Research Article
Volume 11:6, 2022

Journal of Applied & Computational Mathematics

ISSN: 2168-9679 Open Access

MMORPG Data Recovery from Player to Player Interactions: Dead Acquisition Including Game Modification Files

Kayla J Schneider*

Department of Computer Sciences, Carnegie Mellon University, Pittsburgh, United States

Abstract

Imagine a world that allows for open, unmonitored communication, and the ability to trade currency between individuals anonymously. An environment such as this would present itself as a prime location for malicious intent. Money laundering, exploitation, theft, harassment, and stalking could potentially go unnoticed. When discussing World of warcraft or fortnite, malicious intent would generally not come to mind. However, this is precisely the type of environment that massively multiplayer online role-playing games provide.

Keywords: Environment • Massive • Communiction • Malicious

Introduction

Imagine a world that allows for open, unmonitored communication, and the ability to trade currency between individuals anonymously. An environment such as this would present itself as a prime location for malicious intent. Money laundering, exploitation, theft, harassment, and stalking could potentially go unnoticed. When discussing World of warcraft or fortnite, malicious intent would generally not come to mind. However, this is precisely the type of environment that massively multiplayer online role-playing games provide [1].

Materials and Methods

Fifteen years ago, researchers in Taiwan analyzed online gaming characteristics that began occurring as games such as World of warcraft, starcraft, and everquest became popular. Researchers analyzed over 613 criminal occurrences for an analysis of online gaming crime characteristics, observed that illegal activity committed using online gaming included:

- Theft
- Fraud
- Robbery
- Kidnapping
- Threats
- Criminal
- mischief
- Counterfeiting
- Extortion
- Assaults and battery

The cases analyzed were from official crime reports made with authorities. Of the cases analyzed for this study, 69.7% were able to be handled within local jurisdiction while major crimes units dealt with the remainder. Theft and fraud were the most common crimes observed, making up 93.9% of the incidents observed. The means of most criminal activity was found to be by identity theft or social engineering. Males made up most of both victims and offenders

While an analysis of online gaming crime characteristics, terrorism Recruiting and training in virtual Worlds presented a much more ominous projection of the potential for malicious use of virtual environments. Social media platforms were discovered to be a means of communication for terrorist groups using steganography. Service providers, such as Facebook, would cooperate with investigations into terrorist activity using their services. Online games, such as World of warcraft, were discovered to be used for means of communications that go unmonitored. The US national intelligence director acknowledged that terrorist infiltration of online games was a real phenomenon in 2008.

Data mining initiatives were created to detect criminal and terroristic activities online. In 2008 project reynard was created by the US Intelligence Advanced Research Projects Activity (IARPA). Project reynard would join other data mining initiatives

***Address for Correspondence:** Kayla J Schneider, Department of Computer Science, Carnegie Mellon University, Pittsburgh, United States, Tel: 7124900886; E-mail: kayla.schneider85@gmail.com*

Date of Submission: 02 June, 2022; Manuscript No. jacm-20-6694; **Editor assigned:** 04 June, 2022, PreQC No. P-6694; **Reviewed:** 18 June, 2020, QC No. Q-6694; **Revised:** 20 June, 2022, Manuscript No. R-6694; **Published:** 27 June, 2022, DOI: 10.37421/2168-9679.2022.11.476.

across the globe, including the EU's Project Induct. time of the creation of these initiatives about the use of online gaming environments to recruit and train members.

In 2011 these environments proved to be essential not only to criminal organizations but individuals as well. Anders behring breivik killed 77 people in a solo terrorist attack against Norway. Breivik had no military background or training yet was able to pull off the deadliest attack against Norway since World War II. Breivik claims to have used call of duty: Modern Warfare 2 as his training grounds. On July 22, 2011, Breivik detonated a fertilizer bomb outside of the building house of the Prime Minister, killing eight people. He then went on to Utoya Island under the rouse of being a police officer and murdered attendees of a youth camp. Breivik left behind a manifesto detailing his preparation for these events, including his "training."

