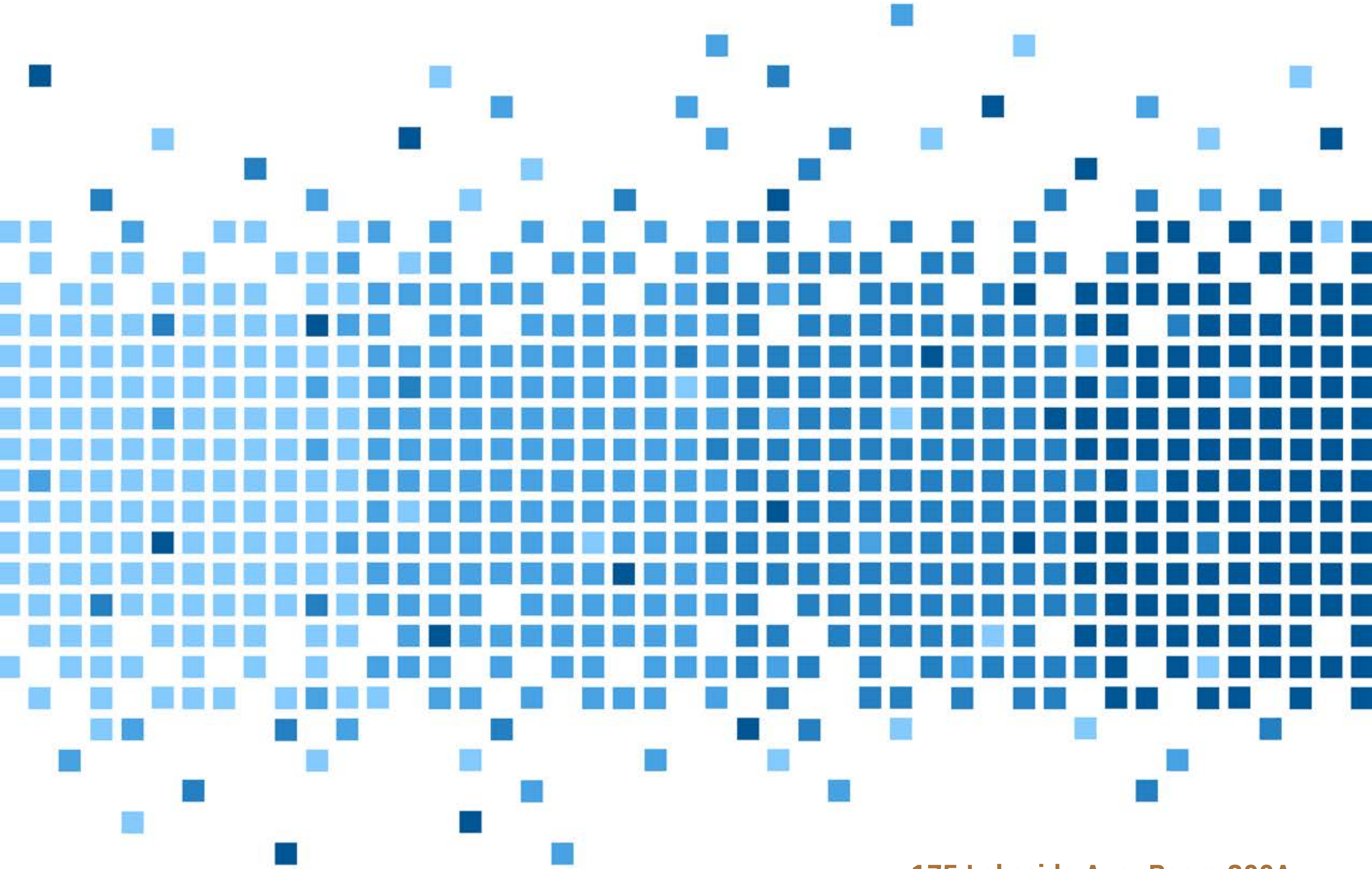
CHAMPLAIN COLLEGE | LCDi Leahy Center for Digital Investigation

[Massively Multiplayer Online Role Playing Game Chat]



175 Lakeside Ave, Room 300A
Phone: (802)865-5744
Fax: (802)865-6446
http://www.lcdi.champlain.edu

1/21/2016

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction

Massively Multiplayer Online Role Playing Games (MMORPGs) have exploded in popularity since their introduction to the gaming community. These games often boast large worlds inhabited by thousands of players at any given time, where they work together or face off against one another as they constantly strive to improve their individual characters. Well-known MMORPGs like Blizzard Entertainment's World of Warcraft have huge user bases, with millions of subscribers populating their servers. Because teamwork is often the key to succeeding in an MMORPG, users can communicate with each other using Voice Over Internet Protocol (VoIP), as well as in-game chat systems similar to instant messaging platforms such as AOL Instant Messenger. The way these systems function differs from game to game, but most MMORPGs allow text communication between players and/or in-game character emotes such as dancing or laughing. Our team selected three MMORPGs to investigate by evaluating the most popular games, selected through online research and a campus-wide community outreach survey conducted by the LCDI's media relations team.

Background:

