Nature and forensic investigation of crime in Second Life

A.S. Rakitianskaia
Dept. of Computer Science
University of Pretoria
Pretoria, South Africa
arakitianskaia@cs.up.ac.za

Prof. M. S. Olivier
Dept. of Computer Science
University of Pretoria
Pretoria, South Africa
molivier@cs.up.ac.za

A. K. Cooper
Built Environment
CSIR
Pretoria, South Africa
ACooper@csir.co.za

Abstract - **Online social spaces have become very popular in the past couple of decades. With the great numbers of users in the online environments it becomes obvious that the human factor plays an important role in the social structure of such environments. In online virtual worlds such as Second Life one may encounter not only civil, but even criminal offenses such as fraud, money laundering, or sexual harassment. It is evident that a digital forensic investigation should take place if any such criminal offense is committed inside the virtual world. This paper presents, categorises, and discusses various crimes that can take place in Second Life, as well as proposes four digital forensic techniques for gathering evidence of these crimes from the inside of the virtual world.**

Keywords: Second Life; virtual world; virtual environment; digital forensics; harassment; discrimination; crime; digital evidence.

I. INTRODUCTION

Nowadays the Internet has become an important part of people's daily life. It is used for transmission and sharing of information, for business, work, studying, as well as in one's private life. People connect with others through e-mail clients, information sharing-centred websites such as YouTube[1] or DeviantArt[2], as well as through various social networks. Many of these social networks are browser-based, but there are a number of online social spaces that take the intercommunication between the people to a new level, providing users with an experience of immersion in the environment. Online virtual worlds such as World of Warcraft, Everquest, or Second Life belong to the category of immersive online social environments. Such online virtual worlds have become very popular, and are being used by millions of people all over the world. Thus it is fair to assume that the human factor plays an important role in the social structure of online social environments. That is where a security problem arises. Due to the human factor, the environment can be misused, causing emotional or material harm to the people involved in this environment. Crimes can take place in the virtual world just as they do in the real world. In most online social spaces people portray themselves as avatars, thus hiding their real identity. This may lead to users behaving offensively towards others, due to the fact that no one knows who they really are [13]. A case of racist behaviour towards certain users is an example of such an offence. Other crimes such as fraud or money laundering can take place in a virtual world such as Second Life, where in-game currency can be exchanged for real-world currency. One can find many other examples of civil and criminal offenses originated from within online social worlds.

In this paper crimes in Virtual Worlds are only discussed in the field of Computer Science. The discussion of the matters of law and other legal aspects behind criminal activity is beyond the scope of this paper, and is not considered.

This paper looks at various criminal offenses that can take place in Second Life, one of the most popular immersive online social environments. Each offense is analysed it terms of its nature, as well as where and whom it usually originates from. Four techniques of gathering digital evidence from the inside of the virtual world itself are presented and given an overview of.

II. BACKGROUND

A. Defining "crime"

Before any discussion can be commenced, it is necessary to provide precise definitions of the legal terms used in this study, such as "crime", "offense", "offender", and "criminal". This section addresses these terms which are used throughout the paper and provides clear definitions of each in the context of the current study.

Crime can be defined as an action that is against the law, and is harmful to the public welfare or morals [8]. In terms of the law crime could be defined as any offence against the public law of the country it is committed in [9]. This term is usually applied to offenses which are bound to be punished by the acts of criminal law. "Offense" is a synonym of the term "crime", and also refers to actions against the public law. In the context of the current study, the misdeeds addressed do not only consist of unlawful actions, but also civil offenses and simply unethical behaviour. Since the focus of this study is on Second Life, anything unlawful or

1. http://www.youtube.com
2. http://www.deviantart.com

unethical that could be done inside the Second Life environment and which needs to be investigated, is considered significant subject for discussion. It is also essential to note that there exists a problem of drawing a line between what should be considered a crime, and what should not. Addressing this problem is outside the scope of this paper, thus the terms "crime" and "offense" are used interchangeably throughout the paper and include both criminal acts and civil offenses.

Similar to the two abovementioned terms, the terms "criminal" and "offender" are synonyms. A criminal is an individual guilty or convicted of crime, as well as someone who commits crimes for a living [24], while an offender is a person who acts against the public law [25]. For the reasons provided above, these two terms are used interchangeably throughout the paper and include civil offenders as well as professional criminals.

B. Virtual Reality vs Virtual Environment

There is a difference between the two terms which are sometimes used interchangeably, namely "virtual environment" and "virtual reality". Both terms describe virtual environments, but, based on various definitions of both, one can see that "virtual reality" is specifically used for immersive environments which are created to imitate the real world or any other world which the user can be a part of while interacting with the virtual reality. The term "immersive virtual environment" is defined as an environment which portrays a digital space in such a way that the users feel as if they are physically present in that environment. Schroeder [3] defines immersive virtual environments 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 [1]:

> "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."