The proprietary nature of these games does limit the availability of data available to law enforcement. Legal authority is necessary to obtain detailed account information. There has been limited success in the testing of keylogger programs. The research was conducted testing keylogger programs while running Massively multiplayer online role-playing games by the Senator Patrick Leahy Center for Digital Investigations (SPLCDI) in 2016 [2].

On October 31st of 2019, California's congressman tweeted a screenshot of a character dressed in white robes with a white hood. The player was captioned to say, "Next stop: Charlottesville," assuming a reference to the 2017 white nationalist rally, where a white nationalist killed a woman with his vehicle. Correa expressed remorse for not being able to welcome attendees to an annual convention hosted by blizzard entertainment held in California. Correa stated disbelief that this type of content was allowed in one of Blizzard's games. The World of Warcraft depicting Hoorigan dressed in white robes with a hood and two characters behind him. One captioned as saying "Next stop: Charlottesville" [3].

The guild brought to light by Congressman Correa, The enclave, appears in multiple game platforms. There are forum threads created by the guild leader horrigan for recruiting members. Horrigan boasts that stormfront officially sponsors. The enclave, a suspected neo-nazism supported and promoter of the white nationalist movement. Horrigan is very active in forums for World of warcraft and reddit. The process of obtaining digital remnants of game interactions is limited. The documented cases of criminal organizations using game environments to camouflage their actions have had little influence on discovery and acquisition.

Research conducted during the following experiments will test the theory of digital remnants found on dead acquisitions of a system containing World of warcraft gameplay. The game files of World of warcraft are heavily encrypted. However, World of warcraft, along with other games, allows for the addition of third-party modifications that interacted with the encrypted game files. The following research will analyze the finding of not only the original game files but also the data associated with common game modifications [4]. Modifications that interact with the game can alter the appearance and functionality of these aspects of gameplay. Analysis of these modification files, stored within the game files, will be analyzed for evidence of player-to-player interactions [5].

Test environment and variables

VM Workstation pro was utilized to create a virtual machine to install and run programs in a sandbox environment to prevent contamination from the host machine. Workstation 15 × with 120 GB of hard disk space was required to run Windows 10 × 64 and the test program World of warcraft.

Common aspects of digital gaming remain the same across several platforms. There is a chat aspect, a virtual currency aspect, and the ability to send and receive in-game items through player-to-player trade or in-game mail. Testing will be done using World of warcraft as a test environment due to its player population size and its use globally. Blizzard entertainment is the creator of many games, including World of warcraft. Finding data in the files of World of warcraft could lead to similar data availability in the many other games they have created.

Blizzard entertainment created World of warcraft and released the game in 2004. The peak number of game subscribers was 12 million in 2010. As of July 2018, the subscriber count was 5.5 million. World of warcraft is the highest-grossing game of all time with $9.23 billion, beating the next highest competitor, crossfire, by over $2 billion.

World of warcraft is a subscriber purchase game, requiring each user to have an account attached to an email address and form of payment. Players interacted with the game and other players in several different ways. The goal of World of warcraft is to create a character and level up through earning experience points. Players can play by themselves or group up with other players in a "party." Players can also join a guild that will act as their "team" within the game. During gameplay, each character will earn items and gold [6]. Because of the social interactions available in the World of warcraft, other reasons to participate in the game include socialization and competition with real-world or online friends.

- Achievers
- Socializers
- Explorers
- killers

These terms would categorize what different players do while logged into the game. Data storage for World of warcraft on each device is done in a way to maximize the gameplay experience. Several different components store data so the program can utilize it: Client- the application installed on the system is the client. The client decodes and displays the games from decoded game data. It also receives input from the user interface, and any game modifications called addons. The client gets feedback from the player and a remote server to change the display accordingly. The player's actions will present themselves as feedback on the graphic interface. The game layout and settings will vary based on this input and output.