Prior research performed by the Digital Forensics Investigator News in May of 2010 set the precedent for this investigation through their analysis of the MMORPG Everquest II. This study showcased the use of a setting within the game that created logs of user commands stored locally on the player's machine; in particular, they noted that the log contained the entirety of the in-game chat the player picked up during the play session, and even archived the username of the message's sender and its intended recipient. The LCDI decided to further their research into in-game chat mechanics and determine whether other MMORPGs would store chat logs locally on the user's system in a similar fashion. This project was conducted to assess the potential value of these chat logs from a digital forensics standpoint. This research becomes particularly relevant when looking at the potential for online child predators to use this technology, and whether to data found could be upheld in a court. An article published from an officer training course run by the state of California talks about the potential for MMORPGs to be used by predators to target children from afar. Shelly Veen, the author of the piece, stated that "one of the most dangerous realities of the virtual world are the predators who have staked out territory of their own" (Veen, 2). Although many believe that children are safe from harm while using a computer, predators can still persuade them into revealing information that may put them in danger, such as their age or location. This makes the records of conversations between suspected predators and children extremely useful to investigators. The only way to prove predatory behavior over the Internet without an eyewitness is to conclusively prove that there was online contact between the predator and child. Beyond this, however, chat logs may prove useful in other disputes requiring a digital forensic investigation, such as to reinforce an alibi by affirming that someone was online and active at a certain time or provide concrete evidence of an incriminating conversation. While deciding the scope of this project, the MMO Forensics team decided to test multiple games from different developers to get a broader image of the genre as a whole and identify trends in the mechanics of these types of video games. We decided to test three MMORPGs based on their popularity and other unique traits within the games that the team felt would be useful to explore. The first MMORPG we decided to investigate, primarily for its overwhelming popularity, was World of Warcraft. Released in 2004, World of Warcraft (WoW) is a veteran MMORPG with an expansive community, making it ideal for our project. We believed a game as popular as World of Warcraft would also be fairly well polished and user friendly, which would hopefully make investigating it less difficult. The second MMORPG we chose to test was Guild Wars 2, which caught our eye because of its recent update, an expansion called Heart of Thorns. The game's active development was a sign that its functionality was being constantly improved and it would be more likely for us to see logging functions within it. However, through our research on Guild Wars 2 we were unable to confirm that it had any built in chat logging functionality, which made us curious about whether the modifications would result in any new features or bugs that could be used to create a chat log in the base game. Note that we performed all tests on the base version of the game only. The third game the team decided to test was PlanetSide 2, which was developed by Everquest II creators Daybreak Games. This led us to wonder if the same chat logging functions would be present in their newer product.

Purpose and Scope:

The goal of this project is to determine what artifacts are left by World of Warcraft, Guild Wars 2, and PlanetSide 2 when using their in-game text chat systems. With millions of people playing MMORPGs, it would be beneficial for forensics examiners to know what chat artifacts, if any, can be extracted from these games. With this project, we also aim to identify how game settings can affect what an MMORPG records, and how that may benefit or harm a digital forensic investigation.

Research Questions:

1. What artifacts or logs do MMORPGs create when a player uses the in-game text chat? Where are they stored?
2. What settings exist that expand or limit what artifacts or logs are created and stored?
3. What do these artifacts and logs reveal about the in-game chat and could they be beneficial during an investigation?

Terminology:

Artifacts - Artifacts are any data generated by user interaction that can be collected and examined. Any user data retrieved from the browser is considered an artifact, including cookies, caches, geolocation, search history, etc.

Disk Image - A disk image is a copy of a hard drive that is compressed into a series of files.

Disk Wipe - The process of removing all data from a hard drive by overwriting it with random characters or 0s.

EnCase- EnCase is a suite of digital forensics tools created by Guidance Software. The software comes in several forms designed for forensic, cyber security, and e-discovery use.

Expansion - When a company releases new content such as characters, events, or explorable areas to a pre-existing game.

Forensic Toolkit (FTK) - Forensic Toolkit or FTK, is a forensic tool made by AccessData. FTK allows users to acquire, process, and verify evidence. FTK supports many image formats.

Full Chat log - A chat log that displays both sides of a conversation (both messages sent from target computer and to target computer are recorded).

Game Client - The launcher for a game, typically the file you download from the game company's website.

Guild Wars 2 - Guild Wars 2 is an MMORPG that allows the player to pick a race and a profession, and then immerses the player into an extensive world that has a wide range of events and a personalized storyline. The game is appealing due to the lack of subscription fees and the ability to play the game without buying its expansion.

Internet Evidence Finder (IEF)- Internet Evidence Finder is a forensic software created by Magnet Forensics that is capable of recovering internet artifacts in areas such as: cloud artifacts, instant messenger chat logs, media, mobile backup files, P2P file sharing, social networking site content, webmail applications, web related activity, and web page recovery**MMORPG -** Massively Multiplayer Online Role Playing Game.

NVIDIA Shadowplay- NVIDIA Shadowplay is a program that records in game and full desktop capture at up to 4K resolution at 130Mbps for an unlimited amount of time while in manual mode. [2]**Partial Chat log** - A chat log that only records half of the conversation (Only messages sent from target computer are recorded).

PlanetSide 2 - PlanetSide 2 is a first-person shooter style MMORPG where the player chooses one of three factions and becomes involved in a ceaseless three-way war. Players also chose a class that will affect their play style, available weapons, and abilities. This free to play game is attractive to both casual players and veteran MMORPG players as you can play the game as a simple multiplayer shooter or delve into the backstories and causes of hatred between the three factions.

World of Warcraft - World of Warcraft (WoW) is an online Massively Multiplayer Online Role Playing Game where the player selects a side to represent alliance, horde or pandaren. Each of these alliances has different species associated with them that the player can select from and roleplay as. (Please note that we were using the trial version of the game.)

Write Blocker - A device that is plugged in between a computer and a hard drive that allows the computer to read information to the disk but does not allow any writing to the disk. In other words the write blocker prevents the disk from being edited in any way, preserving the disk as it was.

Internet Evidence Finder (IEF)- Internet Evidence Finder is a forensic software created by Magnet Forensics that is capable of recovering internet artifacts in areas such as: cloud artifacts, instant messenger chat logs, media, mobile backup files, P2P file sharing, social networking site content, webmail applications, web related activity, and web page recovery. The version of Internet Evidence Finder used for this project was 6.7.1.0501.

Methodology and Methods

The MMO Forensics team generated data for this project using LCDI workstation computers, each containing an installation of the games selected for testing (World of Warcraft, PlanetSide 2, and Guild Wars 2). The team members played each MMORPG to generate chat data between the two LCDI accounts and simulating real players as much as possible (completing missions, exploring, fighting, etc.) while facilitating conversation with the other team members. Each team member individually generated approximately one hour of conversation in each MMORPG. While the chat data was being generated, it was also being recorded on the LCDI workstation computers using the NVIDIA GeForce game capture software Shadowplay. These recordings allowed us to compare any log findings with what occurred during the gaming sessions. Once an hour of chat data had been recorded, the team began analyzing the MMORPG’s files to identify the location and contents of any logs with recorded chat data. Based on the results of the initial test, the team then modified the game settings in an attempt to create logs that contain chat data. Based on this procedure, the MMORPG team generated a total of six hours’ worth of chat data.