"Virtual environment" is a broader term which does not imply that the environment is immersive and can be used to describe various digital environments: environments used for training purposes (such as medical, military, etc), entertainment purposes (e.g. virtual golf [5]), as well as those which fall under the "virtual reality" domain. Although for both Virtual Environments and Virtual Reality the availability of interaction with the environment and feedback are two very important characteristics.

C. Virtual Reality vs Virtual World

We have now defined virtual reality as a virtual environment which represents a digital world in order to make the user feel immersed in it, and which allows for interaction with the environment, as well as gives feedback to the user. Another term which is often used when immersive virtual environments are discussed is "virtual world". It is sometimes considered a synonym for the term "virtual reality", but that assumption is not always correct. Schroeder [2] 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". Thus we can see that virtual worlds are a subset of virtual reality, which consists of immersive virtual environments available on the internet and used by a great number of individuals concurrently, for social or gaming purposes. For the remainder of this article the term "virtual world" is used to discuss such online environments.

III. CRIMES IN VIRTUAL WORLDS

Crime has been present in the human community for as long as the human race existed. There are a vast number of malicious actions aimed at other people, companies, or even countries, many of which are considered criminal offences. This list had been expanding as criminals discovered more and more means of achieving their malicious goals due to the technical progress over the centuries. The opportunities for criminal activity have expanded immensely since the invention of computers, specifically in the last 50 years. The "digital world" of the late 20th century introduced a new category of crimes onto the scene, namely Digital or Cyber crimes. Digital crimes are not new *per se*, but just a realization of some of the known criminal activity via the digital technology. Although there are a number of things which were not heard of before, but were made possible and became basis for security concerns since the computerisation of the human community in modern times, seeing as computers were the new tool for crime commitment (e.g. hacking). Nonetheless, all of those digital crimes serve some or other general purpose, such as money making, and in the end can be classified as one of the previously known crimes.

The crimes addressed in this paper belong to the category of cybercrime, since such crime can be committed in an online virtual world, specifically Second Life. In Table 1 the authors present a broad categorization of the criminal activity that can occur in Second Life. The crimes are organised into four categories, namely Harassment, Anti-social crimes, Discrimination, and Money Making. In Table 2 the authors offer a more detailed classification of the crimes listed in Table 1. The tabular diagram shows which crimes can only be committed inside the Second Life environment itself, and which also involve the real world aspect. In addition, Table 2 shows which offenses only affect the person "virtually" (i.e. the person's avatar or virtual property), and which lead to

real-life damage. The authors do not claim the diagrams to be complete, but it is considered sufficient for the purpose of presenting an overview of the criminal activity in Second Life.

All categories and types of crime depicted in Table 1 are discussed in this section. Every crime is analyzed by the scheme of "5 W's and 1 H", i.e. "Who, What, When, Where, Why and How". "Who" looks at the types of criminals who are likely to commit a specific crime. "What" defines the crime and explains the specifics of it. "When" describes the possible scenarios which the crime is likely to be committed in. "Where" looks at the possible places and areas inside Second Life where the crime can be committed. "Why" lists the possible reasons one would commit the crime for. "How" describes a number of possible ways the specific crime could be committed in Second Life.

Harassment	Anti-social	Discrimination	Money Making
Virtual mugging	*Virtual Brothels*	*Sexism*	*Money Laundering*
Verbal harassment	*Virtual Paedophilia*	*Racism*	*Fraud*
Impersonation	*Vandalism*	*Gold Farming*	*Gold Farming*
Cyberstalking	*Child Pornography Distribution*		*Account Hacking*
			Identity Theft

Table 1. Broad Categorisation of Crime in Second Life.

A. Harassment

Harassment is a type of crime which involves actions aimed to threaten or otherwise disturb the victim (or victims). It can be based on gender, race, and other physical features of the person, or on his religious and moral beliefs and values. A number of different types of harassment have been defined [15] [16], but for convenience and clarity this paper will group the various harassment types into three categories, namely psychological harassment, physical harassment, and stalking. Psychological harassment affects the victim or victims on the psychological level: disturbs them, causes them to lose self-esteem, torment, or in extreme cases might even lead to loss of sanity. Physical harassment involves physically bullying the victim or victims, threatening them, with or without causing them actual physical harm. Physical harassment is often executed by a group against an individual. Stalking is a type of harassment which involves pestering an individual, in real life or by any other type of contact. It can also involve following the person, spying on them and gathering all kinds of information about them without their consent or approval, up to the point of illegally obtaining valuable personal information thus invading on the victim's privacy, which could lead to concerns about their safety. In terms of virtual environments, any kind of action against a person that disrupts his/her activities inside the environment (pushing, attacking, etc) is called "griefing", and the offender "griefer" [11].

