner can re-create it at any time cannot be put on the same level of severity as murder in real life. Section 8.2 addresses this as one of the topics for future research. The authors also presented a classification of the offences according to the subject of the offence, presented in Table 5.1. The table shows the pre-requisites for each offence, its Second Life alternative (if applicable), as well as an indication if the offence can be committed "inside" the virtual world, i.e. through the Second Life viewer's interface, without the aid of any external devices or software. The latter factor was an important characteristic to consider, seeing as the dissertation was focused on the offences committed inside the virtual world. The author underlined the significance of this factor. The goal of the current study was to explore the ways inexperienced users of Second Life experienced offensive behaviour, and the ways the evidence of those offences could be gathered through the Second Life viewer itself. The literature review showed that inexperienced users were the ones who would be more likely to fall victims to offences such as griefing or harassment, thus it was important to explore ways of gathering evidence through the standard Second Life

viewing software, seeing as it was the default software for every new resident. Evidence gathering and digital forensic techniques "outside" of the Second Life environment were mentioned as possble topics for future research.

Having considered some of the possible offences applicable inside Second Life, the next objective of the author was to conduct an exploratory experiment on griefing in Second Life. The reason griefing was chosen among other possible offences is the fact that it is one of the most common offences encountered in online social spaces, as well as one of the easiest to reproduce in experimental conditions. The author conducted the experiment in a small group of people to find the ways griefing could be committed in Second Life, as well as how inexperienced users could protect themselves from griefing attacks. Another object of the experiment was to find possible sources of evidence, and ways of collecting the evidence from inside the standard Second Life viewer. The results showed that most griefing attacks were performed via the interaction with the objects another person was building, as well as pushing other avatars around in the environment. To counteract griefing attacks, one could lock one's objects or move them to another location, as well as teleport away from the griefer. Among the ways of gathering evidence the researchers listed scanning public and private chat logs, as well as looking at objects' metadata and user profile information.

Finding possible sources of evidence for offences committed inside Second Life was one of the main objectives of this study. Chapter 7 listed a number of them, namely screenshots (also called "snapshots"), machinima (video recordings created inside the Second Life environment), public and private chat logs, as well as users' inventories. Pros and cons of each source of evidence were addressed and discussed. The last objective of the dissertation was to present a number of possible digital forensic techniques to investigate offences in Second Life. The author presented three main forensic techniques applicable in Second Life, namely "virtual police", "private investigator", and "honeypot". "Virtual police" involves having a designated group of people to monitor various areas in Second Life and keep order, as well as look for any residents breaking Second Life's Code of Conduct, and report them to Second Life. The "private investigator" technique involves having a person visit suspicious areas/gatherings in Second Life, pretending to be a part of events, scanning the areas for any unlawful activity, and

reporting the findings. The "honeypot" technique involves creating a setting inside the Second Life environment, engineered specifically for the purpose of creating an illusion of an easy target for potential offenders, thus luring them in and thus learning potential dangers for inexperienced newcomers in the Second Life world. The first two techniques appeared to have been implemented before; however, the "honeypot" technique is still to be put into action and measured on its usability and feasibility.

8.2 Future Work

A number of possible future research topics have emerged from this study, and are briefly discussed in this section.

One of the possible topics for future research could be the analysis of the offences listed in Table 5.1 which were not discussed in this dissertation. The encounters of those offences in Second Life, as well as possible ways of preventing the offences, could be considered. The current study also showed that in virtual worlds the line between a simple irritation and a formal offence is not clearly defined and requires clarification. Future research could address this topic and provide a discussion on the difference between various offences in Second Life and their emotional, as well as practical impact on the residents (e.g. a resident losing money due to a fraudulent transaction in Second Life). Another possible future research topic is Second Life law. Currently Linden Labs do not provide Second Life residents with any laws except the Code of Conduct, violations of which do not make any resident legally responsible. It is a great security concern and needs to be addressed by the research community. Virtual laws applicable to Second Life or Second Life-specific laws could be developed and experimented with. Another topic to be considered for future research is griefing, and possible ways for Linden Labs to regulate griefing in Second Life, issuing some more advanced forms of punishment for those offenders who cause serious harm with their griefing activity. Expansion of the experiment conducted by the author in the current study is also a possibility for future research. A bigger group of participants could be invited, making the results more statistically sound. The experiment could also focus on a group with a specific characteristic, or a certain level of Second Life experience, providing insights into Second Life activity of the respective

groups of users. Instead of focusing on in-world offences, future researchers could address offences commmitted via external devices and software. The evidence sources and evidence gathering techniques could also include external sources such as output from network monitoring software or interviews with Second Life residents in real life. Future research could also address the techniques for a digital forensic investigation in Second Life, and attempt to implement them in the virtual world. An experiment could be conducted, exploring the usability and feasibility of these techniques.