Equipment Used

Name	Version
EnCase	7.10.00.103
Forensic Toolkit (FTK)	5.5.0.44
Internet Evidence Finder (IEF)	6.7.1.0501
NVIDIA Shadowplay	N/A
4TB External Drive	N/A
Wiebetech Forensic Ultradock	V4

	Project 2 Computer	Project 3 Computer
Memory	16.00 GB RAM (15.90 GB usable)	16.00 GB RAM (15.89 GB usable)
Processor	Intel(R) Core(™) i7-3770K CPU@3.50 Ghz	Intel(R) Core(™) i7-3770K CPU@3.50 Ghz
Hard Drive Size	1 TB	1 TB
Operating System	Microsoft Windows 7 Enterprise	Microsoft Windows 7 Enterprise
Computer Name	Project2	Project3
GPU	GeForce GTX 650 Ti	GeForce GTX 650 Ti

MMORPG	Version/ Build (installed - last used)
World of Warcraft	6.2.2a - 6.2.2.3
Guild Wars 2	53,120 - 55,043
PlanetSide 2	Hotfix 09/09 - Hotfix 11/3

Data Collection:

This project involved two characters created by team members interacting with each other in common MMORPG situations. It should be noted that while efforts were made to make conversations as organic and akin to conversation actual players would have in an MMORPG, these games are not well-known for being friendly to players attempting to have extensive conversation with one another on the chat interface. Therefore, in order to efficiently generate a full hour of chat data, it was sometimes necessary to remove ourselves from the action of the game and find a quiet location in order to prevent our chat screens from becoming cluttered by the conversations of nearby players. The chats were recorded through screen recordings taken with Shadowplay and physically archived by the players.

To begin the project, two computers had to be configured to accommodate the specific software and hardware requirements for each game. These computers met or exceeded the minimum requirements to run any program necessary for data generation and/or screen recording. Once the machines were configured, the game clients and programs needed for data generation were installed. Two accounts were then created per game and the team was split into three groups, each assigned to a different MMORPG to create efficient in-game chat data in a timely manner.

Analysis

From the start of this project we expected that many MMORPGs would not have full chat logs stored locally onto the player’s system. Based on our research into Everquest II we believed that most games would not store logs locally to lessen the amount of space taken up by game files on the user’s hard drive. We did hypothesize, however, that it was entirely possible for some MMORPGs to have a function like Everquest II, where partial chat logs are stored locally on the player’s system after in-game settings were changed. Our investigation was conducted to learn what was being stored by default and what the user could manipulate based on different settings the game allowed them to configure.

The initial round of data generation took significantly longer than expected due to unforeseen setbacks such as troubleshooting NVIDIA Shadowplay to record game sessions properly and the inability to create multiple accounts using one email. After the initial round of data generation on the workstations, the hard drives were imaged and then wiped. Wiping the hard drive ensured that we had a clean slate for the second round of data generation. We then repeated the data generation process altering certain in-game settings such as /log level in Planetside 2 and /chat log in World of Warcraft. We believed these settings would create chat logs, based on the results gathered from the first round of data generation and research into the game’s settings. For the second round of data generation we also investigated the pagefile.sys and hyberfil.sys of each hard drive to see if they could provide relevant evidence.

To look at the data in a stable, forensically sound environment, we imaged the hard drives of both machines using the Wiebetech write blocker. The images were written to our 4TB hard drive so that they could be accessed by any team member without taking up terabytes of network storage. Once the drives were imaged, we imported the images into Encase to view all relevant files. The Encase case files were also stored on the 4TB hard drive. We also did a brief pass with Internet Evidence Finder, which has a built in utility for finding World of Warcraft logs. This pass was done on the image itself with all options besides the World of Warcraft Chat option, which is option 24 of 25 in chat subset of IEF, disabled.

Results

We did not find anything in either of the pagefile.sys or hyberfil.sys files; however, it should be noted that this may be due to the specifications of our computers. It is entirely possible that our systems simply never needed to use their respective pagefile.sys and hyberfil.sys files to store game data, as these files store data that no longer fits in the machine's RAM and the workstations utilized had more than enough memory to accommodate the needs of the game. It may still be worthwhile to investigate these locations especially if a system's hardware is closer to the minimum requirements for the game. We also did not find any hidden chat logs in World of Warcraft when running Internet Evidence Finder over the image from the first round of data generation. Overall in both Planetside 2 and World of Warcraft, we were able to recover logs that could be beneficial to an investigation provided the settings had already been adjusted accordingly. This means that while these logs can prove valuable in cases it is unlikely that they will be usable unless chat logging is manually enabled.

PlanetSide 2:

We have confirmed from our testing that PlanetSide 2 does not have an official chat log function. However, it does have a command called /log level that will produce a partial chat log. /Loglevel is set to zero (off) by default and can be set to different levels ranging from one to six, six providing the most extensive log. /Loglevel is designed with the various levels so that the user can choose how detailed of a log they would like. If they only want a minimalistic log, they can set /loglevel appropriately so they do not have to sift through a large log file to find the information they are looking for. Note that the full command requires another parameter called local, so the full command is /loglevel local <0-6>. The information we were searching for was found in the command queue and, based on our research, was found at the following levels:

Table 1: PlanetSide 2 Logging Levels

Log Level	Results
0	No logging
1	No log files were created
2	CommandQueue (limited)
3	CommandQueue (limited), various error logs
4	CommandQueue (limited), various error logs, some asset usage logs
5	Command Queue (limited) various error logs, more asset usage logs
6	Command Queue (full) all error logs, all usage logs