Psychological harassment is mostly performed by means of verbal communication. Non-verbal, or physical, communication can also affect a victim on psychological level, although in such cases the offender would have to perform both physical and psychological harassment concurrently to achieve the desired effect. It should be noted at this point that the term "physical" is used in the context of the virtual worlds, thus it implies physical actions of the offender's avatar against the victim's avatar. Verbal harassment involves insulting, disturbing or threatening words directed to the victim by the offender. Such communication may be transmitted via the public chat, private instant messaging system which is built into the environment, or through VoIP technology, built-in at specific areas in Second Life. Such verbal harassment crimes are most likely to be committed by people trying to push their victims into sending them Linden dollars (virtual money), or give them access to their virtual land. The other likely offenders would be individuals suffering from intolerance towards certain human characteristics, e.g. gender, race or nationality. Places in Second Life where verbal harassment is most likely to be committed include public entertainment areas such as dance floors, cafeterias, and night clubs, as well as virtual casinos and adult-oriented areas such as virtual strip clubs and virtual brothels, due to large numbers of people visiting such places.

In the environment of Second Life physical harassment can be performed by various means. The offender's avatar can follow the victim's avatar, block their way or perform "physical" actions against them (e.g. kick them). Virtual mugging is another type of harassment which is present in the world of Second Life. This crime belongs to the physical harassment category due to the fact that it involves an individual or a group of individuals attacking a victim inside the virtual world, threatening them and demanding their money or personal information, and is most commonly performed by a group. The offenders block their victim's way, surround him/her, just like in real life, and get the information or money by force. Such offenses are most likely to happen in quieter areas of Second Life, which are not crowded and are rarely visited by users. Virtual mugging can also happen if the criminals break into their victim's virtual house. Virtual mugging is usually an organized criminal action, so the most likely suspects would be virtual gangs which consist of people who try and steal money, identity, or other important information from their victims. It is unpredictable as to where such gangs may form, since such crimes would usually be organized outside the Second Life environment, e.g. by e-mail or by the means of other social networks such as Facebook[1], or even in person if the members of the gang live in the same country.

A more accurate term for stalking in the context of Second Life is cyberstalking. Cyberstalking is a crime that involves repeated attempts to harass the victim and gather their personal information via the Internet [12]. In Second Life, cyberstalking can be performed by the means of

1. http://www.facebook.com

following the person's avatar, gathering information such as the location of their virtual house, their favourite areas, or their virtual friends. This information can be gathered from a number of sources ranging from the victim's online acquaintances to virtual spies. Knowing the person's nickname, the offender can also continuously send private messages to their victim, thus psychologically disturbing them. The most likely candidates to commit the crime of stalking are individuals with a goal to steal their victim's private information in order to perform illegal impersonation of the victim or commit identity theft and steal their virtual, or even real money (provided their real-world bank account number has been stolen). Stalking can happen in each and every area in Second Life, but the most likely areas, visiting of which may lead to stalking, are public social areas

	In the Real World	Inside the Virtual World`	Real World Damage	Virtual World Damage
Harassment	*Impersonation*	*Virtual Mugging* *Cyberstalking* *Indirect / Direct Harassment*	*Cyberstalking* *Virtual Mugging*	*Impersonation* *Virtual Mugging*
Anti-social	*Child Pornography*	*Virtual paedophilia* *Virtual brothels* *Child Pornography*	*Virtual paedophilia*	*Vandalism* *Virtual brothels*
Discrimination	---	*Sexism* *Racism*		*Sexism* *Racism*
Money-making	*Gold Farming* *Money Laundering*	*Gold Farming* *Fraud* *Account Hacking* *Identity Theft* *Virtual Mugging*	*Gold Farming* *Fraud* *Identity Theft* *Account Hacking*	*Fraud* *Virtual Mugging*

Table 2. Detailed Categorisation of Crime in Second Life.

such as virtual night clubs and virtual casinos, due to a wide variety of people gathering at such places. Virtual casinos can be classified as the most likely area for stalking due to the fact that people regularly visiting casinos are known to be in possession of quite substantial amounts of Linden dollars. As seen in Table 2, cyberstalking affects the victim inside the virtual world, as well as inflicts real-world damage, due to the fact that cyberstalking can disturb the person on psychological level, as well as give the offender access to the person's private information applicable in real life.