Data storage of the client will be on the hard drive of the player's system. Blizzard's proprietary data storage for visual data is in MPQ

- Text-files
- WTF files that open with a text reade

World of warcraft game settings will allow a user to customize format. WAV or MP3 files are the data format for sounds associated with the game. Some of this data is cached for quicker program access. Launcher-the launcher is a small program that provides the user with new information and hyperlinks on the Blizzard website. The launcher will also detect viruses, cheating software, and hacks. The latest downloads and patches will also appear at the launcher. WTF Folder as the client receives and sends data, individual account and character data will be stored in the WTF folder on the hard drive. Data located in this folder will be in the following formats: their gameplay to an extent. The LUA programming files enable full customization of the user interface and display with third-party add-ons or modifications. The addons interact with the game's file structure. These modifications will be the focus of this research [7].

Highly encrypted C++ is the programming language used for World of warcraft. LUA program files have been structured to interact with the encryption to allow input and output of the game content. Proprietary data concerning player-to-player interaction requires the official legal authority of subpoena, affidavit, and warrants to obtain data from Blizzard entertainment. The standard privacy practices of most large account companies comparable to facebook and Google.

The proposed theory is that the LUA programs may log data that would remain on a system without encryption for discovery with standard digital forensic acquisition and analysis. This research will include the installation of World and warcraft and three modification LUA programs. The modifications to World of warcraft chosen for this research are a chat enhancement add-on [8]. The following adjustments are some of the alterations will make to the chat window and gives the user several options to modify the chat window within the World of warcraft even further:

- Displayed player level
- Copy and paste is enabled
- A history of conversations is maintained
- Added icons

Bagnon: It is a customizable inventory add-on. Features with the use of this modification to game files include:

- Color changes based on inventory value and quality
- Item search engine
- Item count and ruleset provided

Z-perl unit frames: Z-Perl replaces the original game unit frames.Added functions of gameplay with the use of Z-Perl include:

- Assist View will monitor the number of other players targeting the same opponent as the user
- Item Check will check all players with the same group or team as the player and determine which items the other players have or do not have.

These modifications will produce a wide range of dataset potential. There are too many addon files available to get an accurate count; a player can find thousands of modification files through source pages [9]. After installation of World of warcraft to the virtual machine, the modification files were installed using a program called Twitch. Twitch is a third-party resource that allows players to upload created modifications, player videos, blogs, and other interactions. Twitch provides for ease of use for downloading, installing, and updating modification files.

Each modification file was installed separately, followed by a test process of player interaction including chat, trading of items between two players, and mailing of objects between two players. After each test, the single installed modification file was uninstalled using twitch. The final test procedure included installing all the modifications to run at the same time during gameplay. This last test was to see if there would be any cross-traffic picked up between the modification files [10].

Results

Analysis tools

- Analysis of files will be completed using:
- Forensic tool kit imager v4.2.0.13
- Autopsy v4.10.0
- DB browser v3.11.2
- Regripper v2.02
- Process monitor v3.5 (Figure 1).

Figure 1. Image verification results created with FTK Imager.

Owner account identification

Asterisks will represent any unique identifying data for account security purposes. Representation of version of the game is in the file path phrase retail, World of warcraft now comes as Retail or Classic. World of warcraft classic is a release of the game in its original form to be compatible with new technology. The initial version of World of warcraft released fifteen years ago. The file structure for both game versions is the same. The standard game files contained the game account name used for testing (Figure 2).

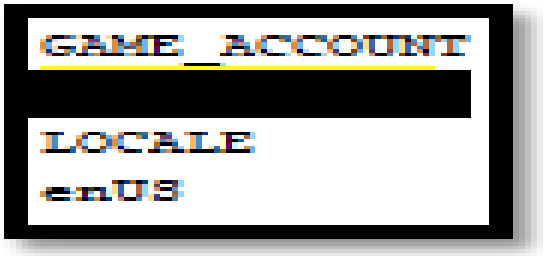


Figure 2. This registry hive data for this account's set region of play.

Region data would be important as it could provide user geographic data. Blizzard entertainment releases game content all over the globe. The REGION data indicates if the account is active on servers based in the United States, Europe, China, or Korea. Reversing of this process to find the region with contents of the WFT folder is achievable. The file path located after the account name would indicate active servers for the account. Stormreaver is the active account server for the test account, stormreaver can be searched and identified as a US Server. Further analysis located more specific user data in the cache folders. Under user files in the registry the following path will provide the Battle Tag or an account ID; \AppData\Local\Battle.net\CashedData.db (Figure 3).