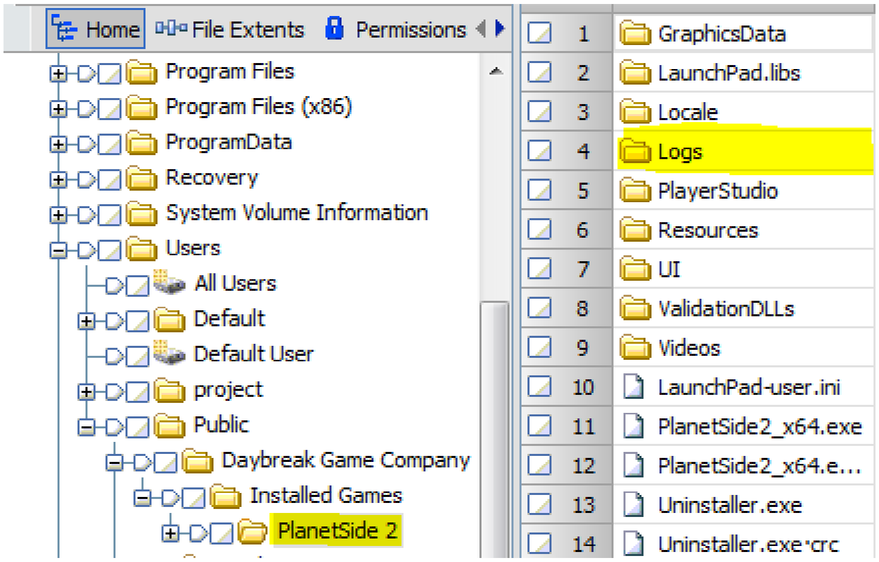
Any logging files that were created were stored in C:/Users/Public/DaybreakGameCompany/Installed Games/PlanetSide2/Logs. When /loglevel 2-6 was enabled, one of the files it created is called CommandQueue, which is where the player's commands are recorded and where the system acknowledges if the command was run successfully. The CommandQueue was limited at lower levels and would not start logging chat commands until it was set on level five, and would not record the actual text being sent until it was set to level 6. See Figure 2: Command Queue Log as Opened in a Text Document to see the command queue log created by a /loglevel 6 command.

Therefore, for the purposes of creating a chat log, the only level that was particularly useful was /loglevel 6. While only a partial chat log, it did allow us to have a complete record of one side of the conversation. Unfortunately, because it was not a formal log other commands may be required to follow a timeline of a full conversation. It is important to note that the logs only save the current session's chat information, meaning that once the MMORPG was relaunched, the log file would be purged and /loglevel would be reset to 0. This means, for continual logging in Planetside 2, it is necessary to save log files to an alternate location when done playing and to set loglevel back to 6 when you next log back into the game.

From our work in EnCase, we have confirmed that no special steps had to be taken with the logs after they had been deleted. In other words, the logs will still exist on the hard drive until they were overwritten and, depending on the user's frequency of play and their system specifications; an investigator could potentially recover these log files. See Figure 1 below to see how the log appears in EnCase, Figure 2 to see how the log appears when opened as a text document, or Figure 3 to see the overwritten logs in EnCase.

These findings were largely expected from PlanetSide 2 due to the previous studies of games produced by its developer. The log functionality in PlanetSide 2 reports in a manner similar to Everquest's, which leads us to infer that this could be Daybreak Game's standard method of chat logging.

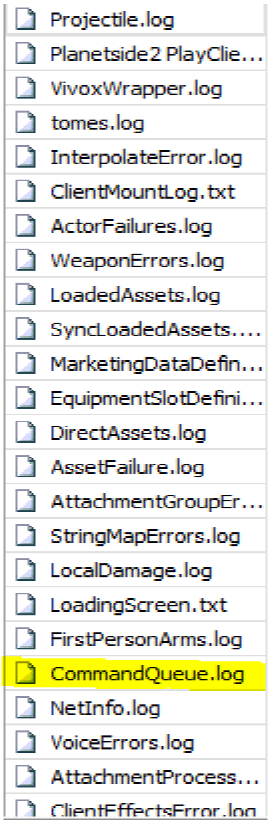
Figure 1: EnCase View of CommandQueue



- Program Files
- Program Files (x86)
- ProgramData
- Recovery
- System Volume Information
- Users
  - All Users
  - Default
  - Default User
  - project
  - Public
    - Daybreak Game Company
      - Installed Games
        - PlanetSide 2