8.3 Derived Publications

The following publications have been derived from this dissertation:

- A. Rakitianskaia, M. Olivier, and A. Cooper. Nature and forensic investigation of crime in second life. In *Proceedings of the 10th International Conference on Information Security for South Africa*, 2011.

Bibliography

[1] R. Abu Hana, C. Freitas, L. Oliveira, and F. Bortolozzi. Crime scene classification. In *Proceedings of the 2008 ACM symposium on Applied computing*, pages 419–423. ACM, 2008.

[2] A. Adams, C. Wankel, and S. Malleck. *Emerging Ethical Issues of Life in Virtual Worlds – Virtual sex with child avatars (Chapter 10)*. Information Age Publishing, 2010.

[3] A. Adrian. Intellectual property or intangible chattel? *International Journal of Intercultural Information Management*, 1(4):331–343, 2009.

[4] A. Adrian. Beyond griefing: Virtual crime. *Computer Law & Security Review*, 26(6):640–648, 2010.

[5] J. Allee. *Webster's dictionary*. Galahad Books, 1975.

[6] A. Ariffin, K.-K. Choo, and J. Slay. Digital camcorder forensics. In *Proceedings of the Eleventh Australasian Information Security Conference-Volume 138*, pages 39–47. Australian Computer Society, Inc., 2013.

[7] M. Ashton and C. Verbrugge. Measuring cooperative gameplay pacing in world of warcraft. In *Proceedings of the 6th International Conference on Foundations of Digital Games*, FDG '11, pages 77–83, New York, NY, USA, 2011. ACM.

[8] W. Au. Tax revolt in americana! Available at: http://nwn.blogs.com/nwn/2003/09/tax_revolt_in_a.html (Accessed: 26 May 2013).

[9] W. Au. Copying a controversy, 2012. Available at: http://nwn.blogs.com/nwn/2006/11/second_life_clo.html (Accessed: 06 Jan. 2013).

[10] B. B. Spectacular interventions in second life: Goon culture, griefing, and disruption in virtual spaces. *Journal of Virtual Worlds Research*, 1(3), 2009.

[11] M. W. Bell. Toward a definition of virtual worlds'. *Journal of Virtual Worlds Research*, 1(1):1–5, 2008.

[12] P. Black, T. Hartzenberg, and B. Standish. *Economics: Principles and Practice. A South African Perspective*. Pearson Education South Africa, 2001.

[13] R. Böhme, F. Freiling, T. Gloe, and M. Kirchner. Multimedia forensics is not computer forensics. *Computational Forensics*, pages 90–103, 2009.

[14] d. m. boyd and N. B. Ellison. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1):210–230, 2007.

[15] F. P. Brooks. What's real about virtual reality? *IEEE Comput. Graph. Appl.*, 19(6):16–27, Nov. 1999.

[16] E. Brown and P. Cairns. A grounded investigation of game immersion. In *Proceedings of the Premier International Conference for Human-Computer Interaction*, Vienna, Austria, 2004.

[17] J. Brownlee. John edwards meets second life 'feces spewing obscenity'. Wired, 2007. Available at: http://www.wired.com/table_of_malcontents/2007/03/john_edwards_me/ (Accessed: 06 Jan. 2013).

[18] M. Caloyannides. *Computer forensics and privacy*. Artech House Publishers, 2001.

[19] E. Casey. *Handbook of computer crime investigation: forensic tools and technology*. Elsevier Academic press, London, UK, 2002.

[20] E. Castronova. Virtual worlds: A first-hand account of market and society on the cyberian frontier, 2001.

[21] E. Castronova. *Synthetic worlds*. The University of Chicago Press, Chicago, USA, 2004.

[22] CEOP. Threat assessment of child sexual exploitation and abuse, 2013. Available at: http://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf (Accessed: 04 2014).