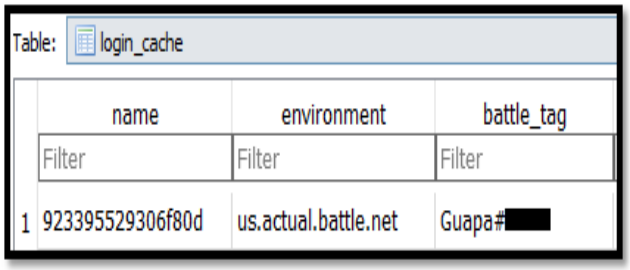


Table: login_cache

	name	environment	battle_tag
	Filter	Filter	Filter
1	923395529306f80d	us.actual.battle.net	Guapa#[redacted]

Figure 3. DB Browser indicated a login_cache producing an environment of us.actual.battle.net and the battle_tag of Guapa #****. The database held the only instance of a located battle_tag without encryption upon complete analysis.

The addition of a player's battle net ID will add the entire account to a "friends list. Without a Battle Net ID, "friends" will show as individual characters. This game tag covers the full battle.net account identity, even if logged into another game owned by Blizzard entertainment. With another player's battle tag, communication is available *via* chat across games, World of warcraft, to Diablo III, for example. Analysis of the WTF files provided identification of individual character data. Storage of individual character data is under the Server file. The character name used for testing purposes was Drorrlock. The following file path provided the location of that individual character data [11].

Modification files

Data storage of modification files installed to interact with World of Warcraft are in the following folder path: The modification files will contain the LUA coding for the modification, any licensing documentation, and texts released with the modification regarding configuring of the modification. Each addon may be composed of several files, and each file will be responsible for a separate ability within the totality of the LUA program. For example, ZPerl contains over fifteen files, each one responsible for a different aspect of the GUI. Details of each addon will be in a .toc-table of contents-file. The .toc file will name the author and version of the addon. The author can also place any notes, instructions, saved variables, and other options within this file. There may be .xml, .txt, .db, and .rtf files located with the LUA addon files as well. Some add-ons are very complex files and will contain more file components than others. Creation of the following files occurred with the installation of the four add-on files in the Add on folder:

- Bagnon
- Bagnon_Config
- Bagnon_GuildBank
- Bagnon_VoidStorage
- Prat-3.0
- Page 4 of 6
- Prat-3.0_Libraries
- ZPerl
- ZPerl_ArcaneBar
- ZPerl_CustomHighlight
- ZPerl_Options
- ZPerl_Party
- ZPerl_PartyPet
- ZPerl_Player
- ZPerl_PlayerBuffs
- ZPerl_PlayerPet
- ZPerl_RaidAdmin
- ZPerl_RaidFrames
- ZPerl_RaidHelper
- ZPerl_RaidMonitor
- ZPerl_RaidPets
- ZPerl_Target

As shown, ZPerl requires several add-on folders to complete all its components. Each file is a separate addon and can be enabled or disabled separately. Each ZPerl file contains a .toc file. After testing was completed using all the add-ons, each file was analyzed and explored for evidence of remaining data from the player to player interactions conducted. The files Access Time was the only change to each file found. Program Files (× 86)\World of Warcraft _retail_\Interface\Addons. As these are the program coding files and other program associated data, it was expected to see little or no change in these folders (Figures 4 and 5). Process Monitor was enabled during gameplay to record any alterations to the system as game playtesting. The Prat and ZPerl add-ons created changes into the account file path: \Program Files (× 86)\World of Warcraft _retail_\WTF\Account********\Stormreaver\Drorrlock\SavedVariables.