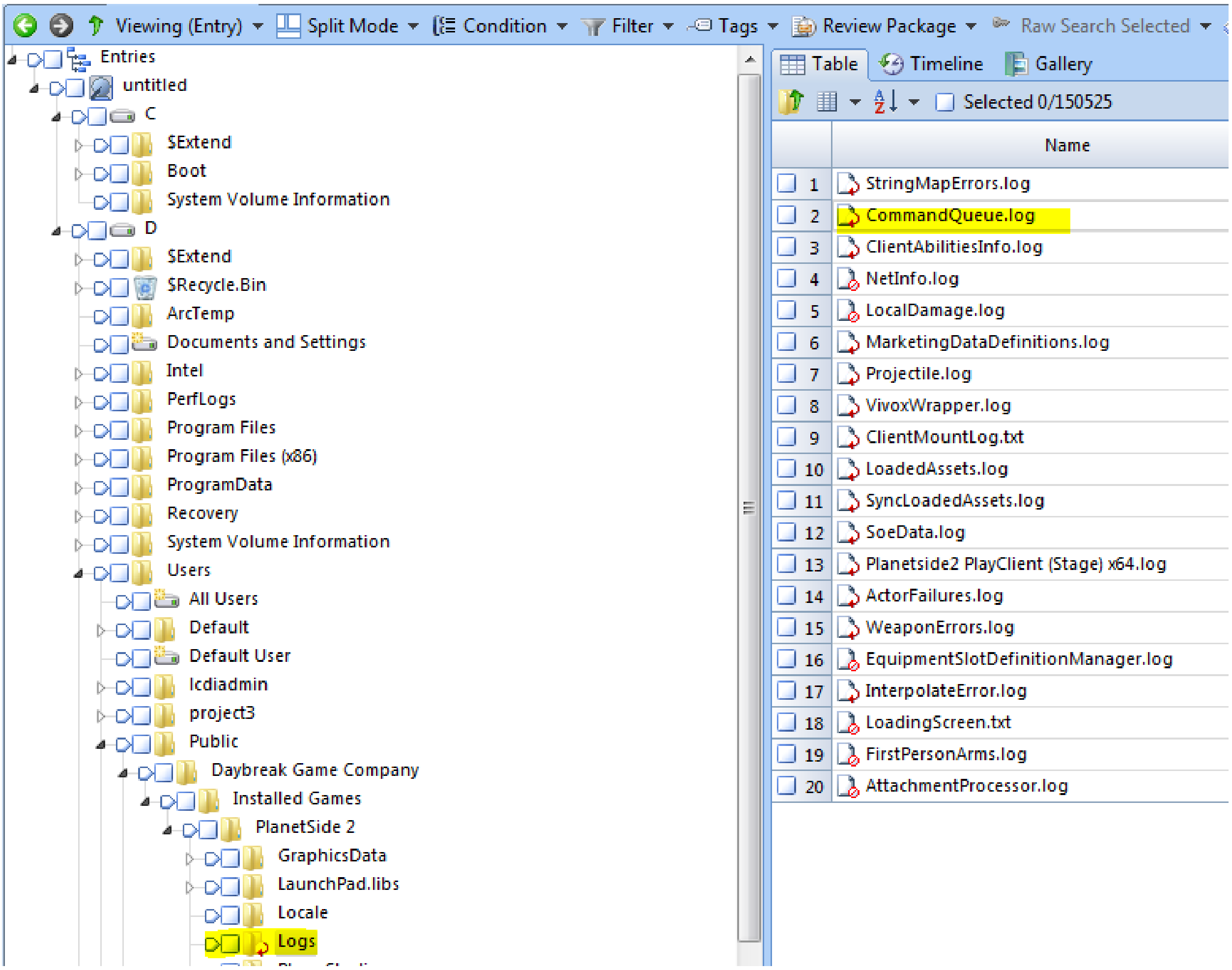
1	GraphicsData
2	LaunchPad.libs
3	Locale
4	Logs
5	PlayerStudio
6	Resources
7	UI
8	ValidationDLLs
9	Videos
10	LaunchPad-user.ini
11	PlanetSide2_x64.exe
12	PlanetSide2_x64.e...
13	Uninstaller.exe
14	Uninstaller.exe·crc

Figure 2: Command Queue Log as Opened in a Text Document



- Projectile.log
- Planetside2 PlayClie...
- VivoxWrapper.log
- tomes.log
- InterpolateError.log
- ClientMountLog.txt
- ActorFailures.log
- WeaponErrors.log
- LoadedAssets.log
- SyncLoadedAssets....
- MarketingDataDefin...
- EquipmentSlotDefini...
- DirectAssets.log
- AssetFailure.log
- AttachmentGroupEr...
- StringMapErrors.log
- LocalDamage.log
- LoadingScreen.txt
- FirstPersonArms.log
- CommandQueue.log
- NetInfo.log
- VoiceErrors.log
- AttachmentProcess...
- ClientEffectsError.log

Figure 3: Log Files After Next-day Log Purge



- Entries
  - untitled
    - C
      - $Extend
      - Boot
      - System Volume Information
    - D
      - $Extend
      - $Recycle.Bin
      - ArcTemp
      - Documents and Settings
      - Intel
      - PerfLogs
      - Program Files
      - Program Files (x86)
      - ProgramData
      - Recovery
      - System Volume Information
      - Users
        - All Users
        - Default
        - Default User
        - lcdiadmin
        - project3
        - Public
          - Daybreak Game Company
            - Installed Games
              - PlanetSide 2
                - GraphicsData
                - LaunchPad.libs
                - Locale
                - Logs