B. Anti-social crimes

This subsection covers anti-social crimes using vandalism, paedophilia, and child pornography distribution as examples. Child pornography distribution or virtual paedophilia can be committed in Second Life by various means and in various places.

Virtual paedophilia is the virtual analogue of the paedophilia in real life, i.e. a mental disorder which causes the person's sexual interests to be focused on prepubescent children, aged 13 years or younger [17]. Due to the fact that Second Life is open for all ages, there are a great number of pre-teens registered in the virtual world. This may lead to their abuse by virtual paedophiles. Criminals themselves are most likely to be males [18] 16 years or older [17]. The most likely places where one might encounter virtual paedophilia are areas which children are admitted to, or adult-oriented areas such as virtual brothels or virtual strip-clubs. Specific adult areas in Second Life are also places where one is likely to encounter virtual paedophiles. Virtual paedophilia can be committed by gaining access to and gathering of child pornography images and videos, as well as talking to underage users of Second Life and sexually harassing them by threatening and demanding specific kinds of photos or videos from them, as well as arranging meetings in real life for possible physical sexual abuse. Real-life possibilities of virtual paedophilia make it a crime that affects the victims in the real life as well as virtual space, as seen in Table 2.

Adult areas such as virtual brothels or virtual strip clubs are areas where distribution of child pornography is likely to happen. Among other adult content criminals might hide illegal child pornography images and videos and distrib

ute them between the members of the club. The distribution is most likely to happen outside Second Life (i.e. in the real world, as seen in Table 2), after the criminals exchange contact information via one of the various communication technologies built into the Second Life environment. Virtual brothels can also be used as a means of illegal money-making. If the owner managed to force his/her employees (by paying them per hour) to spend time in the virtual brothel and use their avatars to perform sexual actions on demand of the visitors to the brothel, and gain profit from the money being paid for entrance by each visitor, he/she could be rightfully called a person committing an anti-social crime. The reason to commit such a crime is quite straight-forward: making easy money by abusing others. Since the abuse would only happen inside Second Life, the authors categorised virtual brothels as only applicable inside the virtual world, inflicting damage on the victims only in the Second Life environment (see Table 2).

Vandalism is a criminal offense of damaging or defacing of property belonging to other people or the public. Some real-life examples of vandalism include graffiti on the walls of private houses or public buildings such as museums and breaking of tombstones and monuments or windows. In the context of Second Life, examples of virtual vandalism could include planting unwanted objects on private property, sticking virtual posters on the walls of private houses, as well as damaging or altering public domain objects such as notice

boards without permission. The most likely candidates to commit vandalism would be adolescents aged 11-17 [22] and young adults with personality traits such as anger, hostility, venturesomeness [21], and sensation-seeking [23]. The acts of vandalism are usually carried out for reasons of social protest or the assertion of one's rights or self-esteem [23]. Vandalism can be committed in any area of Second Life, but public places such as entertainment areas or gardens, as well as private property, are most prone to vandalist attacks. The only damage virtual vandalism can bring is damage of virtual property, thus in Table 2 this crime is listed under "Inside Virtual World", as well as "Virtual World Damage".

C. Discrimination

Discrimination is an act of prejudice against a person, based on their physical, mental, or social characteristics, e.g. gender, race, social status, or religion [20]. There are two types of discrimination, namely direct and indirect [20]. Direct discrimination refers to discriminative acts against a person or persons. Indirect discrimination occurs when a certain policy claimed to treat everyone fairly effectively puts a certain group of people at a disadvantage. This section discusses direct discrimination using the two most commonly encountered examples, namely racism and sexism, as well as covers general indirect discrimination traits in Second Life. Such discrimination is only applicable inside the virtual world, in the Second Life context, as seen in Table 2.

Racism is prejudice towards a person based on their race. It can lead to discrimination in the workplace, social community, as well as virtual worlds such as Second Life. Some examples of racism include prohibiting a person of a certain race to take part in specific activities in Second Life, be part of certain clubs and social spaces, or enter certain areas. Racism is a crime which can be committed by any person, of any age group or gender, thus it is difficult to determine a specific group of people who are most likely to be guilty of racism. Manifestation of racism can be encountered in various places in Second Life, but more specifically in social spaces and entertainment areas, where culture-specific activities may lead to discussions on culture and race differences. People suffering from certain race intolerance are more likely to offend other people based on their race. Due to the fact that one's avatar can be easily changed to whichever race the user wants, it is possible to avoid being offended if one is suspecting people in a certain area to be specific race-intolerant. Nonetheless, it is still considered unacceptable behaviour to discriminate against other users based on their race and may lead to the offence being taken to court. The main reason for racism would be to cause the person belonging to a certain race psychological harm and show the superiority of the offender's race compared to the victim's race.