[23] T. Chesney, I. Coyne, B. Logan, and N. Madden. Griefing in virtual worlds: causes, casualties and coping strategies. *Information Systems Journal*, 19(6):525–548, 2009.

[24] R. Chisholm and M. McCarty. *Principles of Economics*. Scott, Foresman, 1978.

[25] D. Clark. South african law reform commission issue paper 22 project 130: Stalking. 2003.

[26] A. Cockburn and B. McKenzie. Evaluating the effectiveness of spatial memory in 2d and 3d physical and virtual environments. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 203–210. ACM, 2002.

[27] T. Conklin. Method or madness phenomenology as knowledge creator. *Journal of Management Inquiry*, 16(3):275–287, 2007.

[28] V. Corey, C. Peterman, S. Shearin, M. Greenberg, and J. Van Bokkelen. Network forensics analysis. *Internet Computing, IEEE*, 6(6):60–66, 2002.

[29] S. Decker. Second life scam !!!! [msg 01], 2012. Message posted to http://www.sluniverse.com/php/vb/general–sl–discussion/70098–second–life–scam.html (Accessed: 05 Jan. 2013).

[30] N. Denzin and Y. Lincoln. *The Sage handbook of qualitative research*. Sage Publications, Incorporated, 2005.

[31] K. Derrickson. Second life and the sacred: Islamic space in a virtual world. *Digital Islam*, 2008.

[32] M. W. C. Dictionary. Merriam-webster. *Incorporated, 10th edition edition*, 1996.

[33] Diplo. Virtual embassy - maldives, 2007. Available at: http://archive1.diplomacy.edu/DiplomacyIsland/Embassies/display.asp?Topic=Maldives (Accessed: 10 2013).

[34] D. Douglass. Cyberself: The emergence of self in on-line chat. *The Information Society*, 13(4):375–397, 1997.

[35] G. e. a. Dunnet. Realism meets virtual reality. In *Real World Visualisation - Virtual World - Virtual Reality, IEE Colloquium on*, pages 6/1–6/4, London, England, 1991.

[36] J. Farrell. Investigation: Paedophilia and second life, 2011. Available at: http://news.sky.com/story/898210/investigation-paedophilia-and-second-life (Accessed: 03 2014).

[37] J. Fernandez, S. Smith, M. Garcia, and D. Kar. Computer forensics: a critical need in computer science programs. *Journal of Computing Sciences in Colleges*, 20(4):315–322, 2005.

[38] C. Foo and E. Koivisto. Defining grief play in mmorpgs: player and developer perceptions. In *Proceedings of the 2004 ACM SIGCHI International Conference on Advances in computer entertainment technology*, pages 245–250. ACM, 2004.

[39] K. Fowler. Sql server database forensics. *Blackhat USA briefings and training*, 2007.

[40] P. Fruhwirt, M. Huber, M. Mulazzani, and E. Weippl. Innodb database forensics. In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on*, pages 1028–1036. IEEE, 2010.

[41] S. Garfinkel. Network forensics: Tapping the internet. *IEEE Internet Computing*, 6:60–66, 2002.

[42] G. Garvey. Dissociation and second life: Pathology or transcendence? *Technoetic Arts*, 8(1):101–107, 2010.

[43] E. Goffman. The presentation of self in everyday life. 1959. *Garden City, NY*, 2002.

[44] A. Gray, P. Sallis, and S. MacDonell. Software forensics: Extending authorship analysis techniques to computer programs. 1997.

[45] A. Guinchard. Crime in virtual worlds: The limits of criminal law. *International Review of Law, Computers & Technology*, 24(2):175–182, 2010.

[46] C. Haugtvedt, K. Machleit, and R. Yalch. *Online consumer psychology: understanding and influencing consumer behavior in the virtual world*. Advertising and consumer psychology. LAWRENCE ERLBAUM ASSOC Incorporated, 2005.

[47] K. Hunt. This land is not your land: Second life, copybot, and the looming question of virtual property rights. *Tex. Rev. Ent. & Sports L.*, 9:141, 2007.

[48] D. Johnson. Ethics online. *Communications of the ACM*, 40(1):60–65, 1997.

[49] M. Johnson and K. Rogers. Too far down the yellow brick road cyber-hysteria and virtual porn. *Journal of International Commercial Law and Technology*, 4(1):61–70, 2009.