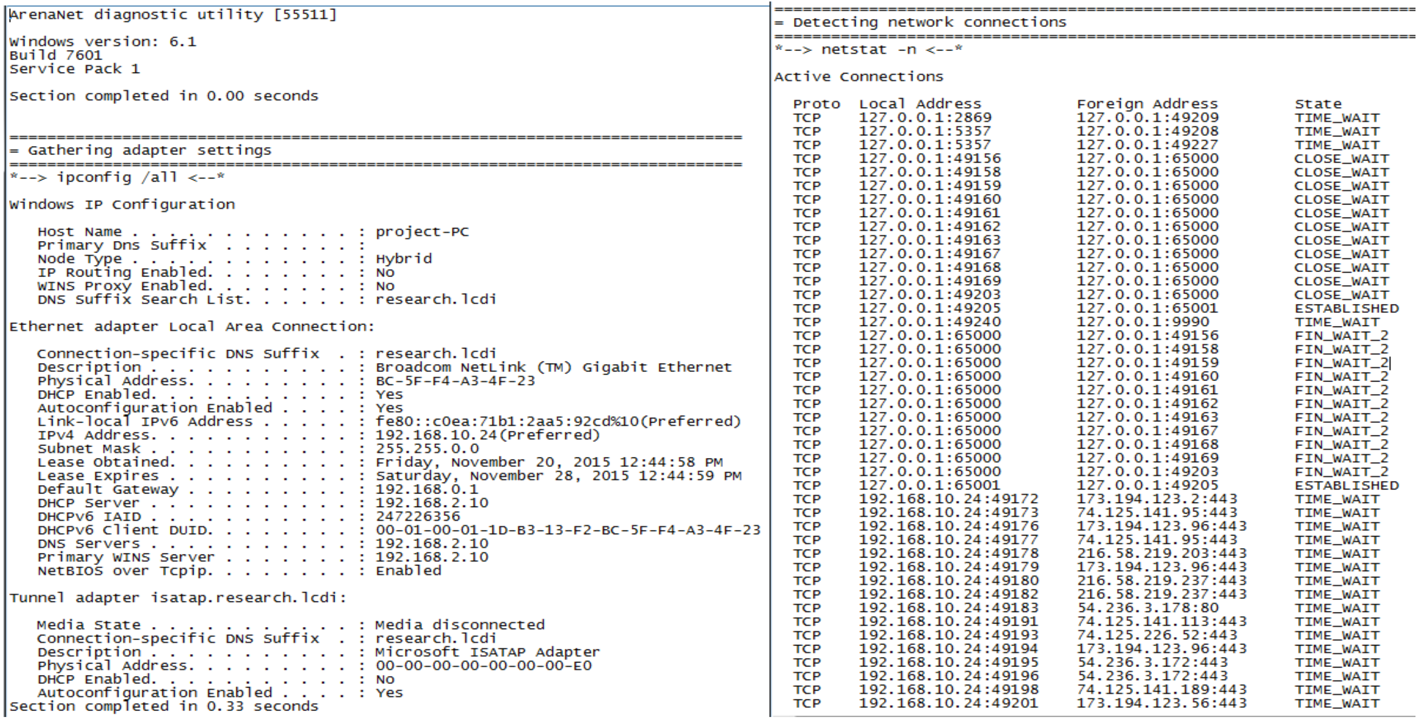
Selected 0/150525

	Name
1	StringMapErrors.log
2	CommandQueue.log
3	ClientAbilitiesInfo.log
4	NetInfo.log
5	LocalDamage.log
6	MarketingDataDefinitions.log
7	Projectile.log
8	VivoxWrapper.log
9	ClientMountLog.txt
10	LoadedAssets.log
11	SyncLoadedAssets.log
12	SoeData.log
13	Planetside2 PlayClient (Stage) x64.log
14	ActorFailures.log
15	WeaponErrors.log
16	EquipmentSlotDefinitionManager.log
17	InterpolateError.log
18	LoadingScreen.txt
19	FirstPersonArms.log
20	AttachmentProcessor.log

Guild Wars 2:

Guild Wars 2 proved to be quite elusive when it came to logging in-game chat. Despite our best efforts, we could not retrieve any form of chat log out of Guild Wars 2. This is actually a well-known issue in the Guild Wars 2 community as we found a number of forum posts on various websites that all denote the fact that there is currently no way to record or save chat conversation in game without manually taking screenshots (Eggman, 1405). Once we discovered the well-documented lack of logging functionality in Guild Wars 2, we broke procedure and did not perform a second set of data generation, having concluded that nothing would be gained by altering settings. However, we did find a command line argument, -diag, which creates a report of basic information about the user's computer and its network status. –diag is appended to the end of the file path of a user created shortcut pointing to the game as a launch setting. To read more about how to setup a shortcut with a command line argument, see this page on command line arguments on the official Guild Wars 2 Wiki. After analyzing -diag, we discovered that the command simply runs ipconfig /all and netstat –n in the command terminal. While this records a large amount of information and is a surprisingly powerful network diagnostic tool, it does not record any chat information.

Figure 4: View of –diag command



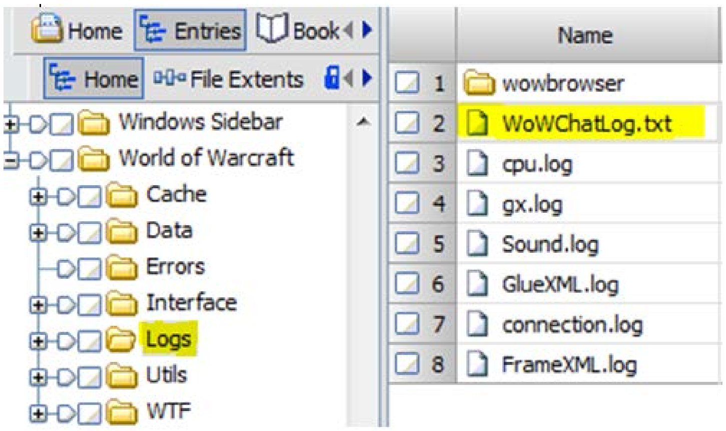
```
ArenaNet diagnostic utility [55511]

Windows version: 6.1
Build 7601
Service Pack 1

Section completed in 0.00 seconds


================================================================================
= Gathering adapter settings
================================================================================
*--> ipconfig /all <--*

Windows IP Configuration

   Host Name . . . . . . . . . . . . : project-PC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : research.lcdi

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : research.lcdi
   Description . . . . . . . . . . . : Broadcom NetLink (TM) Gigabit Ethernet
   Physical Address. . . . . . . . . : BC-5F-F4-A3-4F-23
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c0ea:71b1:2aa5:92cd%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.24(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Lease Obtained. . . . . . . . . . : Friday, November 20, 2015 12:44:58 PM
   Lease Expires . . . . . . . . . . : Saturday, November 28, 2015 12:44:59 PM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.2.10
   DHCPv6 IAID . . . . . . . . . . . : 247226356
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1D-B3-13-F2-BC-5F-F4-A3-4F-23
   DNS Servers . . . . . . . . . . . : 192.168.2.10
   Primary WINS Server . . . . . . . : 192.168.2.10
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.research.lcdi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : research.lcdi
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
Section completed in 0.33 seconds
```

```
======================================================================
= Detecting network connections
======================================================================
*--> netstat -n <--*

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:2869         127.0.0.1:49209        TIME_WAIT
  TCP    127.0.0.1:5357         127.0.0.1:49208        TIME_WAIT
  TCP    127.0.0.1:5357         127.0.0.1:49227        TIME_WAIT
  TCP    127.0.0.1:49156        127.0.0.1:65000        CLOSE_WAIT
  TCP    127.0.0.1:49158        127.0.0.1:65000        CLOSE_WAIT
  TCP    127.0.0.1:49159        127.0.0.1:65000        CLOSE_WAIT
  TCP    127.0.0.1:49160        127.0.0.1:65000        CLOSE_WAIT
  TCP    127.0.0.1:49161        127.0.0.1:65000        CLOSE_WAIT
  TCP    127.0.0.1:49162        127.0.0.1:65000        CLOSE_WAIT
  TCP    127.0.0.1:49163        127.0.0.1:65000        CLOSE_WAIT
  TCP    127.0.0.1:49167        127.0.0.1:65000        CLOSE_WAIT
  TCP    127.0.0.1:49168        127.0.0.1:65000        CLOSE_WAIT
  TCP    127.0.0.1:49169        127.0.0.1:65000        CLOSE_WAIT
  TCP    127.0.0.1:49203        127.0.0.1:65000        CLOSE_WAIT
  TCP    127.0.0.1:49205        127.0.0.1:65001        ESTABLISHED
  TCP    127.0.0.1:49240        127.0.0.1:9990         TIME_WAIT
  TCP    127.0.0.1:65000        127.0.0.1:49156        FIN_WAIT_2
  TCP    127.0.0.1:65000        127.0.0.1:49158        FIN_WAIT_2
  TCP    127.0.0.1:65000        127.0.0.1:49159        FIN_WAIT_2
  TCP    127.0.0.1:65000        127.0.0.1:49160        FIN_WAIT_2
  TCP    127.0.0.1:65000        127.0.0.1:49161        FIN_WAIT_2
  TCP    127.0.0.1:65000        127.0.0.1:49162        FIN_WAIT_2
  TCP    127.0.0.1:65000        127.0.0.1:49163        FIN_WAIT_2
  TCP    127.0.0.1:65000        127.0.0.1:49167        FIN_WAIT_2
  TCP    127.0.0.1:65000        127.0.0.1:49168        FIN_WAIT_2
  TCP    127.0.0.1:65000        127.0.0.1:49169        FIN_WAIT_2
  TCP    127.0.0.1:65000        127.0.0.1:49203        FIN_WAIT_2
  TCP    127.0.0.1:65001        127.0.0.1:49205        ESTABLISHED
  TCP    192.168.10.24:49172    173.194.123.2:443      TIME_WAIT
  TCP    192.168.10.24:49173    74.125.141.95:443      TIME_WAIT
  TCP    192.168.10.24:49176    173.194.123.96:443     TIME_WAIT
  TCP    192.168.10.24:49177    74.125.141.95:443      TIME_WAIT
  TCP    192.168.10.24:49178    216.58.219.203:443     TIME_WAIT
  TCP    192.168.10.24:49179    173.194.123.96:443     TIME_WAIT
  TCP    192.168.10.24:49180    216.58.219.237:443     TIME_WAIT
  TCP    192.168.10.24:49182    216.58.219.237:443     TIME_WAIT
  TCP    192.168.10.24:49183    54.236.3.178:80        TIME_WAIT
  TCP    192.168.10.24:49191    74.125.141.113:443     TIME_WAIT
  TCP    192.168.10.24:49193    74.125.226.52:443      TIME_WAIT
  TCP    192.168.10.24:49194    173.194.123.96:443     TIME_WAIT
  TCP    192.168.10.24:49195    54.236.3.172:443       TIME_WAIT
  TCP    192.168.10.24:49196    54.236.3.172:443       TIME_WAIT
  TCP    192.168.10.24:49198    74.125.141.189:443     TIME_WAIT
  TCP    192.168.10.24:49201    173.194.123.56:443     TIME_WAIT
```