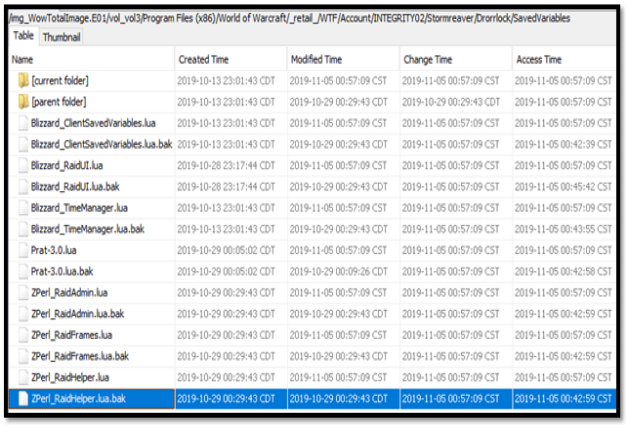
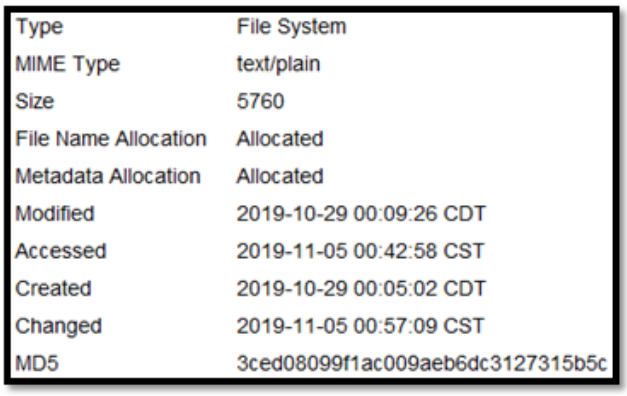

\Img_WowTotalImage.E01/vol_vol3/Program Files (x86)/World of Warcraft/_retail_/WTF/Account/INTEGRITY02/Stormreaver/Drorrlock/SavedVariables

Table | Thumbnail

Name	Created Time	Modified Time	Change Time	Access Time
[current folder]	2019-10-13 23:01:43 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST
[parent folder]	2019-10-13 23:01:43 CDT	2019-10-29 00:29:43 CDT	2019-10-29 00:29:43 CDT	2019-11-05 00:57:09 CST
Blizzard_ClientSavedVariables.lua	2019-10-13 23:01:43 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST
Blizzard_ClientSavedVariables.lua.bak	2019-10-13 23:01:43 CDT	2019-10-29 00:29:43 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:42:39 CST
Blizzard_RaidUI.lua	2019-10-28 23:17:44 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST
Blizzard_RaidUI.lua.bak	2019-10-28 23:17:44 CDT	2019-10-29 00:29:43 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:45:42 CST
Blizzard_TimeManager.lua	2019-10-13 23:01:43 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST
Blizzard_TimeManager.lua.bak	2019-10-13 23:01:43 CDT	2019-10-29 00:29:43 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:43:55 CST
Prat-3.0.lua	2019-10-29 00:05:02 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST
Prat-3.0.lua.bak	2019-10-29 00:05:02 CDT	2019-10-29 00:09:26 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:42:58 CST
ZPerl_RaidAdmin.lua	2019-10-29 00:29:43 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST
ZPerl_RaidAdmin.lua.bak	2019-10-29 00:29:43 CDT	2019-10-29 00:29:43 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:42:59 CST
ZPerl_RaidFrames.lua	2019-10-29 00:29:43 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST
ZPerl_RaidFrames.lua.bak	2019-10-29 00:29:43 CDT	2019-10-29 00:29:43 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:42:59 CST
ZPerl_RaidHelper.lua	2019-10-29 00:29:43 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST	2019-11-05 00:57:09 CST
ZPerl_RaidHelper.lua.bak	2019-10-29 00:29:43 CDT	2019-10-29 00:29:43 CDT	2019-11-05 00:57:09 CST	2019-11-05 00:42:59 CST

Figure 4. Prat crated log files that included chat, trade requests made by the character, items received into inventory, and invites to private groups referred to as "party" in gameplay.