Sexism is very similar to racism. It is an action of prejudice towards people of a certain gender. In real life examples of sexism would be limiting the work opportunities for people of a certain gender, limiting their salary, denying access to certain places or certain information. In Second Life environment examples would be denying individuals of certain gender access to specific areas, clubs, restricting their involvement in certain activities, limiting their virtual work opportunities or denying them higher authority posts (e.g. company manager). Acts of sexism are most likely to be performed in unrestricted social spaces such as night clubs, various other social entertainment areas, as well as some of the elite clubs or areas in the world of Second Life. Similar to racism, the most common reasons to commit sexism are to traumatize the victim in one way or the other, show them how people belonging to the opposite gender are superior to the people of their gender. This is usually done by people feeling hate for the opposite gender for personal reasons.

Indirect discrimination can be encountered in virtual workplaces in Second Life, such as virtual shops and virtual cafeterias. Similar to real life, virtual shop owners can demand of their employees to dress or behave in a certain way, which may be uncomfortable for certain employees for personal reasons such as religion. Main reasons for indirect discrimination are usually the same as those for direct discrimination. Indirect discrimination is just a more subtle way to discriminate against a certain group of people.

D. Money making

This type of crime is quite straight-forward: the main goal is making substantial amounts of money by means which are considered illegal. A number of crimes fall under this category. One can list crimes such as fraud, money laundering, account hacking, as well as gold farming, the latter being specific to online virtual worlds such as online games and social spaces. Due to the fact that Second Life has its own economy, as well as the fact that its virtual currency can be exchanged for real-world money, most of the crimes which belong to the money-making category can be applied in the Second Life environment. As seen in Table 2, most of these crimes affect the victims in both the virtual world and real life. In this section the crimes listed above are explained and analysed in the context of Second Life.

Fraud is a criminal offense that involves tricking the victim into performing some or other action, or making a deal which would let the offender make illegal profit or gain unfair advantage. There are various types of fraud, but not all of them are applicable to Second Life. An example of fraud in a virtual world would be taking the money (virtual money, which are easily exchanged to real money), but not delivering the virtual goods in a scenario of a virtual shop [10]. Fraud is also committed when a person makes a deal with another to create a certain unique item and share the profit equally, but when the item is created, the offender copies it to his inventory and disappears, selling it as an individual later and gaining all the profit for him/herself. The most likely places where fraud is committed are virtual shops, virtual factories, or individual trades between users in Second Life. 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 commit fraud. People most likely to be guilty of fraud are individuals skilled in persuasion, as well as those who possess good charisma and know how to make people

trust them, since these attributes are essential to the success of the crime.

Account hacking is a crime which originated as a type of theft specific to digital environments where users create personal digital profiles and store valuable personal information such as passwords, bank account numbers, ID numbers, etc. A hacker acquires means of access to a person's account without their consent, using specific techniques, and steals all the valuable information. That gives various opportunities to the criminal to use the information for illegal money-making or identity theft. Any person skilled enough in programming and the works of computer operating systems can be a hacker. Many of the convicted hackers had been young individuals, usually in their 20s [14]. One of the reasons for it may be the fact that sometimes account hacking happened because the individual responsible for it was curious as to what extent could he/she push their skill, and set such a misleading goal as a challenge. Once successful, the young hacker could not help to see all the opportunities it opened, and was not able to withstand the temptation. Account hacking can also sometimes be a part of organised crime. If the criminal's purpose is to commit identity theft, the hacking of the victim's account might just be a way to get access to the needed information. Cyberstalking could also lead to account hacking, due to the offender's goal of gathering all the possible information regarding a certain individual. In Second Life, account hacking happens mostly because the hacker is trying to get access to the victim's virtual goods, land or money. If a Second Life user heedlessly gives fellow users his/her password or other personal details, via chat or other kinds of communication inside Second Life's environment, he/she could easily become a victim of account hacking. Thus it is vital that the personal information is only shared with people one knows in real life. Account hacking is not bound to any specific areas inside Second Life, thus making it possible to hack an account at any place inside the environment, as well as from the outside, via a network.