World of Warcraft:

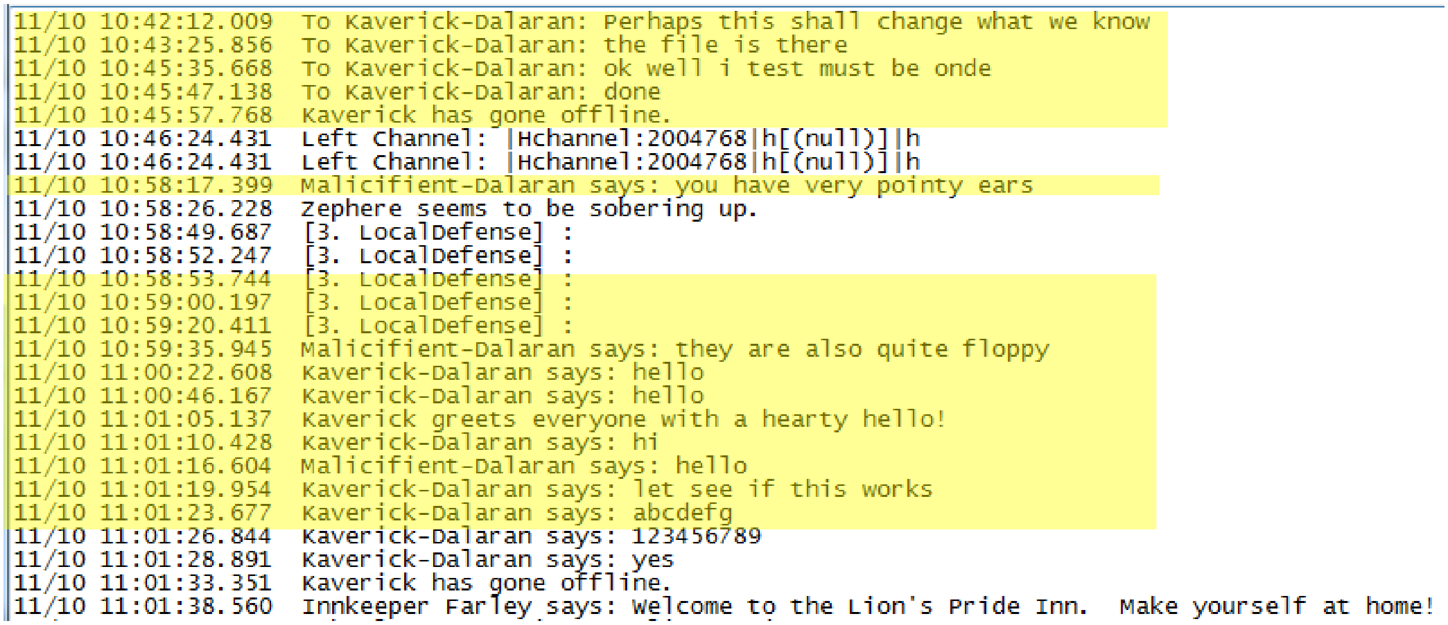
Like the other two MMORPGs, no chat logs were created with the default game settings. With our second round of data generation, however, we confirmed that in-game chat can be stored if the player uses the in-game command /chatlog..By using /chatlog, we were able to obtain a full chat log that also logs in-game items crafted, chat channel loss and user commands such as /dance. This file opens as a .txt file which makes combing through the information a lot easier than reading from digital forensic software such as EnCase. However, because the log records actions of the user and everyone surrounding the user in their immediate in game area as well as chat conversations, the log becomes cluttered very rapidly. Unfortunately for an investigator, these extra events are largely worthless and make following a single conversation through the log more difficult. We were also able to recover the chatlog using IEF on the image from the second session of data generation. Figure 5 below shows how the chat log appears in EnCase and Figure 6 shows how the chat log appears when opened as a text document.