[50] Y. Kafai, D. Fields, and M. Cook. Your second selves: avatar designs and identity play in a teen virtual world. In *Digital Games Research Association Conference*, pages 1–9, 2007.

[51] T. King, I. Warren, and D. Palmer. Would kitty genovese have been murdered in second life? researching the "bystander effect" using online technologies. In *TASA 2008: Re-imagining sociology: the annual conference of The Australian Sociological Association*, pages 1–23. University of Melbourne, 2012.

[52] R. Kluft, L. E. Michelson, and W. E. Ray. Dissociative identity disorder. pages 337–366, 1996.

[53] R. Koster. Online feuds a big headache. WIRED NEWS, 2004. Available at: http://www.wired.com/news/games/0,2101,65562,00.html (Accessed: 02 Jan. 2013).

[54] R. Koster. A virtual world by any other name? [msg 21], 2004. Message posted to http://terranova.blogs.com/terra_nova/2004/06/a_virtual_world.html (Accessed: 11 Feb. 2012).

[55] A. Kring, S. Johnson, G. Davison, and J. Neale. *Abnormal psychology*. Wiley, 2009.

[56] W. Kruse II and J. Heiser. *Computer forensics: incident response essentials*. Addison-Wesley Professional, 2001.

[57] C.-A. La and P. Michiardi. Characterizing user mobility in second life. In *Proceedings of the first workshop on Online social networks*, pages 79–84. ACM, 2008.

[58] L. Lab. New transaction history. Available at: http://wiki.secondlife.com/wiki/New_Transaction_History (Accessed: 10 May 2014).

[59] L. Lab. Permissions. Available at: http://wiki.secondlife.com/wiki/Permission (Accessed: 24 Aug. 2014).

[60] L. Lab. Second life community standards. Available at: http://secondlife.com/corporate/cs.php (Accessed: 02 Jan. 2013).

[61] L. Lab. Second life terms of service. Available at: www.secondlife.com/corporate/tos.php (Accessed: 28 Dec. 2012).

[62] T. G. Lanterns. Griefers in second life. Second Life anti-griefer group. Available at: http://thegreenlanterns.wordpress.com/2011/01/02/welcome–to–the–blog/ (Accessed: 09 Jan. 2013).

[63] B. Latane and J. Darley. *The unresponsive bystander: Why doesn't he help?* Appleton-Century Crofts New York, 1970.

[64] C. Lee. Understanding security threats in virtual worlds. In *AMCIS*, page 466, 2009.

[65] F. Linden. Linden lab official: Death and other worries outside second life. Available at: http://wiki.secondlife.com/wiki/Linden_Lab_Official:Death_and_other_worries_outside_Second_Life (Accessed: 26 May 2013).

[66] J. Linden. Friends and partnering, 2012. Available at: http://community.secondlife.com/t5/English–Knowledge–Base/Friends–and–partnering/ta–p/700067#Section_.3.2 (Accessed: 24 Aug. 2014).

[67] J. Linden and R. Linden. Usernames and display names, 2011. Available at: http://community.secondlife.com/t5/English–Knowledge–Base/Usernames–and–display–names/ta–p/700173 (Accessed: 23 Feb. 2012).

[68] G. Llewelyn. First church of rosedale. Available at: https://my.secondlife.com/groups/2e650b89-14cd-4ded-4113-d68ac99f2d2d?username=gwyneth.llewelyn (Accessed: 26 May 2013).

[69] Z. Lynch. Second life: Combat. Available at: http://wiki.secondlife.com/wiki/Combat (Accessed: 26 May 2013).

[70] N. Malamuth and M. Huppin. Drawing the line on virtual child pornography: bringing the law in line with the research evidence. *N.Y.U. Review of Law and Social Change*, 31:773–827, 2007.

[71] B. Mann. Social networking websites–a concatenation of impersonation, denigration, sexual aggressive solicitation, cyber-bullying or happy slapping videos. *International Journal of Law and Information Technology*, 17(3):252–267, 2009.

[72] A. Marcella Jr and F. Guillossou. *Cyber forensics: From data to digital evidence*, volume 623. John Wiley & Sons, 2012.