Another money-making technique (also used for other kinds of profit, which highly depends on the environment) often used in online social spaces is gold farming. One can define gold farming as a branch of Real Money Trading (RMT) [6], or trading virtual money/goods for real-world currency by making one's character/avatar engage in certain activities or simply be situated in a certain place inside the digital world for a set amount of time, obtaining virtual currency or virtual goods (referred to as "camping"). It has been utilized as a job opportunity: people founded businesses which were based solely on hired workers who spent up to 18 hours straight "playing" a MMOG (Massively Multiplayer Online Game) in order to gain as much virtual money as possible, for $75 to $250 per month [6][7]. Practice of such gold farming business has been widely spread throughout China, and even created a stereotype that all gold farmers were Chinese, as well as all online gamers with poor English were Chinese gold farmers [7]. Gold farming has been an acute topic of discussion ever since it became prominent that it has become a huge market of poorly paid jobs, employing thousands of people from developing countries. The fact that the employees of gold farming businesses were almost always paid very little effectively made such businesses "virtual sweatshops", exploiting workers via virtual worlds such as World of Warcraft and Lineage. Second Life has also been used as a means for profit-making via gold farming. Although being an official virtual economy it does not restrict gold farming practice as much as online gaming communities do. The most likely people to engage in gold farming are young people, specifically males 18-25 years old [6], living in developing countries, mostly China and Korea [20]. Some gold farm workers are students trying to gain extra income, and some are unemployed rural migrants trying to find work in urban areas [6]. Their employers are usually from the US or somewhere in Europe. It is difficult to pinpoint the exact locations where gold farming is likely to take place, since it usually happens unnoticed and there aren't specific places for it. For example, "camping" can happen in any location inside Second Life; all the observer sees is an avatar either standing still or engaging in an activity in a certain location. Also, farming and plain re-selling of items might be difficult to distinguish from each other. Another possible point of discussion would be to determine if gold farming should be considered an illegal activity. For people of poorer countries the choice sometimes stands between hours of gold farming for paltry amounts of money, or no job at all. In addition, actual "virtual sweatshops" do not exist; it is impossible to judge whether a person in Second Life is being abused, since all the oppression and exploitation happens outside of the virtual world, in-world seeming like an avatar engaging in different activities. If the gold farming process is automated via a bot and an avatar is controlled from outside Second Life, no human labour is engaged in that specific type of gold farming.

Money laundering is another crime which falls into the money-making category. The essence of the crime is in hiding the origin of illegally obtained money, thus making it possible to use these funds without any complications. It is possible to achieve money laundering in Second Life by creating multiple fake avatars and transferring small chunks of illegally obtained money between them, making it difficult to trace back to the original avatar who is the criminal him/herself. Fake characters can also be created by bots, to prevent IP address trace evidence. The most likely people to commit money laundering are individuals capable of obtaining money by some or other illegal means, such as account hacking or virtual mugging. Thus they have to have sufficient computer skills, as well as be able to easily persuade or intimidate other people (as in case of virtual mugging), or have good charisma to organise virtual gangs. Once again, this type of crime is not bound to any specific place in Second Life, since it can happen in any area inside the virtual world.

IV. Investigative techniques inside Virtual Worlds

As has been mentioned in the sections above, cyber crime is just a new realization of "traditional" crime, through digital technology and the Internet. It becomes apparent that

the standard techniques of investigation which apply to real-world crimes do not necessarily apply to the crimes in the digital world, since the evidence sources for the digital criminal offences are considerably different from the real world.

Various ways for conducting a digital forensic investigation of a crime committed in a virtual world could be utilized, such as studying of network logs or monitoring network traffic via diverse packet capturing tools. Although these techniques imply that the investigation happens outside the virtual world itself, i.e. the investigator is not logged in to the virtual environment but operates on the data captured during the interaction with the environment and stored elsewhere. This paper investigates whether it is possible and viable to conduct a digital forensic investigation while being inside the virtual world. In this section, four possible techniques of investigation, as applied to Second Life, are presented, namely:

1) *Official virtual police*
2) *Private virtual investigation*
3) *Luring the potential criminals in via an attraction (similar to a honeypot)*
4) *Adding extra evidence gathering functionality/widgets as the creator of the virtual world*

These four techniques are discussed below.

A. Official Virtual Police

Official Virtual Police is an investigative technique which involves creating an avatar or multiple avatars in Second Life to serve as virtual police in specific or all areas of the virtual world. Since it is possible to customize one's avatar, the avatars of the virtual police could be given an official uniform so that the police could be recognised by other users. Since some areas in Second Life are created in resemblance to different countries (e.g. Spain), different virtual police groups could be created, dedicated to each virtual country and resembling the police officers' look in that country. Virtual policemen could officially interview the users of Second Life to gather information about a crime from them as victims or witnesses. Official meetings could also be organised, where all the members of the virtual police would share the information they gathered, compile it together, and send it by e-mail to the higher police officers in the real-world. Virtual police stations could be created where users would come to if they feel the need to report any malicious activity. There are an immense number of possibilities with regard to specifics of introducing virtual police into Second Life environment.