Type	File System
MIME Type	text/plain
Size	5760
File Name Allocation	Allocated
Metadata Allocation	Allocated
Modified	2019-10-29 00:09:26 CDT
Accessed	2019-11-05 00:42:58 CST
Created	2019-10-29 00:05:02 CDT
Changed	2019-11-05 00:57:09 CST
MD5	3ced08099f1ac009aeb6dc3127315b5c

Figure 5. ZPerl file contains a .toc file.

The logs created by Prat were found to be inclusive. Two .lua files remained after testing, one created during the initial trial that stayed after the deletion of the program. The second shows the same creation time as the original but with a modified time upon log out the second test phase. The log files presented the following data:

- Timestamps-each log event is accompanied by a timestamp set to the game time zone setting [12].
- Player name and server-records of the player data for the player on the testing account were available if the parties were in a group. Communication is possible *via* chat cross-server. Analysis that if players were not in a group, the player data did not populate.
- Chat content-logging indicates chat messages to and from the test character. If the players were in a group, the individual character information appears before the chat content [13].
- If the players are not in a party together, then there is a "to" or "from" tag that appears. There is a tag BN_WHISPER that is suspected to mean battle.net whisper-a whisper is a term used for a private message in-game. Logs included chat even though the player that sent the whisper was playing in World of Warcraft classic, a different game platform. Trade requests-when the test account was used to initiate a trade, the request was logged. Inventory received-items received into inventory logs appeared with each addition. This action did not change when multiple items were traded or mailed at the same time. No indication about the method of acquiring the object was present [14].
- The screenshots below show artifacts found in the .LUA files created using Prat 3.0. Highlighted data include: screenshots, player/server data, actions, inventory items, and chat contents [15].

1, -- [2]
0.5019608139991776, -- [3]
1, -- [4]
10, -- [5]
False, -- [6]
1, -- [7]
2, -- [8]
0, -- [2]
}, -- [1]
1, -- [3]
0.99647059440612793, -- [4] 52, --
[5]
Fasle, -- [6]
4, -- [7]
5, -- [8]
}, -- [3]
1, -- [2]
1, -- [3]
0, -- [4]
1, -- [5]
False -- [6]
10, -- [7]
11, -- [8] 1,
-- [2]
1, -- [3]
0, -- [4]
1, -- [5]
False, -- [6]
10, -- [7]
11, -- [8] 1,
-- [2]
1, -- [3]
0, -- [4]
1, -- [5]
False, -- [6]
3, -- [7]
4, -- [8]
O, -- [2]
0.666666865348816, -- [3] 0, --[4]
28, -- [5]
False, -- [6]
11, -- [7]
12, -- [8]
}, -- [29]
0, -- [2] 0.6666666865348816, -- [3]
6, -- [4]

28, – [5]

False, – [6]

11, – [7]

13, – [8]

Discussion

Throughout the past fifteen years, law enforcement has suspected digital gaming environments shielding criminal activity discovery. Often, the amount of data input these games receive leaves little way of monitoring for suspicious activity. This paper has discussed an enormous project undertaken by agencies to data-mine data to understand the trends and ongoings of criminal enterprises and groups. The suspected utilization of online gaming to camouflage criminal activity leads to a lengthy process of attaining legal authority to obtain records-retention of records, subpoenas, affidavits, and warrants. The international activity can become a jurisdiction issue. These companies retain records for a potentially short time frame also.

Research has overlooked the retention of digital evidence that does not require a legal authority to acquire. Keylogging software has shown minor success but requires access to the target system to install. Besides major data mining projects and keylogging software, very few published attempts to obtain data is available. There were no published attempts to acquire data from third-party software that is built to interact with the game files located. Analysis completed discovering player-to-player interaction evidenced by analysis of three popular modification-addon-files that interact with World of Warcraft. While the game itself is heavily encrypted, the add-on files are not. The use of C++ for the language of the game files; LUA is the code language for add-on files. The three add-on programs tested were Prat, Bagnon, and Zperl.