[73] M. McCann. History of second life. Available at: http://wiki.secondlife.com/wiki/History_Of_Second_Life (Accessed: 26 May 2013).

[74] J. McDonough and R. Olendorf. Saving second life: Issues in archiving a complex, multi-user virtual world. *International Journal of Digital Curation*, 6(2):89–108, 2011.

[75] J. McDowell and G. Novis. The consequences of money laundering and financial crime. *Economic Perspectives*, 6(2):6–10, 2001.

[76] M. Meadows. *I, Avatar: The culture and consequences of having a second life*. New Riders Pub, 2007.

[77] C. Meek-Prieto. Just age playing around-how second life aids and abets child pornography. *NCJL & Tech.*, 9:88, 2007.

[78] A. Mislove, M. Marcon, K. Gummadi, P. Druschel, and B. Bhattacharjee. Measurement and analysis of online social networks. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, pages 29–42. ACM, 2007.

[79] I. Mokube and M. Adams. Honeypots: concepts, approaches, and challenges. In *Proceedings of the 45th annual southeast regional conference*, pages 321–326. ACM, 2007.

[80] S. Morris. Second life affair leads to real life divorce, 2008. Available at: http://www.guardian.co.uk/technology/2008/nov/13/second–life–divorce (Accessed: 23 Feb. 2012).

[81] S. Morris. Second life affair leads to real life divorce, 2008. Available at: http://www.guardian.co.uk/technology/2008/nov/13/second-life-divorce (Accessed: 26 May 2013).

[82] F. Mouton and H. Venter. A prototype for achieving digital forensic readiness on wireless sensor networks. In *AFRICON, 2011*, pages 1–6, Sept 2011.

[83] F. Mouton and H. Venter. Requirements for wireless sensor networks in order to achieve digital forensic readiness. In N. Clarke and T. Tryfonas, editors, *6th International Workshop on Digital Forensics and Incident Analysis*, pages 108–121, London, UK, July 2011.

[84] J. Mulligan and B. Patrovsky. *Developing online games: An insider's guide*. New Riders Pub, 2003.

[85] J. Nah, J. Kim, and J. Kim. Video forensic marking algorithm using peak position modulation. *Applied Mathematics & Information Sciences*, 7(6), 2013.

[86] J. Nechvatal. *Immersive Ideals / Critical Distances : Study of the Affinity Between Artistic Ideologies in Virtual Reality and Previous Immersive Idioms*. LAP Lambert Academic Publishing AG & Co KG, 2010.

[87] B. Nelson, A. Phillips, and C. Steuart. *Guide to computer forensics and investigations*. Course Technology Ptr, 2010.

[88] C. Neustaedter and E. Fedorovskaya. Presenting identity in a virtual world through avatar appearances. In *Proceedings of Graphics Interface 2009*, GI '09, pages 183–190, Toronto, Ont., Canada, Canada, 2009. Canadian Information Processing Society.

[89] J. Newman. (not) playing games: Player-produced walkthroughs as archival documents of digital gameplay. *International Journal of Digital Curation*, 6(2):109–127, 2011.

[90] D. OHara. Religion in second life. Available at: http://ganymedescostagravas.wordpress.com/2008/11/12/religion-in-second-life-by_danni_ohara/ (Accessed: 26 May 2013).

[91] M. Olivier. On metadata context in database forensics. *Digital Investigation*, 5(3):115–123, 2009.

[92] T. W. G. on Crime Scene Investigation. Electronic crime scene investigation: A guide for first responders. 2001.

[93] F. Paine. Dealing with griefers. Available at: http://wiki.secondlife.com/wiki/User Fr43k_Paine/Dealing_With_Griefers (Accessed: 04 Jan. 2013).

[94] G. Palmer. A road map for digital forensics research-report from the first digital forensics research workshop (dfrws). *Utica, New York*, 2001.

[95] J. Pearsall and P. Hanks. *The new Oxford dictionary of English*. Clarendon Press, 1998.

[96] S. Peisert, M. Bishop, and K. Marzullo. Computer forensics in forensis. In *Systematic Approaches to Digital Forensic Engineering, 2008. SADFE'08. Third International Workshop on*, pages 102–122. IEEE, 2008.

[97] E. Pilli, R. Joshi, and R. Niyogi. A generic framework for network forensics. *International Journal of Computer Applications IJCA*, 1(11):1–6, 2010.