Figure 5: WoW Chat Log as Viewed in EnCase



	Name
1	wowbrowser
2	WoWChatLog.txt
3	cpu.log
4	gx.log
5	Sound.log
6	GlueXML.log
7	connection.log
8	FrameXML.log

Figure 6: WoW Chatlog as Viewed in a Text Document



```
11/10 10:42:12.009  To Kaverick-Dalaran: Perhaps this shall change what we know
11/10 10:43:25.856  To Kaverick-Dalaran: the file is there
11/10 10:45:35.668  To Kaverick-Dalaran: ok well i test must be onde
11/10 10:45:47.138  To Kaverick-Dalaran: done
11/10 10:45:57.768  Kaverick has gone offline.
11/10 10:46:24.431  Left Channel:  |Hchannel:2004768|h[(null)]|h
11/10 10:46:24.431  Left Channel:  |Hchannel:2004768|h[(null)]|h
11/10 10:58:17.399  Malicifient-Dalaran says: you have very pointy ears
11/10 10:58:26.228  Zephere seems to be sobering up.
11/10 10:58:49.687  [3. LocalDefense] :
11/10 10:58:52.247  [3. LocalDefense] :
11/10 10:58:53.744  [3. LocalDefense] :
11/10 10:59:00.197  [3. LocalDefense] :
11/10 10:59:20.411  [3. LocalDefense] :
11/10 10:59:35.945  Malicifient-Dalaran says: they are also quite floppy
11/10 11:00:22.608  Kaverick-Dalaran says: hello
11/10 11:00:46.167  Kaverick-Dalaran says: hello
11/10 11:01:05.137  Kaverick greets everyone with a hearty hello!
11/10 11:01:10.428  Kaverick-Dalaran says: hi
11/10 11:01:16.604  Malicifient-Dalaran says: hello
11/10 11:01:19.954  Kaverick-Dalaran says: let see if this works
11/10 11:01:23.677  Kaverick-Dalaran says: abcdefg
11/10 11:01:26.844  Kaverick-Dalaran says: 123456789
11/10 11:01:28.891  Kaverick-Dalaran says: yes
11/10 11:01:33.351  Kaverick has gone offline.
11/10 11:01:38.560  Innkeeper Farley says: Welcome to the Lion's Pride Inn.  Make yourself at home!
```

Conclusion

Overall, this project has confirmed some of our theories and revealed interesting game features. As we predicted, none of the MMORPGs that we tested stored logs locally on the player's system by default. This, combined with the fact that many MMORPGs have limits on how many logs can be created and how long logs will be when stored, makes them of limited use as evidence in digital forensic investigations barring any extraordinary circumstances. For example, if chat logs were deliberately enabled and recorded, they have the potential to be extremely useful as proof of incriminating conversations, threats, or verbal attacks over the Internet. If the chat logs can be confirmed by server records from the game developer itself, then the chat log can be a very useful piece of evidence. However, it is also important to understand that proving that a chat log is valid and unedited can be difficult. In the MMORPGs that produced chat logs, we found they are stored as a simple text (.txt) file that will need to be proven to be unedited in order to be accepted as evidence. In the end, we can conclude that under the right circumstances, it is entirely possible to recover MMORPG chat logs from a target computer and that the logs may contain pertinent information. This makes chat logs a valid source of evidence and something worth checking in relevant cases.

Further Work

While our project has provided some insight into the mechanics of MMORPGs, it is by no means a far reaching study. Having investigated only three games and we cannot claim to have a comprehensive understanding of how chat logs work in the gaming world. This is also compounded by the fact that there is no universal format for chat logs or in-game chat functions in MMORPGs. Each company is left to decide on their own the best way to implement chat conversations and logs, which means that every multiplayer video game will approach chat functionality and logging differently. Continued investigation of other MMORPGs will be required.

However, it is worth noting that there is a notable limitation to the variation of chat functions in MMORPGs made by the same company. For instance there were noticeable similarities between Everquest II and PlanetSide 2 chat logs. MMORPG companies most likely recycle portions of code from previous MMORPGs into their new MMORPGs to save time and provide the player with a familiar interface. It is entirely possible; therefore, that an investigator could find themselves getting very similar chat log results from multiple MMORPGs made by the same company.

This project is one that will likely be continued and expanded in the future as MMORPGs change how their users can talk to one another and new MMORPGs are released. We have scratched the surface of the research that can be done in this field with our project and we are excited to see what other research can be done on chat log forensics in the future.

Works Cited

"Command Line Arguments." - *Guild Wars 2 Wiki (GW2W)*. N.p., 3 Dec. 2015. Web. Oct. 2015.

Daniel, Larry E. "Multiplayer Game Forensics." Forensic Magazine. Advantage Business Media, 21 May 2010. Web. 2 Dec. 2015.

Eggman.1405. "Please Let Us save Chat." Web log post. *GuildWars2.com*. ArenaNet, Winter 2014. Web. 2 Dec. 2015.

Makuch, Eddie. "World of Warcraft Loses Nearly 3 Million Subscribers in Three Months." GameSpot. GameSpot, 6 May 2015. Web. 01 Dec. 2015.

"ShadowPlay PC Game Capture Software | GeForce." ShadowPlay PC Game Capture Software. NVIDIA Corporation, *n.d.* Web. 2 Dec. 2015.

"The Game – GuildWars2.com." GuildWars2.com. ArenaNet. Web. 2 Dec. 2015.

Veen, Shelly V. *Virtual Worlds: The New Playground for Sexual Predators*. Claremont: Claremont Police Department, Aug. 2011. PDF. 01 Dec. 2015.

"What Is World of Warcraft." *World of Warcraft*. Blizzard Entertainment, *n.d.* Web. 01 Dec. 2015.