This approach has a couple of drawbacks. To efficiently install virtual police and maintain its effectiveness, quite a large number of people have to be involved and organised together as a group. Virtual police officers themselves have to be authorised and authenticated to prevent bots and individuals with malicious intents from infiltrating the virtual police. In addition, to effectively monitor the virtual world and prevent any illegal behaviour, the virtual police must be continuously present in Second Life, which is difficult to accomplish. A possible solution to this problem could be the employment of police officers all over the world as virtual police. Although a question as to the way of salary disbursement to all the employed officers arises from the proposed solution. Another drawback to this technique is the fact that law conflicts may arise in the various virtual countries inside Second Life, if the laws of each respective country in real life are taken into account when criminal cases are constructed by the virtual officers.

The specific ways of instalment of virtual police and overcoming the abovementioned drawbacks will be discussed in future research.

B. Private virtual investigation

A private virtual investigator is an investigator inside Second Life who is a regular registered user, but whose goal is to gather evidence of the various offenses that happen in Second Life. Such a private investigator could also take requests from other users to investigate various cases, e.g. harassment. For example, if the private investigator received such a request, he/she could follow the offender around the environment, trying to witness the act of harassment and record what he/she witnessed as evidence. This technique also has its drawbacks. To be a virtual investigator, the person must be willing to spend plenty of time online, as well as to make the effort to record all the possible evidence he/she comes across. The question of such an investigator's salary also arises, as well as the question as to whom should the virtual investigator be employed by. These, and other uncertainties will have to be resolved if this technique is to be realised, and the specific ways of dealing with these drawbacks will be addressed in future work.

C. Luring possible criminals in

Luring possible criminals in may seem advantageous compared to the techniques discussed above, since it requires much less human involvement. The essence of this technique is in creating an object or an area inside the Second Life environment that would provoke potential criminals to show illegal behaviour. If such behaviour is detected it would be logged for the information to be used as evidence of the committed crime (the details of logging are outside of scope of this paper). Evidently, this approach is similar to the notion of a "honeypot" – a trap created to detect and prevent unauthorised use of information systems. In the context of Second Life an example of such a honeypot would be creating a fake avatar and purposefully make it easy to obtain the avatar's password, to provoke potential criminals to hack the account hoping to gather some profit from it. An advantage of this approach is in the fact that the logging of an intrusion (or anything else) could be automated so that human involvement is minimised. A drawback of this technique is in the fact that it should not be obvious to other users that the object/avatar is not controlled by a human, otherwise it might arise suspicion. The specifics of the realisation of this technique will be addressed in future research.

D. *Extra evidence gathering functionality/widgets inside the virtual world*

This technique implies that the creators of Second Life and their employees would be involved in the process, since it concerns the environment itself. Security is a great concern for any social network, especially if it is as massively populated as Second Life. Thus it is considered a possibility that, given a proposal, the creators of the environment would indeed consider adding extra functionality to the environment or special widgets to the interface. A drawback of this approach is the fact that the potential criminals will have access to this functionality as well as the regular users. Thus the hackers might find a way to abuse the extra functionality and make it work to their advantage instead of against it. The advantage of this approach is in the fact that controlling one's security inside Second Life will be easier provided the extra functionality is user-friendly, effective, and efficient. This technique will be discussed in more detail in our future work.

CONCLUSION

In this paper various types of criminal activities that can take place in a virtual world, on an example of Second Life, were presented, categorised, and discussed. Each crime was analysed by the scheme of "Who, What, When, Where, Why and How", or "5W's and 1 H". In addition, four techniques for gathering evidence from the inside of Second Life (or any other virtual world) were presented, namely:

1) *Official virtual police*
2) *Private virtual investigation*
3) *Luring the potential criminals in via an attraction (similar to a honeypot)*
4) *Adding extra evidence gathering functionality/widgets as the creator of the virtual world*

An overview of each of these techniques was presented, and special attention was paid to the advantages and disadvantages of each approach.

This paper has not discussed the four presented investigative techniques in detail or dealt with the law background of crime in Second Life. We will explore the techniques for digital investigation further and in more detail in the future research. The topic of law in Second Life environment could also be given further attention to in the future.

ACKNOWLEDGEMENTS

We would also like to thank the ICSA Research Lab for providing this opportunity to present this paper and get valuable feedback from the research community.