[98] A. Piva. An overview on image forensics. *ISRN Signal Processing*, 2013, 2013.

[99] W. Porter. Exclusive interview with second life liberation army leader (slla), 2006. Available at: http://www.revenews.com/internet-strategy/exclusive-interview-with-second-life-liberation-army-leader-slla (Accessed: 06 2013).

[100] J. Prothero and H. Hoffman. Widening the field-of-view increases the sense of presence in immersive virtual environments. *Human Interface Technology Laboratory Technical Report TR-95*, 2, 1995.

[101] A. Rakitianskaia. Lurking evil, 2014. Available at: http://leg-o-lass.deviantart.com/art/Lurking-evil-481885183 (Accessed: 12 2014).

[102] A. Rakitianskaia, M. Olivier, and A. Cooper. Nature and forensic investigation of crime in second life. In *Proceedings of the 10th International Conference on Information Security for South Africa*, 2011.

[103] F. Ramalho and G. Santos. A parametric analysis and classification of quests in mmorpgs. In *Proceedings of SBGames 2012*. Federal University of Pernambuco, Brazil, 2012.

[104] M. Ranum. Network flight recorder. *Inc. Intrusion Detection: Challenges and Myths*.

[105] M. Ranum, K. Landfield, M. Stolarchuk, M. Sienkiewicz, A. Lambeth, and E. Wall. Implementing a generalized tool for network monitoring. *Information Security Technical Report*, 3(4):53–64, 1998.

[106] C. Reeves. Fantasy depictions of child sexual abuse: The problem of ageplay in second life. *Journal of Sexual Aggression*, 19(2):236–246, 2013.

[107] R. Reis, P. Escudeiro, and N. Escudeiro. Comparing social virtual worlds for educational purposes. In *Advanced Learning Technologies (ICALT), 2010 IEEE 10th International Conference on*, pages 186–190. IEEE, 2010.

[108] M. Reith, C. Carr, and G. Gunsch. An examination of digital forensic models. *International Journal of Digital Evidence*, 1(3):1–12, 2002.

[109] H. Rheingold. *The virtual community*. Citeseer, 1995.

[110] Y. Riabinin. Do night elves dream of virtual gold? a study of virtual economies in online games. 2012.

[111] S. Rider. *Hour: 720. A Massively Multiplayer Experience*. ProQuest, 2006.

[112] J. Rossignol. A deadly dollar. *The Escapist*, 19:18–22, 2005.

[113] K. Rufer-Bach. *The Second Life grid: the official guide to communication, collaboration, and community engagement*. Sybex, 2009.

[114] P. Samuelson. Information as property: Do ruckelshaus and carpenter signal a changing direction in intellectual property law? *Cath. UL Rev.*, 38:365, 1988.

[115] P. Savvas, B. Michael, and L. Feng. Making real money in virtual worlds: {MMORPGs} and emerging business opportunities, challenges and ethical implications in metaverses. *Technological Forecasting and Social Change*, 75(5):610 – 622, 2008.

[116] R. Schroeder. Defining virtual worlds and virtual environments. *Journal of Virtual Worlds Research*, 1, 2008.

[117] S. A. P. Service. Common law offences.

[118] R. Slade. *Software Forensics*. McGraw-Hill Professional, 2004.

[119] P. Smith, J. Mahdavi, M. Carvalho, S. Fisher, S. Russell, and N. Tippett. Cyberbullying: Its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, 49(4):376–385, 2008.

[120] E. Spafford and S. Weeber. Software forensics: Can we track code to its authors? *Computers & Security*, 12(6):585–595, 1993.

[121] P. Steiner. On the internet, nobody knows you're a dog. The New Yorker, 1993. The caption for Steiner's July 1993 single-panel cartoon.

[122] P. Stephenson. The forensic investigation steps. *Computer Fraud & Security*, 2002(10):17–19, 2002.

[123] A. Stevenson and M. Waite. *Concise Oxford English Dictionary: Main Edition*. OUP Oxford, 2011.

[124] A. Studios. Anshe chung becomes first virtual world millionaire. *Online: http://www.anshechung.com (Accessed: 05 Jan. 2013)*, 2006.

[125] N. T. Linden lab responds to wonderland scandal, 2007. Available at: http://www.yellodyno.com/pdf/Linden_Lab_Wonderland_Scandal.pdf (Accessed: 10 May 2014).

