Digital Investigation 9 (2013) 211–221

Contents lists available at SciVerse ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

FrostWire P2P forensic examinations

Joseph Lewthwaite

Defense Cyber Crime Center (DC3), 911Elkridge Landing Rd., Linthicum, MD 21090, USA

ARTICLE INFO

Article history:
Received 2 August 2012
Received in revised form 7 December 2012
Accepted 10 December 2012

Keywords:
FrostWire
Limewire
P2P
Digital forensics
Gnutella
Azureus
Torrent
BitTorrent

ABSTRACT

FrostWire is a peer-to-peer (P2P) application derived from the open source code of Limewire. Frostwire was first released in February of 2005 as a Gnutella P2P client. As interest in the Gnutella network waned, FrostWire switched in later versions to becoming a torrent client. Since the United States government shut Limewire down, FrostWire has become more popular and is seen more often in criminal investigations. This paper describes the different components of FrostWire and the useful information which can be obtained in a digital forensic examination.

1. Introduction

First released in February 2005, FrostWire is a peer-to-peer (P2P) application derived from the open source code of Limewire. In October of 2010 (Limewire Homepage, 2010) Limewire was ordered to shutdown and stop distributing its software. With the demise of Limewire, FrostWire has increased in popularity and has consequently been seen in criminal cases more often.

As a P2P client, FrostWire enables the user to share and download files with other users and includes a basic chat capability, which allows communication about sharing to take place. The FrostWire versions discussed in this paper use two different protocols to trade files: the Gnutella and BitTorrent protocols. The Gnutella protocol is designed as the basis of a decentralized P2P network and allows the user to search for files, and to connect with and download files from other Gnutella clients. Torrents are metadata files that both divide a large file into information chunks and give the location of those chunks. This approach enabled clients to speed up a file download by obtaining chunks from different hosts in parallel and then reassembling the chunks into the original file on the user's computer. The BitTorrent protocol deals strictly with the downloading of a file and so searching for torrents is handled through tracker web sites which organize the registration and searching of torrent clients.

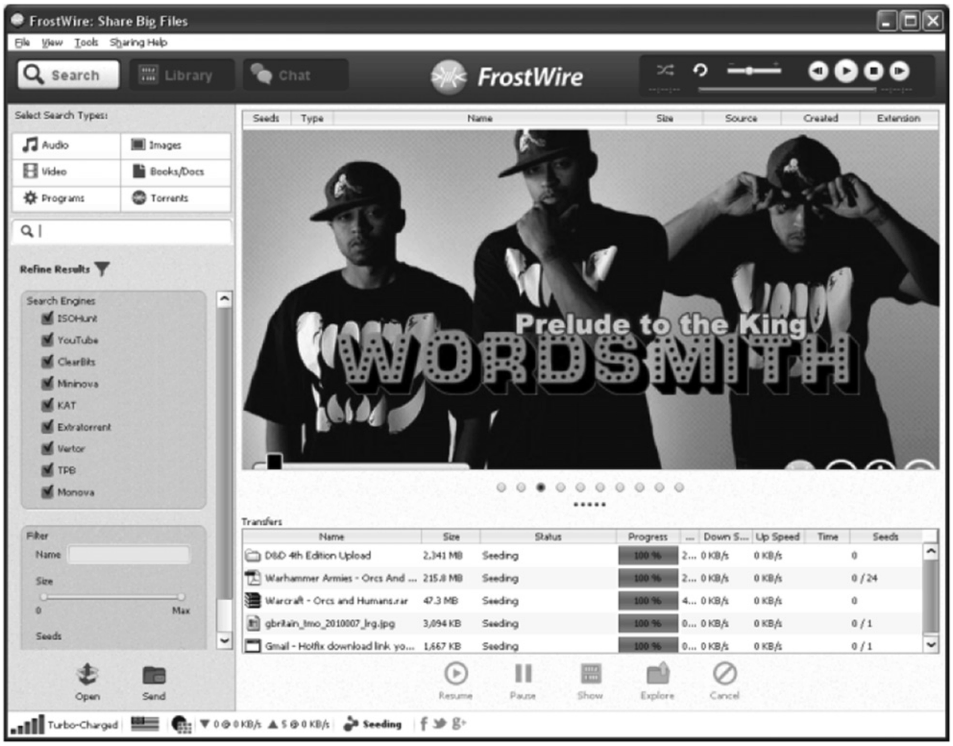
The following images show the three basic areas for FrostWire. Fig. 1 is the main search and download form, Fig. 2 is the user's library where they manage their shares, and Fig. 3 is FrostWire's chat screen.