REFERENCES

[1] G. Dunnet et al, "Realism Meets Virtual Reality", Real World Visualisation - Virtual World - Virtual Reality, IEE Colloquium on, London, UK, pp. 6/1–6/4, September 1991.

[2] R. Schroeder, "Defining Virtual Worlds and Virtual Environments", Journal of Virtual Worlds Research, vol. 1, July 2008.

[3] R. Schroeder, "Possible Worlds: The Social Dynamic of Virtual Reality Technologies", Westview Press, 1996.

[4] Carrier, B., 'Defining digital forensic examination and analysis tools', Digital Research Workshop II, 2002.

[5] V-Golf Sports Bar, Available: http://www.v-golf.com.sg/aboutus.html. Accessed on 29.04.11.

[6] R. Heeks, "Understanding "Gold Farming" and Real-Money Trading as the Intersection of Real and Virtual Economies", Journal of Virtual Worlds Research, vol.2, no. 4, February 2010.

[7] D. Barboza, "Ogre to Slay? Outsource It to Chinese", The New York Times, December 2005.

[8] Dictionary.com, "crime," in *Dictionary.com Unabridged*. Source location: Random House Inc. http://dictionary.reference.com/browse/crime. Available: http://dictionary.reference.com. Accessed: May 11, 2011

[9] The 'Lectric Law Library, "crime", in *The 'Lectric Library Lexicon.* Available: http://www.lectlaw.com/def/c330.htm. Accessed: May 11, 2011

[10] S. Cikic, S. Grottke, F. Lehmann-Grube, J. Sablatnig, "Cheat-Prevention and Analysis in Online Virtual Worlds", in *Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, ICST, Belgium, 2008.

[11] D. Jeffers, "Is there a second life in your future?", in *Proceedings of the 36th annual ACM SIGUCCS fall conference: moving mountains, blazing trails*, USA, 2008.

[12] M. Burmester, P. Henry, L. S. Kermes, "Tracking cyberstalkers: a cryptographic approach", Journal of Computers and Society, vol. 35 issue 3, September 2005.

[13] D. G. Johnson, "Ethics online", Magazine of Communications of the ACM, vol. 40 issue 1, Jan. 1997.

[14] United States Attorney's Office, Central District of California, "Kevin Mitnick sentenced to nearly four years in prison; computer hacker ordered to pay restitution ...", 9 August 1999. Press release. Accessed 12 May 2011.

[15] Harassment101. Real Life Lessons. Available: http://www.harassment101.com/Handbook/T1.html. Accessed: July 7, 2011.

[16] Types of Harassment and Bullying. Available: http://www.lboro.ac.uk/admin/personnel/harassmentandb/types.htm. Accessed: July 7, 2011.

[17] Diagnostic and Statistical Manual of Mental Disorders DSM-IV TR (Text Revision). Arlington, VA, USA: American Psychiatric Publishing, Inc.. 2000-06. p. 943.

[18] Psychopathology and Personality Traits of Pedophiles Psychiatric Times. Vol. 26 No. 6. Press release. Available: http://webcache.googleusercontent.com/search?q=cache:eTF5oUIAmPYJ:www.psychiatrictimes.com/display/article/10168/1420331+Dr+Cohen+is+associate+professor+of+clinical+psychiatry+and+Dr+Galynker&cd=1&hl=en&ct=clnk&gl=us. Accessed 9 July 2011.

[19] James Cook University: Definition of Descrimination. Available: http://www.jcu.edu.au/eo/JCUDEV_010542.html. Accessed 9 July 2011.

[20] R.B. Heeks, Current Analysis and Future Research Agenda on "Gold Farming": Real-World Production in Developing Countries for the Virtual Economies of Online Games. IDPM Development Informatics Working Paper no.32. University of Manchester, UK, 2008. Available: http://www.sed.manchester.ac.uk/idpm/research/publications/wp/di/index.htm. Accessed 9 July 2011.

[21] P. Heaven, Personality predictors of self-reported delinquency. *Personality and Indiridual Differences*, 1993, issue 14. pp. 67-76.

[22] M. Carrasco, E. D. Barker, R. E. Tremblay, F. Vitaro. Eysenck's personality dimensions as predictors of male adolescent trajectories of physical aggression, theft and vandalism, *Personality and Indiridual Differences*, issue 41, 2006.

[23] H. J. Eysenck, G. Gudjonsson. The causes and cures of criminality. 1989. New York: Plenum Press.

[24] The Free Dictionary by Farlex, “criminal”. Available: http://www.thefreedictionary.com/criminal. Accessed 10 July 2011.

[25] The Free Dictionary by Farlex, “offender”. Available: http://www.thefreedictionary.com/offender. Accessed 10 July 2011