[126] N. Tateru. The virtual whirl: A brief history of second life (2002-2003). Available at: http://massively.joystiq.com/2010/06/26/the-virtual-whirl-a-brief-history-of-second-life-2002-2003/ (Accessed:
26 May 2013).

[127] Tyabela. This is a scam i think [msg 01], 2012. Message posted to http://www.sluniverse.com/php/vb/general–sl–discussion/71535–scam–i–think.html (Accessed:
05 Jan. 2013).

[128] D. Warner and M. Raiter. Social context in massively-multiplayer online games (mmogs): ethical questions in shared space. *International Review of Information Ethics*, 4(7), 2005.

[129] B. White. *Second Life: A Guide to Your Virtual World*. Que, Washington, USA, 2008.

[130] S. L. Wiki. Did friendship circle, 2009. Available at: http://wiki.secondlife.com/wiki/DID_friendship_circle (Accessed: 17 2013).

[131] S. L. Wiki. Declaration of avatar rights, 2013. Available at: http://wiki.secondlife.com/wiki/Declaration_of_Avatar_Rights (Accessed:
2 May 2014).

[132] S. L. Wiki. Cage, 2014. Available at: http://wiki.secondlife.com/wiki/Cage (Accessed: 28 Aug. 2014).

[133] S. L. Wiki. Machinima, 2014. Available at: http://wiki.secondlife.com/wiki/Machinima (Accessed: 28 Aug. 2014).

[134] S. L. Wiki. Zindra, 2014. Available at: http://wiki.secondlife.com/wiki/Zindra (Accessed: 4 May 2014).

[135] R. Wilson. Sex play in virtual worlds. *Washington and Lee Law Review*, 66(3):1127, 2012.

[136] H. Yamaguchi. An analysis of virtual currencies in online games. *Social Science Research Network*, 2004.

[137] P. Yu. Intellectual property and the information ecosystem. *Michigan State Law Review*, 2005:1–20, 2005.

Appendix A

Informed Consent Form

The following is the informed consent form which every experiment participant signed before the experiment was commenced.

Informed consent form

(Form for research subject's permission)

(Must be signed by each research subject, and must be kept on record by the researcher)

1 Title of research project: **Digital Forensics in Second Life**

2 I, _____, hereby voluntarily grant my permission for participation in the project as explained to me by Ms. A. S. Rakitianskaia.

3 The nature, objective, possible safety and health implications have been explained to me and I understand them.

4 I understand my right to choose whether to participate in the project and that the information furnished will be handled confidentially. I am aware that the results of the investigation may be used for the purposes of publication.

6 Upon signature of this form, you will be provided with a copy.

Signed: _____ Date: _____

Witness: _____ Date: _____

Researcher: _____ Date: _____

Appendix B

Questionnaire

The following is the questionnaire filled in by all experiment participants after the experiment.

Digital Forensics in Second Life

Questionnaire for Experiment Participants

Please answer all questions (1-6). If your avatar was an "investigator", also answer question 7. When picking an option which states "please specify", please clarify your answer in the space provided. Feel free to comment on any of the questions, or to provide any additional details or comments at the end of the questionnaire.

==========

1. *How easy did you find navigating in the Second Life environment?*
    a. Easy
    b. Mildly difficult
    c. Difficult

2. *To what extent did the extra options of the standard Second Life Viewer facilitate your tasks in the experiment? (e.g. chat, screen capture, gestures, editing objects, etc)*
    a. To a great extent: I used the Second Life Viewer options to perform most of my tasks
    b. To a minor extent: I used a couple of Second Life viewer options
    c. None: I only made use of standard actions such as moving and building.