Conclusion

To allow for testing, completed interaction in the way of chat, trading of inventory, and sending items through in-game mail was done. Analyzation of the files associated with the add-on stored within the World of Warcraft game files in search of evidence of the interactions followed. The study included registry data for additional evidence that may remain. The identification of the target account came through registry data and game file information. Logs generated by Prat 3.0 included detailed chat logs. These logs included player character and server identification, chat communication logs, trade requests, and instances of adding items to the player's inventory. Player character and server identity was only available if the interacting players were in a group or party. Logs included chat between games owned by Blizzard entertainment, but no player identification was possible in those instances. Information indicated if the message was incoming or outgoing without identifying data for the recipient or sender.

Three of many addons were tested, leading to the discovery of digital evidence of interactions between players in World of warcraft. Third-party modification files are allowed in many digital platforms, not limited to World of warcraft or games created by Blizzard Entertainment. These modifications have become more sophisticated, at times communicating with accounts having the same add-ons. The possibility exists that more of these programs log data about events that occur within the game environment. This research shows that there is the potential to gain evidentiary items from game files located on a suspect system. There may be data present that could assist with probable cause or expedite information availability in time-sensitive situations. Where data was expected once to be proprietary may become accessible to investigators by the system user unbeknownst to them. Where a game environment may not be an anticipated source of evidentiary value that may change if there is readily available data to be searched.

References

1. Chen, Ying Chieh, Chen PS, Hwang JJ, and Korba L, et al. "An Analysis of Online Gaming Crime Characteristics." *Internet Res* 3 (2005): 246-261.
2. Wilson, Tracy V. "How World of Warcraft Works." *How Stuff Works* 16 (2007).
3. Hamilton, David. "Charlottesville." *Iowa Review* 3 (2018): 188.
4. De Paoli, Stefano. "Automatic-Play and Player Deskilling in MMORPGs." *Game Stud* 1 (2013): 12-21.
5. Kirschner, David, and Williams JP. "A Microsociological Perspective on Non-Verbal Communicative Strategies in MMORPGS." Nonverbal *Commun Virtual Worlds* (2014): 307-322.
6. De Paoli, Stefano, and Kerr A. " We Will Always Be One Step Ahead of Them" A Case Study on the Economy of Cheating in MMORPGs." *J Virtual worlds Res* 4 (2010).
7. Suznjevic, Mirko, Dobrijevic O, and Matijasevic M. "MMORPG Player Actions: Network Performance, Session Patterns and Latency Requirements Analysis." *Multimed Tools Appl* 1 (2009): 191-214.
8. Ashton, Martin, and Verbrugge C. "Measuring Cooperative Gameplay Pacing in World of Warcraft." *Proceed Int Confer Foundat Digital Games* (2011): 77-83.
9. Bryant, Blake, and Saiedian H. "An Evaluation Of Videogame Network Architecture Performance And Security." *Comput Netw* 192 (2021): 108-128.
10. Kuo, Andrew, Hiler JL, and Lutz RJ. "From Super Mario to Skyrim: A Framework for the Evolution of Video Game Consumption." *J Consum Behav* 2 (2017): 101-120.
11. Kaltman, Eric, Osborn J, and Fruin NW. "From the Presupposition of Doom to the Manifestation of Code: Using Emulated Citation in the Study of Games and Cultural Software ." *Digit Humanit* Q 1 (2021).
12. Gainsbury, King, Delfabbro P, Hing N, and Derevensky J. "The Use of Social Media in Gambling." *Gambling Res Australia* (2015): 2019-2109.
13. Margitay-Becht, András. "Teaching economics in world of Warcraft." *Eme Tools Appl Virtual Real Edu* (2016): 121-144.
14. Lowry, Sharon K. "Property Rights in Virtual Reality: All's Fair in *Life and Warcraft.*" 15 (2008): 109.
15. Rogers, Suzanne E. "Transforming with Avatars: Video Game Developer Licensing Considerations ." *J Copyright Soc* 65 (2018): 57.

How to cite this article: Schneider, Kayla J. "MMORPG Data Recovery from Player to Player Interactions: Dead Acquisition Including Game Modification Files." *J Appl Comput Math* 11 (2022): 476.