This paper explores the operation of FrostWire including downloading, sharing, and searching in order to give digital investigators a better understanding in reconstructing activities related to FrostWire usage on a computer.

This paper begins with technical background and general comparison of Limewire and FrostWire versions. The next section addresses folders created during the installation process. The remainder of the paper addresses the following common questions that arise in forensic examinations involving FrostWire: 1) what did the user download and when, 2) What the user was sharing with the community, and 3) what the user searched for on the network.

E-mail addresses: joseph_lewthwaite@hotmail.com, joseph.lewthwaite.ctr@dc3.mil.

1742-2876/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.diin.2012.12.001



Transfers

Name	Size	Status	Progress	...	Down S...	Up Speed	Time	Seeds
D&D 4th Edition Upload	2,341 MB	Seeding	100 %	2...	0 KB/s	0 KB/s		0
Warhammer Armies - Orcs And ...	215.8 MB	Seeding	100 %	2...	0 KB/s	0 KB/s		0 / 24
Warcraft - Orcs and Humans.rar	47.3 MB	Seeding	100 %	4...	0 KB/s	0 KB/s		0
gbritain_tmo_2010007_lrg.jpg	3,094 KB	Seeding	100 %	0...	0 KB/s	0 KB/s		0 / 1
Gmail - Hotfix download link yo...	1,667 KB	Seeding	100 %	0...	0 KB/s	0 KB/s		0 / 1

Fig. 1. FrostWire search screen.

2. Background

For the purposes of this study, two versions of FrostWire were downloaded for examination, version 4.21.8 because it was the last version supporting the Gnutella protocol, and version 5.3.7 which was the latest version when this paper was written and supports only torrent downloads. As FrostWire is an open source project, the source Java code was downloaded and used to supplement the testing. All testing was performed on a Microsoft Windows XP machine running service pack 3.

Because FrostWire started as a fork of Limewire, a peer-to-peer client using the Gnutella network, many of the methods and tools developed for performing forensic examination of Limewire usage artifacts apply to FrostWire. Therefore, much of the information for version 4 of FrostWire overlaps with findings in the paper “Limewire Examinations” (Lewthwaite and Smith, 2008).

In version 4, FrostWire worked primarily as a Gnutella P2P client with legacy Limewire code allowing torrent access. In version 5, FrostWire drops support of Gnutella P2P and becomes exclusively a search client for torrents, allowing the user to search multiple torrent trackers for content. The torrent capability is provided by integrating Azureus open source code into Frostwire. Azureus was an early torrent client released through SourceForge in 2003 (Vuze, 2012).

FrostWire also has a chat capability embedded in the client and can attach to chat servers. FrostWire.com runs one chat server that is configured in the FrostWire client by default. The FrostWire client has no inherent save capability to archive the chats, or a logging option, but if a volatile memory snapshot was taken or the digital investigator has access to the systems pagefil.sys or hiberfil.sys, then a Unicode search using the user’s chat name can return the content of chat sessions.

Below is a high level comparison of the features between Limewire and FrostWire (Table 1).

3. Installation

On installation, FrostWire places two major folder sub-trees under the user’s folder. For the downloads and content, FrostWire creates a sub-tree under the “My Documents” folder. The second sub-tree handles the user’s application use and is placed under the “Application Data” folder. For digital investigators, the application’s settings folder contains the pieces of the puzzle that will generally shed the most light on their case. In version 4, the settings folder will contain the files that any digital investigator familiar with Limewire will recognize: “FileURNs.cache”, “Library.dat”, and “Createtimes.dat” describing the user’s Gnutella library. This folder will also contain the files “Azureus.config” and “downloads.config” describing the torrent library. The file “FrostWire.props” contains the basic properties relating to sharing.

FrostWire versions prior to 5.x install the following structure onto a Windows XP machine to hold a user’s downloads and shared files:

- <User>\My Documents\FrostWire\ – Files being downloaded