3. *How easy was it to find the options needed for your tasks in the Second Life Viewer interface?*
    a. Very easy: I knew exactly where to look
    b. Mildly easy: I had to search for some time
    c. Difficult: I did not know where to look and spent a lot of time searching

4. *Did the internet connection quality affect any of your tasks in the experiment?*
    a. Yes, I had trouble performing many of my tasks due to internet connection problems
    b. Yes, but I only had minor difficulties
    c. No, I did not have any problems with the internet connection

5. *Did you notice anything interesting that you have not noticed before, during the experiment?*
    a. No
    b. Yes (please specify):

    ……
    ……
    ……
    ……
    ……
    ……
    ……
    ……

6. *Did we miss anything in the experiment setup?*
    a. No
    b. Yes (please specify):

    ……
    ……

……
……
……
……
……
……
……

For "investigator" avatars:

7. *What kinds of evidence did your manage to gather? (please specify)*

……
……
……
……
……
……
……
……

Any other comments? (You may elaborate on your answer to any of the preceding questions and/or provide any other comments)

……
……
……
……
……
……
……
……
……
……
……
……
……
……

THANK YOU FOR YOUR PARTICIPATION

Appendix C

Public Chat Log

The following is the public chat log saved by one of the "investigator" avatars.

[2012/05/02 06:10] ** HOLO VENDOR Star Raiser Transfer Versions **: Now Showing: Star Raiser V 3 T -20m - Silver / Orange
[2012/05/02 06:10] Visitor Counter v1.19: Greetings, Shay Streusel, Welcome to RMS Titanic = Ship of Dreams = Enjoy your visit-
[2012/05/02 06:13] Second Life: Teleport completed from http://maps.secondlife.com/secondlife/Titanic/39/210/43
[2012/05/02 06:15] Murderer Notebook: whispers: Gnomey Goldkey's Notebook is ready.
[2012/05/02 06:40] Gnomey (gnomey.goldkey): Hi guys! Testing chat.
[2012/05/02 06:53] Aladrinn: it's fascinating hey?
[2012/05/02 06:53] Aladrinn: hehe
[2012/05/02 06:56] Gnomey (gnomey.goldkey): I'm going to try make a house too
[2012/05/02 06:56] enos22: lets see
[2012/05/02 06:57] Chest: Hi Aladrinn Resident! Touch me to change pose. Say /1a to Adjust.
[2012/05/02 07:00] Aladrinn: /la
[2012/05/02 07:01] Aladrinn: very nice
[2012/05/02 07:02] Aladrinn: mdosi...what are u doing?
[2012/05/02 07:02] Gnomey (gnomey.goldkey): I think mdosi is building a foundation
[2012/05/02 07:02] mdosi: wanna destroy the building
[2012/05/02 07:04] mdosi: what up?
[2012/05/02 07:04] Aladrinn: mmm....waiting...
[2012/05/02 07:04] Aladrinn: for better days
[2012/05/02 07:04] Aladrinn: hehe
[2012/05/02 07:05] mdosi: the builder is no where to be seen now
[2012/05/02 07:05] Aladrinn: hehe
[2012/05/02 07:05] Aladrinn: true
[2012/05/02 07:07] mdosi: some gy is joking here i wanna slap them
[2012/05/02 07:15] Loser Mode: whats happening?
[2012/05/02 07:20] mdosi: whats happening is waht you can see
[2012/05/02 07:44] JMMBC Okelli: hi
[2012/05/02 07:44] Aladrinn: hi
[2012/05/02 07:44] JMMBC Okelli: a beatyfull lady
[2012/05/02 07:44] JMMBC Okelli: :)
[2012/05/02 07:53] 69 Shuuhei (archernighthound): what are you doing?
[2012/05/02 07:57] Makenzii: May I help you?

Appendix D

Ethics Clearance Certificate

The following is the ethics clearance certificate issued to the author by the University of Pretoria EBIT Ethics Committee with regards to the current study.

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Reference number: EBIT/52/2011 5 December 2011

514 Missouri Street
Faerie Glen
Pretoria
0043

Dear Ms Rakitianskaia,

FACULTY COMMITTEE FOR RESEARCH ETHICS AND INTEGRITY

Your recent application to the EBIT Ethics Committee refers.

1 I hereby wish to inform you that the research project titled "Digital forensics in second life" has been approved by the Committee.

This approval does not imply that the researcher, student or lecturer is relieved of any accountability in terms of the Codes of Research Ethics of the University of Pretoria, if action is taken beyond the approved proposal.

2 According to the regulations, any relevant problem arising from the study or research methodology as well as any amendments or changes, must be brought to the attention of any member of the Faculty Committee who will deal with the matter.

3 The Committee must be notified on completion of the project.

The Committee wishes you every success with the research project.

Prof. J.J. Hanekom
Chair: Faculty Committee for Research Ethics and Integrity
FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY