Introduction to File Sharing Services

An IT-Forensic Examination of P2P Clients

NITEC

Nationalt IT-Efterforskningscenter

National High Tech Crime Centre

Contents

What is File Sharing – P2P?

The expression peer-to-peer is especially used within the field of data communication to describe communication or the direct exchange of data between equal units of a communication network, without involving a central computer. The expression “P2P” or file sharing is used for the same form of communication as well.

Apart from the above-mentioned, it may be added, that the users of file sharing programmes are connected to each other in a larger network, that works more or less autonomously. As a consequence of this, it is not possible immediately afterwards to carry out an investigation in this environment, since the communication lines are interrupted at log-out of the programme and the connection is disconnected. This again means, that no log-outs are generated elsewhere, but only between the involved parties. frThere are, however, several file sharing programmes that contain internal log files, which may give information about files downloaded earlier and which files have been available for sharing and so on.

The programmes work in such a way that you, during installation, define a folder as being “shared” with other users of file sharing services (it is not necessary to make use of the same file sharing programme – as long as the programme is active in the same network – typically Gnutella Network, eD2k Network or Fast Track Network). The content of this shared folder is available to all the other users, just as they are able to run searches of the content. In some programmes it is possible to “switch off” the file sharing function, which means that files cannot be downloaded from the computer.

In order to explain the functionality of file sharing programmes, you have to metaphorically compare a film file to a jigsaw, for example. All the users of the file sharing programmes place a number of “jigsaws” at the disposal of all the other users of the file sharing service/network (the files in their shared folders).

When a user searches the network for a certain file – the film “Titanic”, for instance – the user will be told which users have the file in question. Our user may click on a file corresponding to his wish and then start downloading the file. He is not restricted to one single user, but can download from several different users that have the desired file. The programme now gets pieces for the complete jigsaw from several other users at the same time and the final result will be gathered together at our user's computer. This functionality ensures, that the individual users' bandwidth is not burdened too much, just as the user is not immediately affected when individual remote users shut down and close their connection.

The History of File Sharing – in Short

Ever since the infancy of computers, there has been a need for exchanging files between several computers and users. In the beginning no actual storage medias existed, which meant that if any information should be transferred from one computer to another, everything had to be typed in manually. Later on, the first magnetic storage medias arrived and these could contain data, but were very difficult to move around. Later on, the punch card was a reality and you were suddenly able to print cards that could be read into another computer – a difficult, but usable method.

By the introduction of the floppy disk and the magnetic tape unit, the sharing of files became much easier, but the spreading of files still went very slowly, since the files had to be moved physically from one place to another.

With the rising popularity of the Internet in the beginning of the nineties, the ordinary user quickly figured out that it was possible to download and send files to each other through the network, even **though you were both sitting on each side of the Earth.**

USENET was the first network in which you could actually share files with many other unknown users; in everyday speech this is referred to as newsgroups. Here it became possible to post smaller files that other users then could download. Newsgroups are still being used, but not quite to such an extent as they have been.

In the start of the nineties it also became very popular to set up FTP servers. By using an ordinary FTP client, you could log on a server and download the content that was available. The FTP server's popularity soon fell, because different intellectual property rights holders could easily identify the owner of the server and thus claim large sums in compensation from him. Today, FTP servers are seldom seen.

At the same time as the FTP servers appeared, the IRC also started gaining ground. Especially the client mIRC became very popular, as it was possible to develop script extensions for the programme, by which you could set up the so-called file server (F server), a bit like the FTP servers. mIRC is still being used for file sharing.

In the end nineties, the first modern file sharing programme, Napster, came into existence. This service worked in such a way, that a number of central indexing servers registered the content of all users in the network and their files. However, in 2001, the service was sued by, amongst others, Lars Ulrich from the band Metallica. The legal actions lead to the closure of Napster.

Same year, the next generation of file sharing services appeared. This generation was no longer dependent on central servers, but was a so-called distributed system, in which all requests went through other clients connected to the network, without involving central servers.

The first distributed client was KaZaA. Through KaZaA it now became possible to share other things than music files and it was very easy to make use of. The programme became a huge success and you quickly had up to several million users in the network at the same time. In the time after, a number of different clients were developed.

In 2002, the client eMule saw the light of day. eMule was a further development of the client eDonkey 2000, which was made by a group of programmers getting tired of the client eDonkey2000. eMule became an open-source programme and many people could now participate in the improvement of the client.

Since then, many new versions of eMule and other file sharing clients have been developed.

Networks

The different file sharing services often make use of their own network protocols, which is why you sometimes have to have specific clients in order to act in a specific network. However, many clients have started to become so-called multi-network-clients, which means that they can operate in different networks at the same time. That way the user gets more search options and search hits.

Many different networks exist, a number of them are listed below:

eD2K
KAD
Gnutella
FastTrack
BitTorrent
Freenet
I2P
AntsP2P

and many more...

The first 5 networks mentioned on the list are open and unencrypted, whereas the last 3 are encrypted networks.

As mentioned earlier, many clients are written to operate in several networks. eMule, for instance, is able to connect to eD2K, KAD, Gnutella and BitTorrent.

As it appears, encrypted networks also exist. These are not that popular, since the clients are not as straight forward to use as the unencrypted clients and the network is very slow, just as there are not nearly as many files available in these networks.

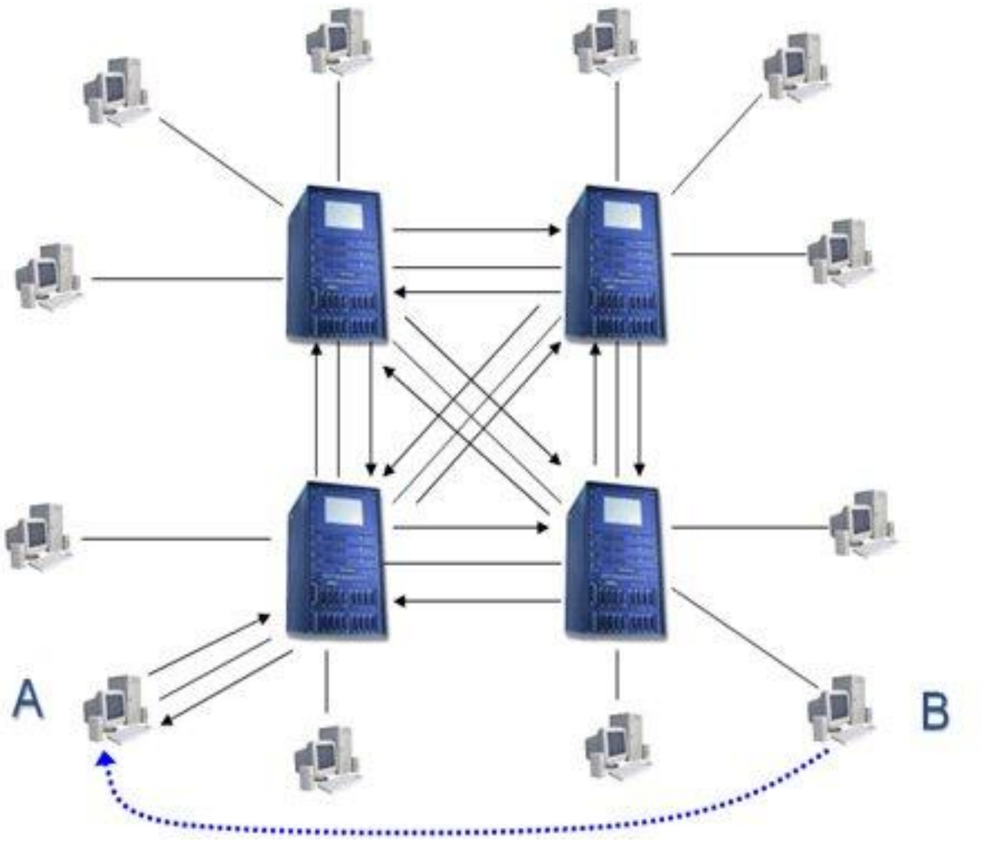
The individual networks, of course, have different topologies and these will be described in the next paragraph.

Network Topologies

First-generation networks

Centralized networks (Napster, for instance).

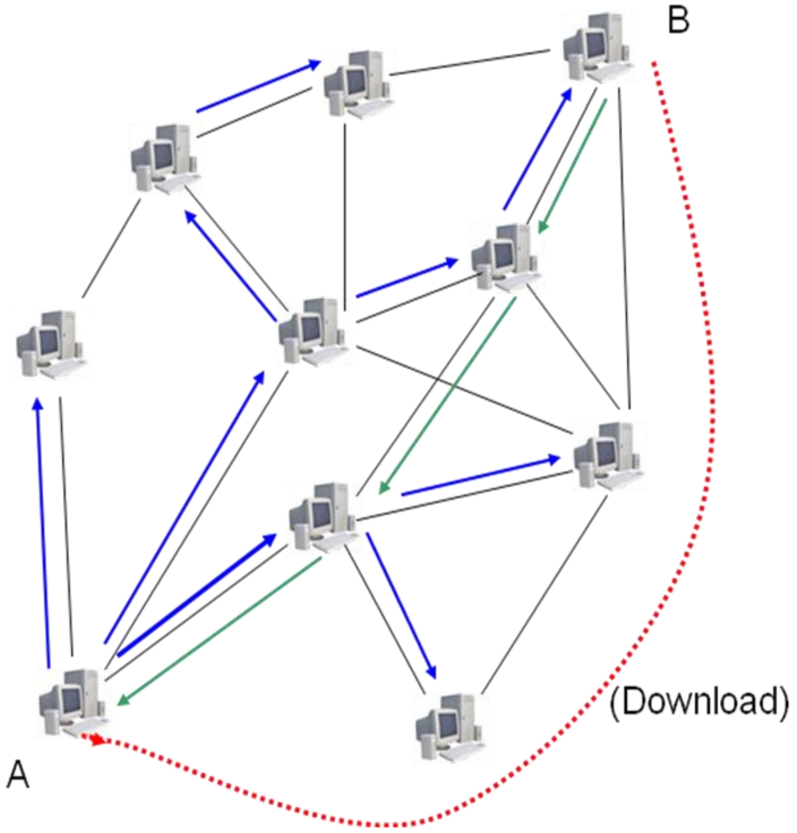
First-generation network architecture was based on a number of centralized indexing servers, which kept up a data base on all clients logged in and their shared files. The database was updated every time a client logged on to the network.



Second-generation networks

Decentralized networks (KaZaA, for instance).

Second-generation networks implemented a fully decentralized and distributed network-structure. Instead of central servers, the individual user's PC now formed an integral part of the network, since it acted, and still acts, both as an indexing server, carries out local searches and carries out routings of requests between the different clients.



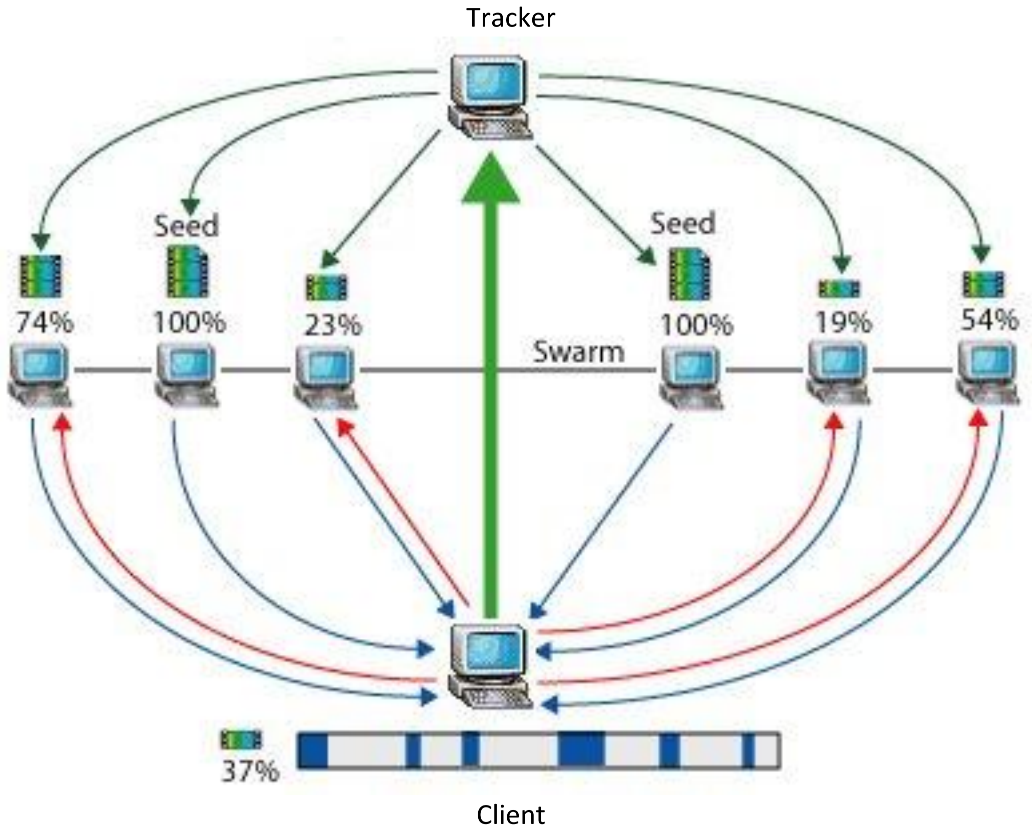
Third- generation networks

Encrypted networks (Ants, for instance).

These networks are based on the same topology as second-generation networks, but are encrypted.

Fourth-generation networks

The BitTorrent network is based on a “partly decentralized network”, in the way that you download a so-called “.torrent” file through a homepage. Through your client you are then connected to a “tracker”, which is a server keeping track of the different files that are available. Files found complete, are called “seeds” and the tracker sends information about where you can download the file. Downloading takes place from the complete seeds, whereas the parts missing in the incomplete files are being uploaded to the clients at the same time. BitTorrent is based on the principle of “tit-for-tat” and it is impossible to disconnect this “share” function.



Clients

In the following paragraphs, I will go through the different file sharing clients.

Below there is a list of clients, which at present form a part of this material:

- **eMule**
- **LimeWire**

eMule

The text given below has been taken directly from eMule's official homepage on www.emule-project.org.

What is eMule?

At dawn of May 13th, 2002, a guy called Merkur was dissatisfied with the original eDonkey2000 client and was convinced he could do better. So he did. He gathered other developers around him, and eMule project was born. Their aim was to put the client back on track where eDonkey had been famous before, adding tons of new features and a nice GUI. They couldn't imagine what impact this decision would have...

As of today, eMule is one of the biggest and most reliable peer-to-peer file sharing clients around the world. Thanks to its open source policy, many developers are able to contribute to the project, making the network more efficient with each release.

What does eMule mean?

The name "eMule" comes from an animal called "Mule", which is somehow similar to a donkey. ;-)

How often is eMule updated?

eMule is not updated regularly, but at the moment the frequencies are between 1 and 3 months. Don't take this for guaranteed.

A short list of eMule's features

Clients use several networks to create one reliable network (ED2K, Source Exchange, Kad).

Kad has now been implemented and versions 0.48 onwards connect automatically to Kad.

eMule's "Queue and Credit" system helps to ensure that everyone will get the file he wants by promoting those that upload back to the network.

eMule is completely free. eMule is also completely free of any Adware, Spyware and etc. We do this for fun and knowledge, not for money.

Each file is checked for corruptions while downloading to ensure an error free file

The eMules Intelligent Corruption Control helps to speed up the correction of corrupted parts.

Auto priorities and Source management allows you to start many downloads without having to monitor them.

The Preview function allows you to look at your videos and archives (zip, rar and so on) before they are completed. For video previewing, we recommend the Video Lan Client (VLC).

The eMule features web services and a web server that allows you to have quick access to and from the Internet.

You can create categories for your downloads to organize them.

To find the file you want, eMule offers a wide range of search possibilities which include: Servers (local and global), web based (Jigle and Filedonkey) and Kad (still in Alpha).

eMule also allows you to use very complex Boolean searches that make the searches much more flexible.

With the messaging and friend system, you can send messages to other clients and add them as friends. In your friend list, you can always see if a friend is online.

With the built-in IRC client, you can chat with other downloaders and chatters around the globe.

The files used in eMule

While eMule is performed a large number of files are being used. If they do not exist already, they will be made the first time eMule is started. Most of the files will be found in eMule’s “Config” folder, whereas the rest will be found either in eMule’s “Temp” folder or in the installation folder.

Known.met

The “Known.met” file contains information about all files eMule has downloaded. Information about size, file name, hash sets, hash values and some statistics are saved for each file.

Known2_64.met

The “Known2_64.met” file saves information about hash values for each file in connection with eMule’s AICH (Advanced Intelligent Corruption Handler).

Clients.met

This file saves all users, which have credit at your eMule.

Clients.met.bak

This file contains a backup of the above-mentioned file.

Server.met

Contains all known servers.

Webservices.dat

In this file you have the possibility to build in functionality in eMule, in relation to homepages. The file can be opened by a text editor such as Notepad and contains an explanation about the functionality.

Statistics.ini

This file contains all statistics shown in eMule’s statistics window.

Emfriends.met

If there are any users added to eMule’s friend list, they are being saved in this file.

Preferences.ini

All settings made in eMule’s “Settings” are saved here, just as information about the user interface, such as width of columns etc.

Fileinfo.ini

Comments or evaluations of your own shared files.

Category.ini

Saves the settings for your categories such as name, comments and choice of colour.

Ipfilter.dat

This file contains IP areas as well as access levels that have to be filtered by eMule. You can find more information about IP filtration on http://www.emuleguides.dk/support.php?id=18

Onlinesig.dat

The online signature is a small file containing the server eMule is connected to, as well as statistics on uploads and downloads. It can be used in IRC scripts and pictures for signatures.

Preferences.dat

The user hash is saved here. It is a value that is computed the first time eMule is started up and it is used to identify the client on the network. It is used for the credit system and for friends.

Sharedir.dat

Contains the paths for all shared files.

cancelled.met

Contains information about the files you have cancelled.

Staticservers.dat

Static servers never change IP address and are, in theory, always online on the network. By right-clicking on a server, you may add servers to this list.

Addresses.dat

eMule updates its server list when the programme starts up, if the file contains correct addresses for “server.met” files. In eMule’s “Settings -> Servers”, there is a button that gives you the option to edit this list and change the settings for updating at start up. The file can contain several addresses (one for each line), but only the first line that has a correct address to a “server.met” file will be used.

AC_SearchStrings.dat

Each search expression used in eMule is saved in this file

AC_ServerMetURLs.dat

The same principles as the above-mentioned file, except that this file saves typed addresses for “server.met” files.

AC_BootstrapIPs

The same principles as the above-mentioned file, except that this file saves typed IP addresses for the use of bootstrap in the Kad network.

Cryptkey.dat

Contains the unique 384bit private RSA key for your eMule client.

eMule.tmpl

The files with the extension “.tmpl” are necessary if you want to make use of eMule’s web interface. They define layout and settings of the shown pages.

xxx.part

The files with the extension “.part” are downloads in eMule that are not yet finished. eMule downloads from more than one user at a time, which means that the “.part” files always have the size of the final download. The missing parts are zerofilled. In the newer versions, and when using the NTFS file system, you have the option to share your incomplete downloads as “sparse”. This counteracts the mentioned process and therefore saves space on your hard disk.

xxx.part.met

Each “.part” file has a ”.part.met” file belonging to it. In order to identify downloads on the network and check for errors all downloads are divided into parts of 9,28MB (9500 bytes). For each part a so-called hash value is computed. After that a new hash value is computed for all the hash value parts. This information, together with file name and status of all the different hash’es, is saved in “.part.met” files.

xxx.part.met.BAK

A backup of each “.part.met” file is generated and saved, since it is critical if these files become corrupt by a mistake.

eMule.log

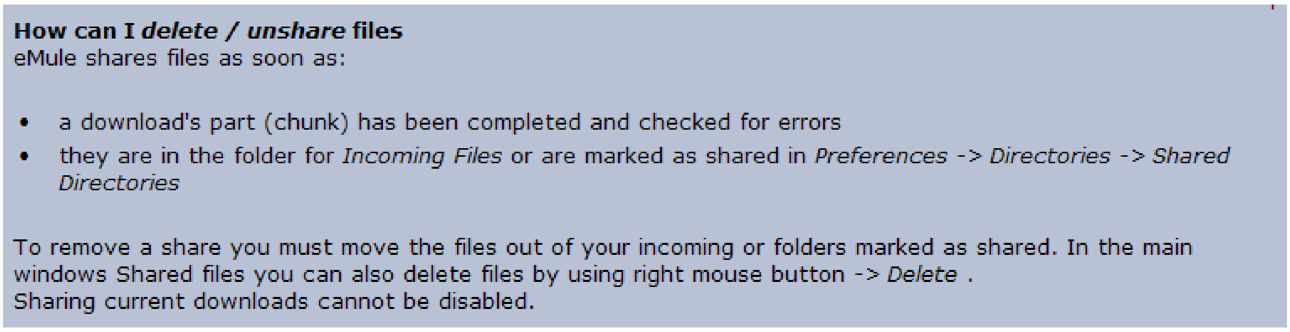
The log, you can see in the server window, is saved here if the window is activated in eMule’s “Settings -> Advanced”.

eMule_Debug.log

The debug_log, you can see in the server window, is saved here if the window is activated in eMule’s “Settings -> Advanced”.

Information about file sharing

From the “FAQ” on the official homepage, the following appears about sharing files and folders:



How can I *delete / unshare* files
eMule shares files as soon as:

- a download's part (chunk) has been completed and checked for errors
- they are in the folder for *Incoming Files* or are marked as shared in *Preferences -> Directories -> Shared Directories*

To remove a share you must move the files out of your incoming or folders marked as shared. In the main windows Shared files you can also delete files by using right mouse button -> *Delete* .
Sharing current downloads cannot be disabled.

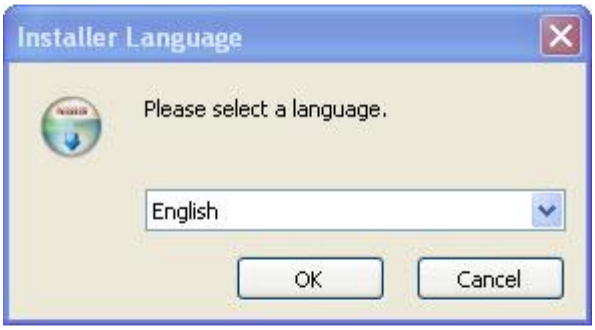
Notice that the share function cannot be switched off, as regards the folders created by the system!!!

(http://www.emule-project.net/home/perl/help.cgi?l=1&rm=show_topic&topic_id=311#unshare)

The Installation of eMule

The actual installation file for the newest eMule client is found on the official homepage www.emule-project.org, where the page has been set up in several languages – including Danish. As of today, version 0.49c (June, 2009) is the latest addition.

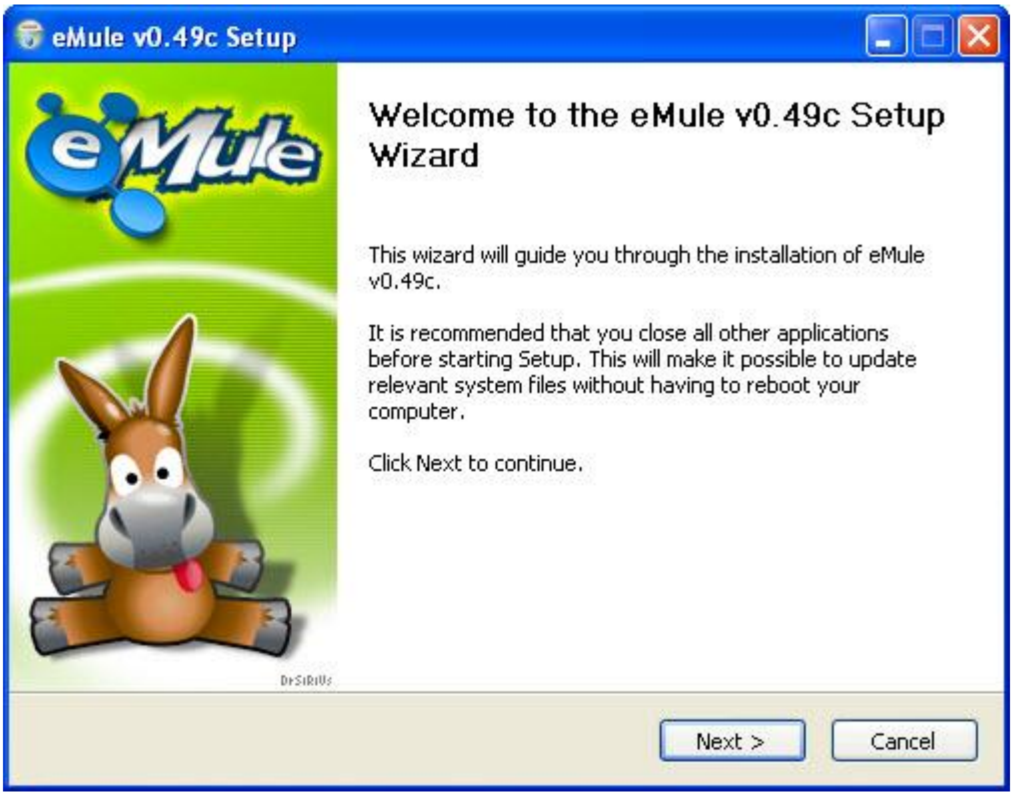
Below you can see all displays from a standard installation of version 0.49c:



Installer Language

Please select a language.

English



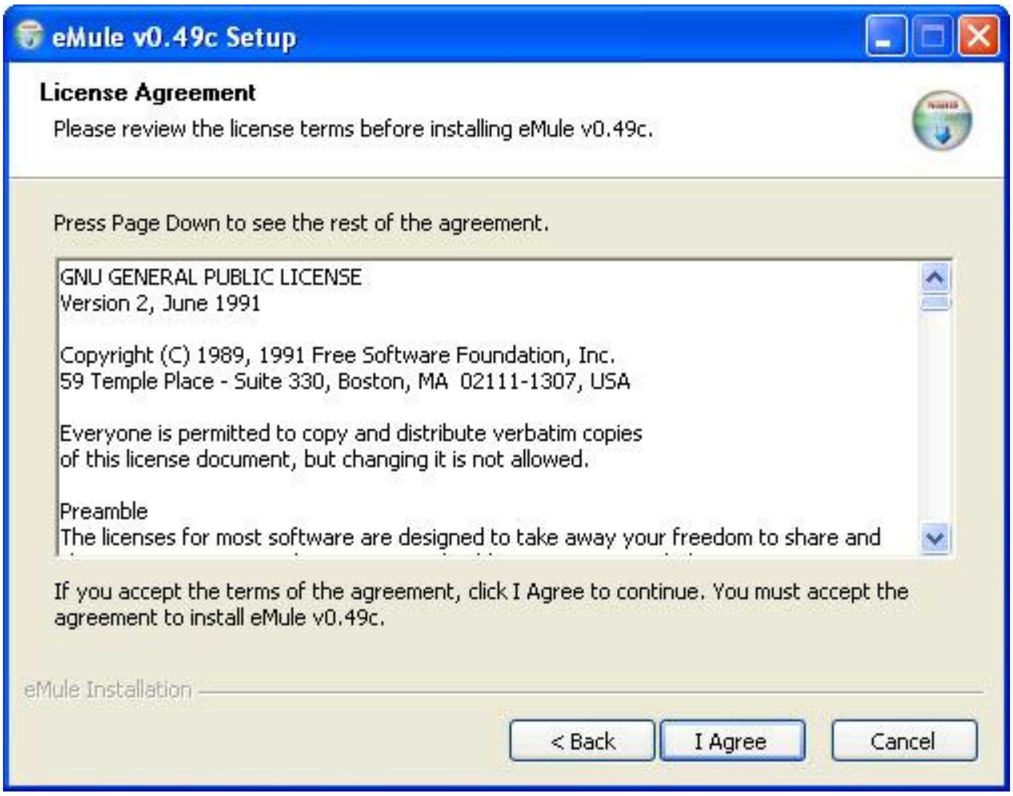
eMule v0.49c Setup

Welcome to the eMule v0.49c Setup Wizard

This wizard will guide you through the installation of eMule v0.49c.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.



License Agreement

Please review the license terms before installing eMule v0.49c.

Press Page Down to see the rest of the agreement.

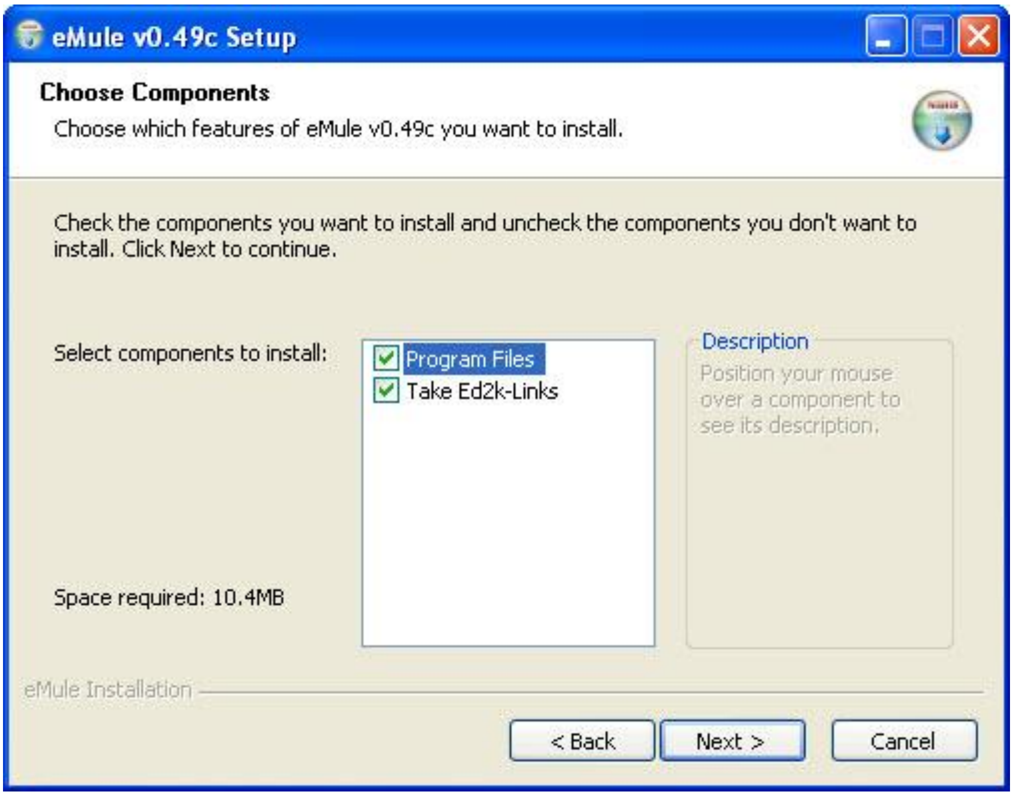
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble
The licenses for most software are designed to take away your freedom to share and

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install eMule v0.49c.



Choose Components

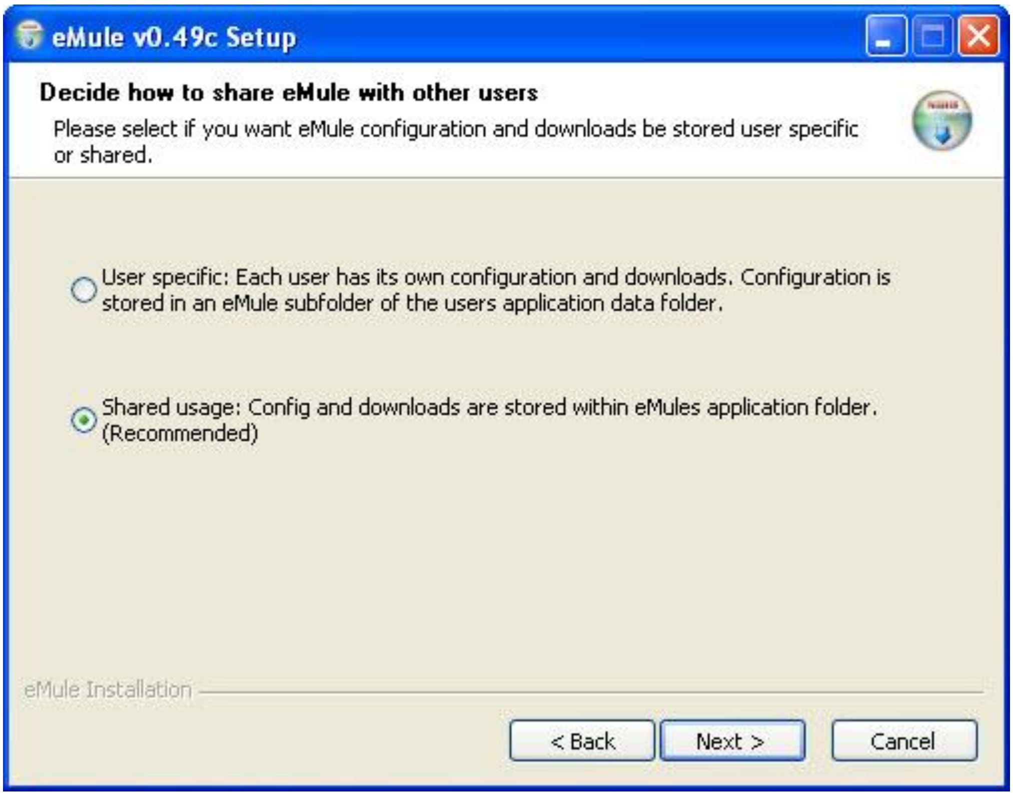
Choose which features of eMule v0.49c you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:
☑ Program Files
☑ Take Ed2k-Links

Space required: 10.4MB

Description
Position your mouse over a component to see its description.



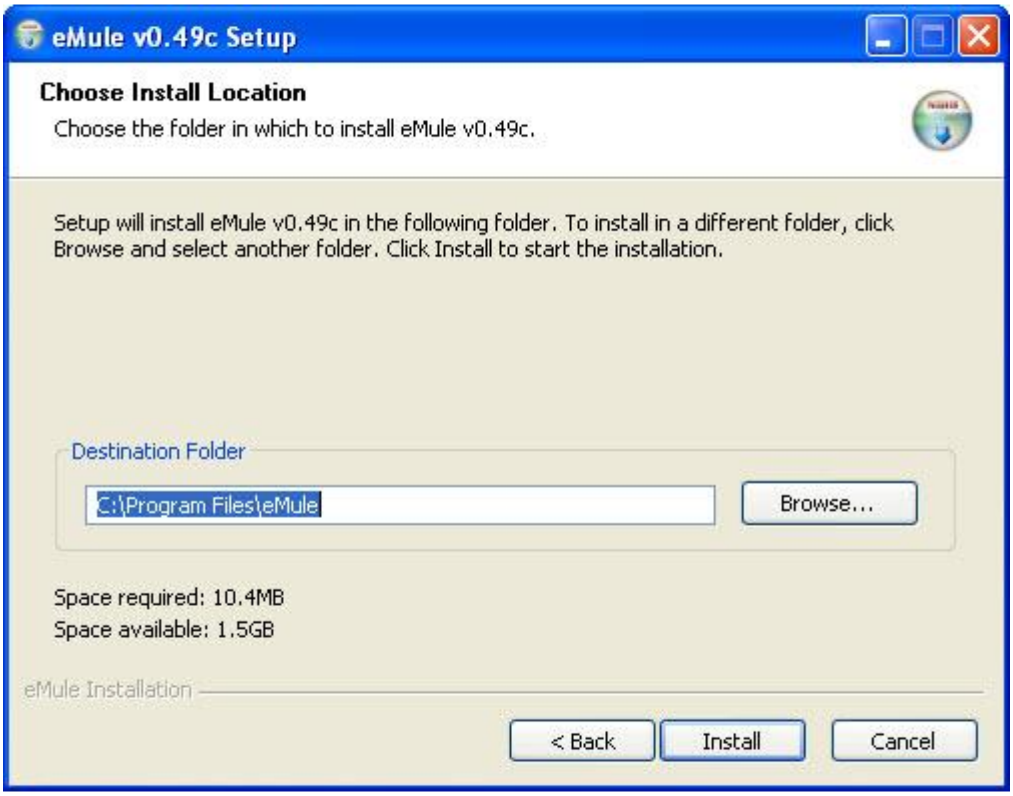
eMule v0.49c Setup

Decide how to share eMule with other users

Please select if you want eMule configuration and downloads be stored user specific or shared.

○ User specific: Each user has its own configuration and downloads. Configuration is stored in an eMule subfolder of the users application data folder.

● Shared usage: Config and downloads are stored within eMules application folder. (Recommended)



eMule v0.49c Setup

Choose Install Location

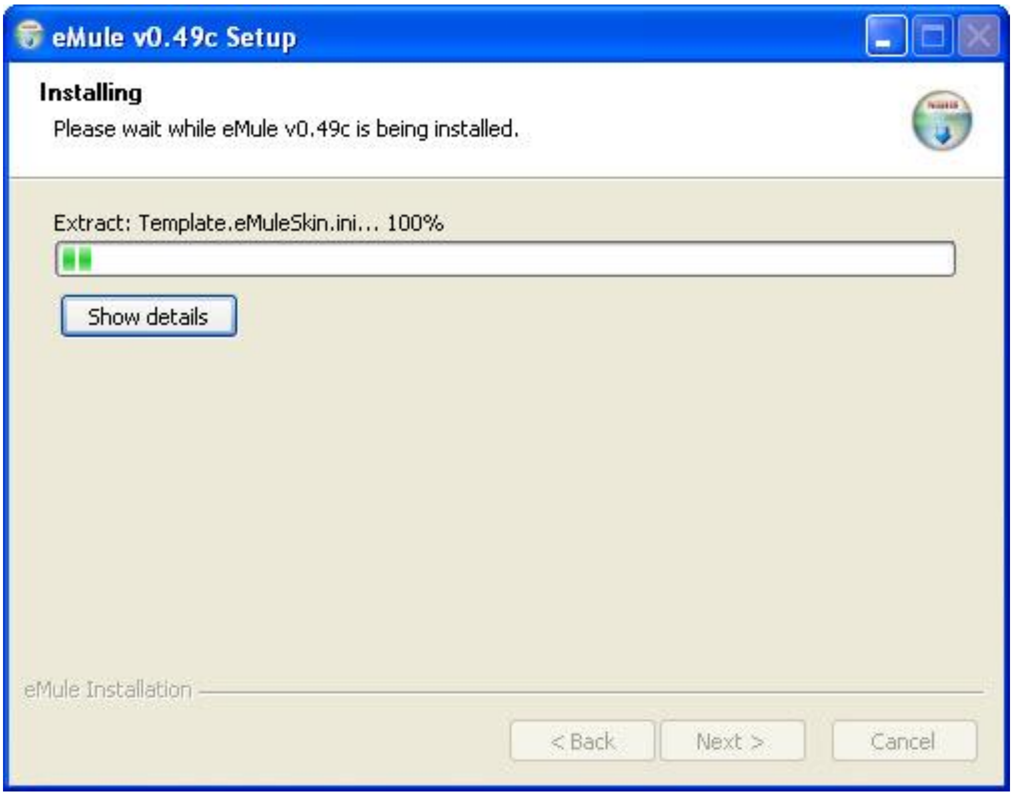
Choose the folder in which to install eMule v0.49c.

Setup will install eMule v0.49c in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files\eMule

Space required: 10.4MB

Space available: 1.5GB

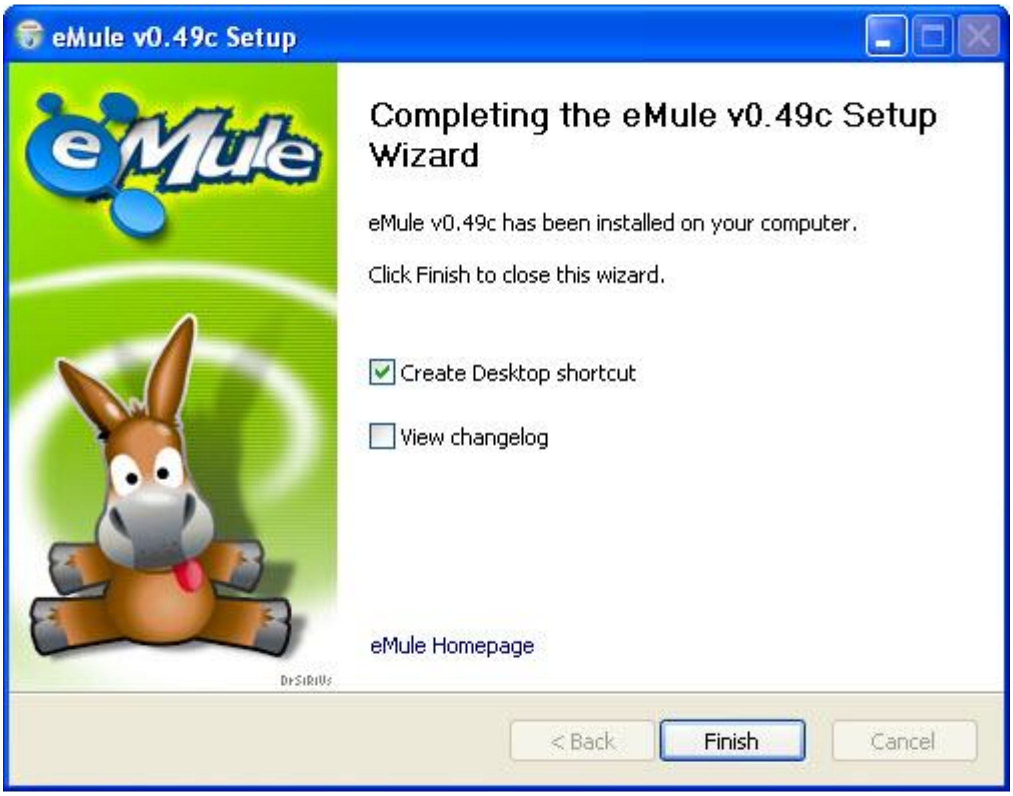


eMule v0.49c Setup

Installing

Please wait while eMule v0.49c is being installed.

Extract: Template.eMuleSkin.ini... 100%



eMule v0.49c Setup

Completing the eMule v0.49c Setup Wizard

eMule v0.49c has been installed on your computer.

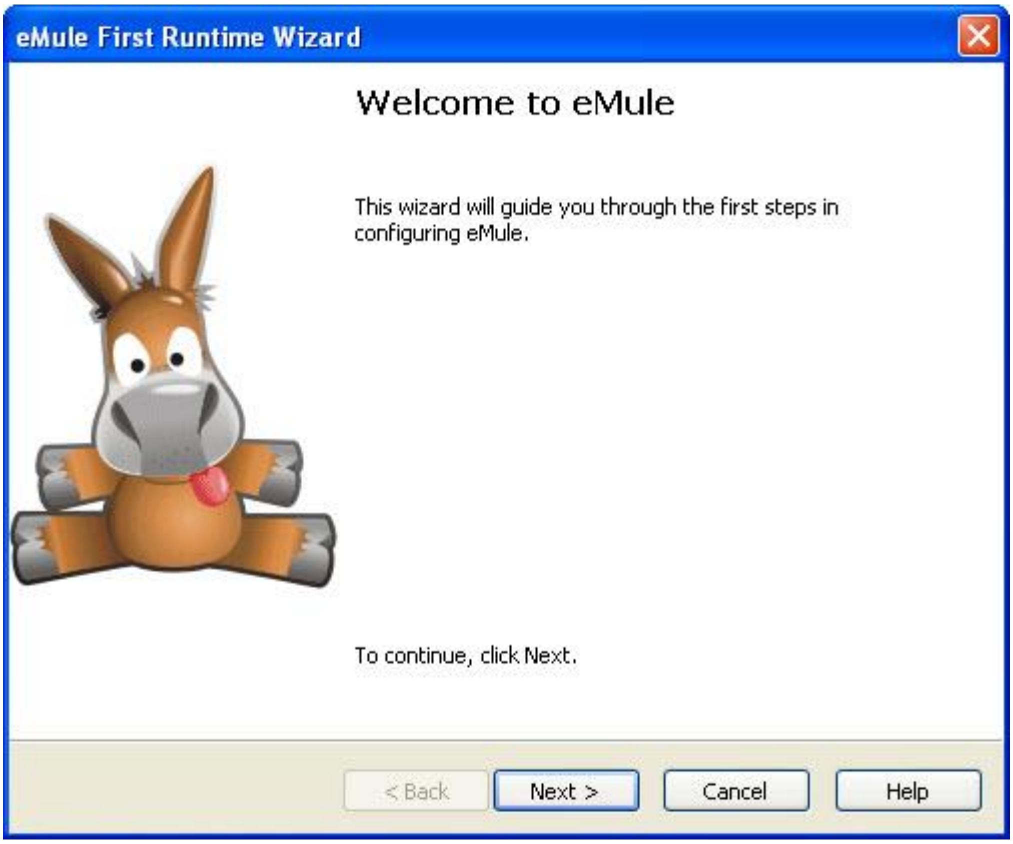
Click Finish to close this wizard.

☑ Create Desktop shortcut

□ View changelog

The first part of the installation stops here. The user now has to start the application manually, by using one of the shortcuts to the programme.

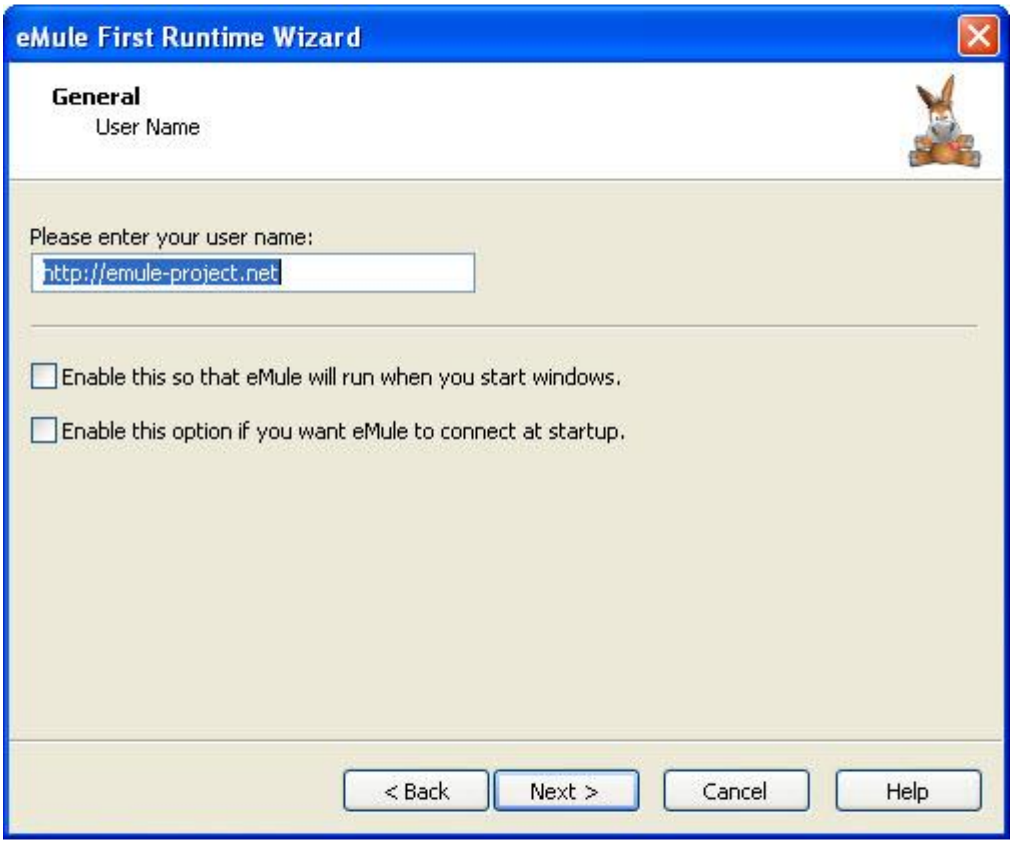
When the programme has started up, the set up of the programme continues.



Welcome to eMule

This wizard will guide you through the first steps in configuring eMule.

To continue, click Next.



eMule First Runtime Wizard

General

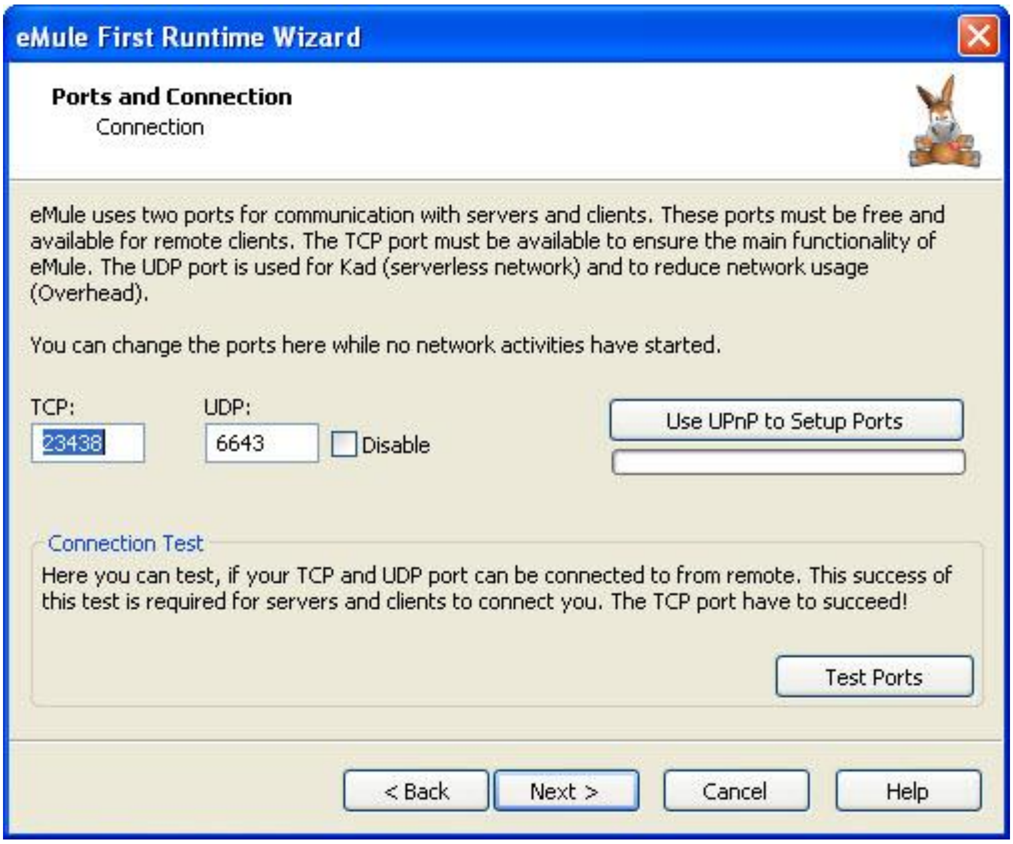
User Name

Please enter your user name:

http://emule-project.net

□ Enable this so that eMule will run when you start windows.

□ Enable this option if you want eMule to connect at startup.



eMule First Runtime Wizard

Ports and Connection

Connection

eMule uses two ports for communication with servers and clients. These ports must be free and available for remote clients. The TCP port must be available to ensure the main functionality of eMule. The UDP port is used for Kad (serverless network) and to reduce network usage (Overhead).

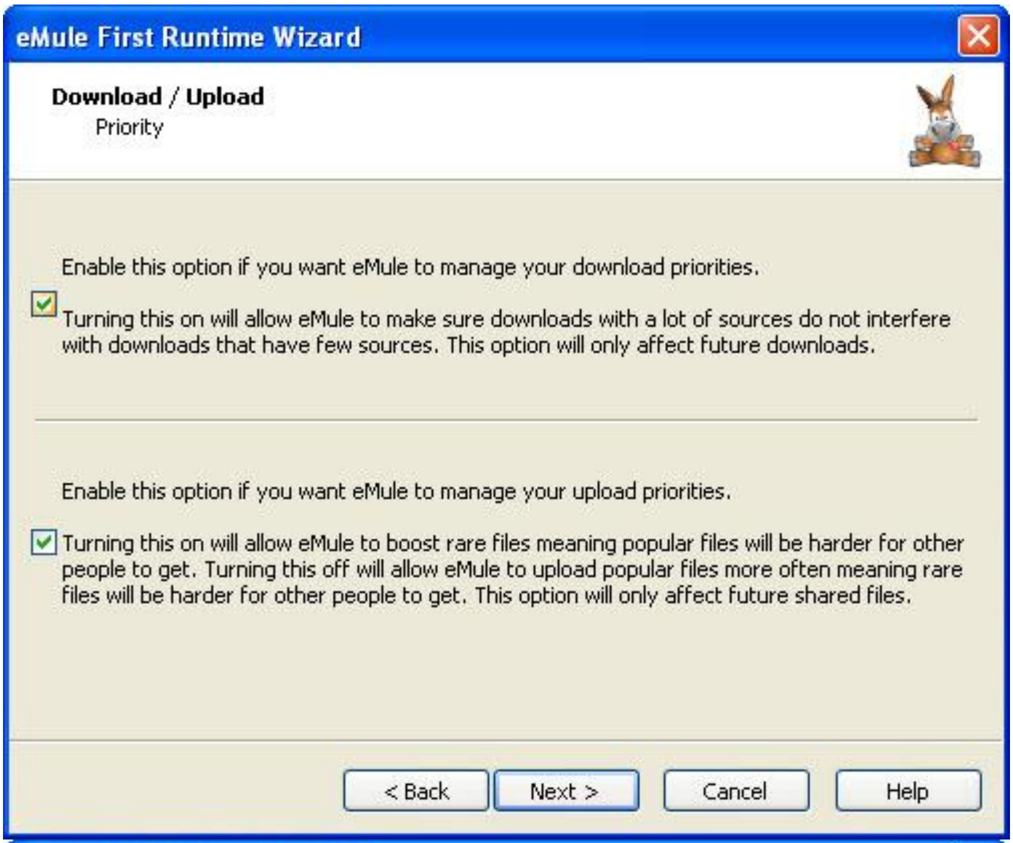
You can change the ports here while no network activities have started.

TCP: 23438

UDP: 6643 □ Disable

Connection Test

Here you can test, if your TCP and UDP port can be connected to from remote. This success of this test is required for servers and clients to connect you. The TCP port have to succeed!



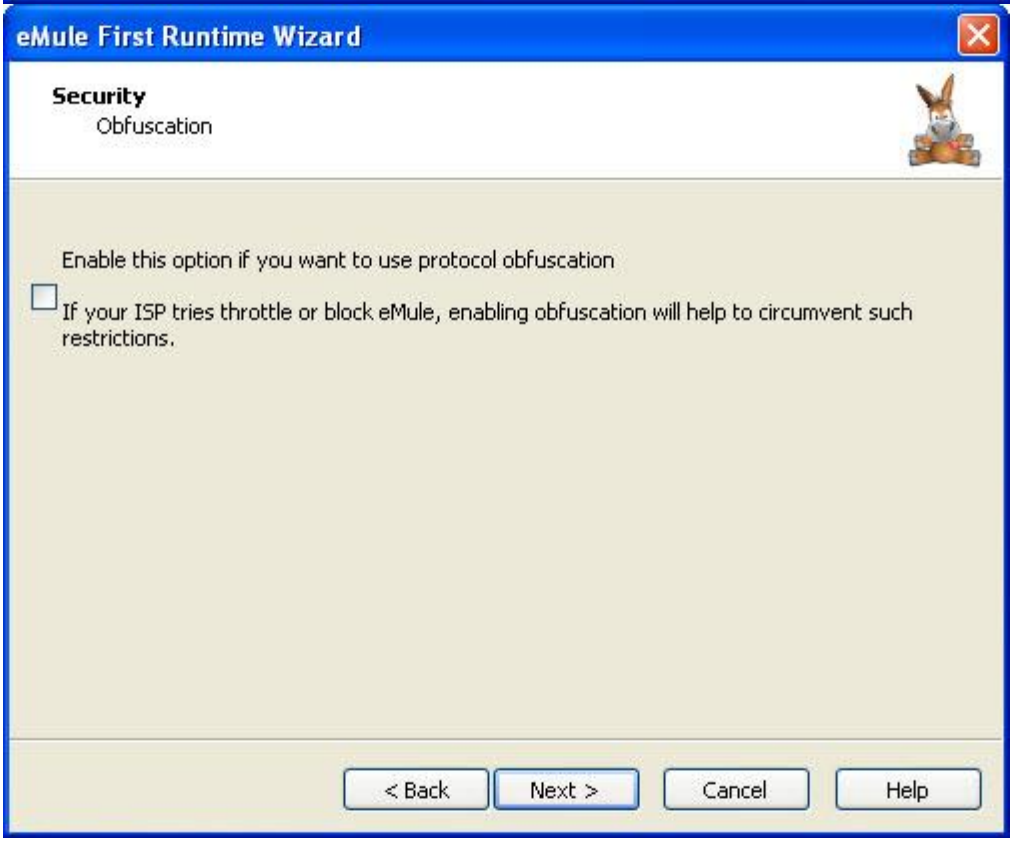
Download / Upload
Priority

Enable this option if you want eMule to manage your download priorities.

☑ Turning this on will allow eMule to make sure downloads with a lot of sources do not interfere with downloads that have few sources. This option will only affect future downloads.

Enable this option if you want eMule to manage your upload priorities.

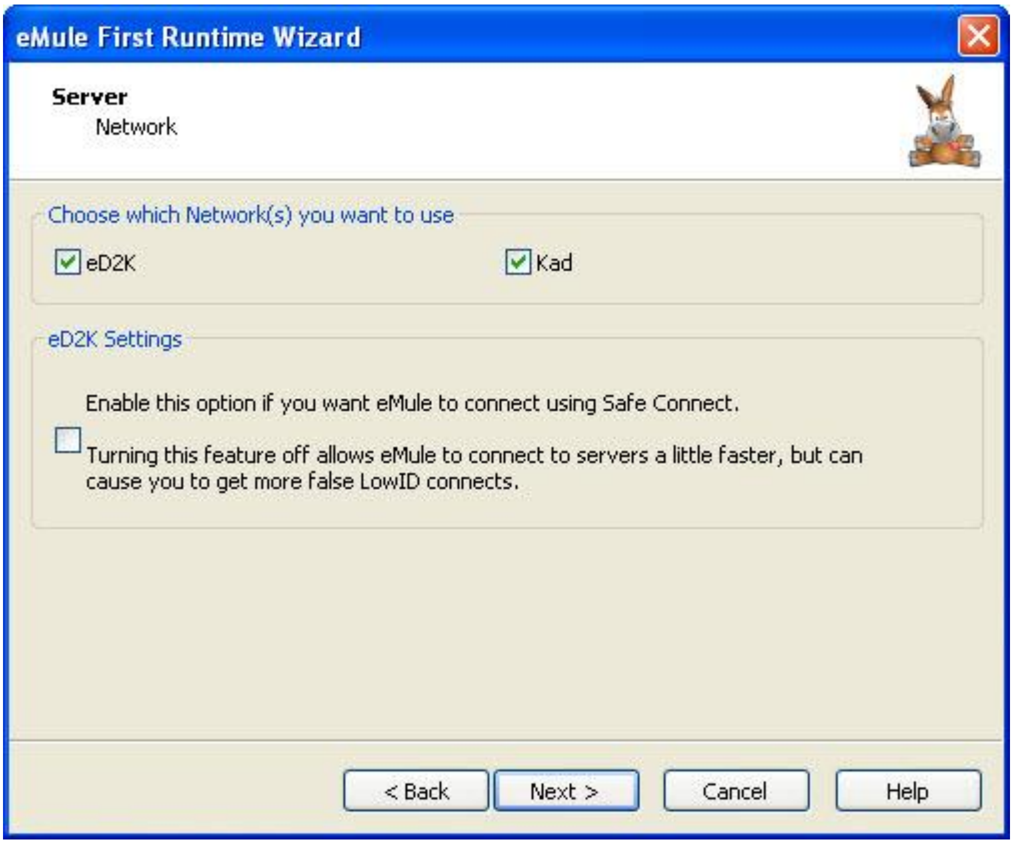
☑ Turning this on will allow eMule to boost rare files meaning popular files will be harder for other people to get. Turning this off will allow eMule to upload popular files more often meaning rare files will be harder for other people to get. This option will only affect future shared files.



Security
Obfuscation

Enable this option if you want to use protocol obfuscation

☐ If your ISP tries throttle or block eMule, enabling obfuscation will help to circumvent such restrictions.



Server

Network

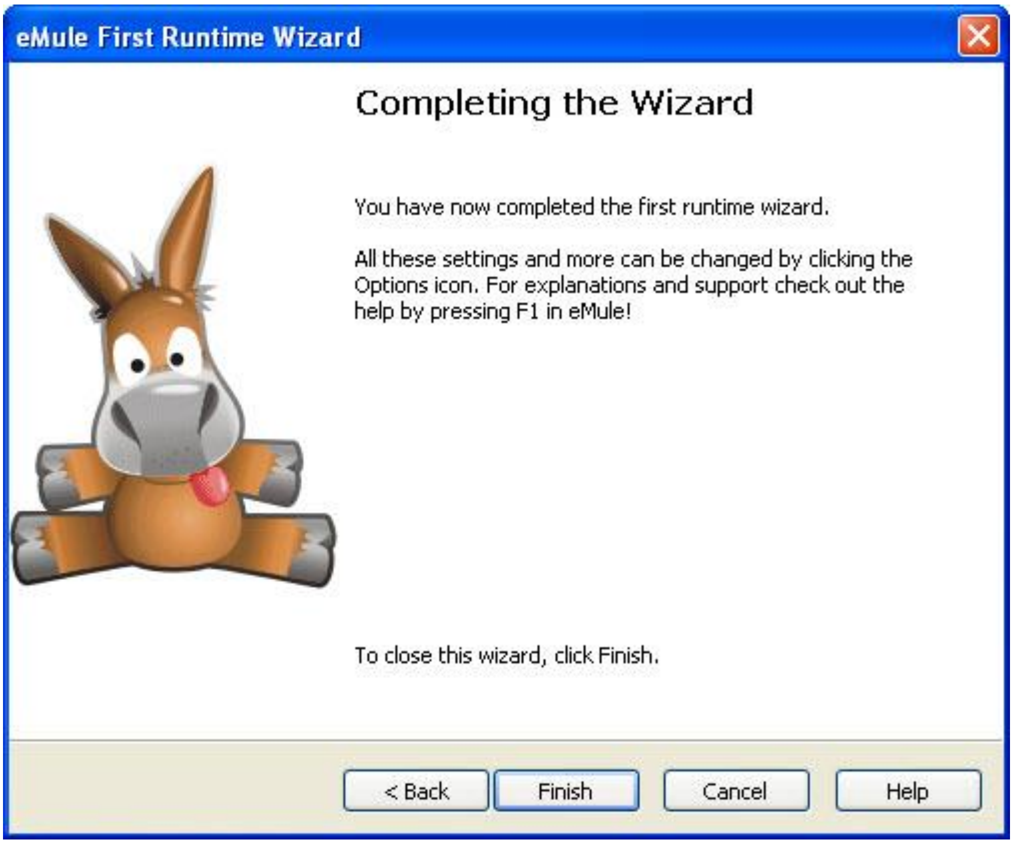
Choose which Network(s) you want to use

☑ eD2K ☑ Kad

eD2K Settings

Enable this option if you want eMule to connect using Safe Connect.

□ Turning this feature off allows eMule to connect to servers a little faster, but can cause you to get more false LowID connects.



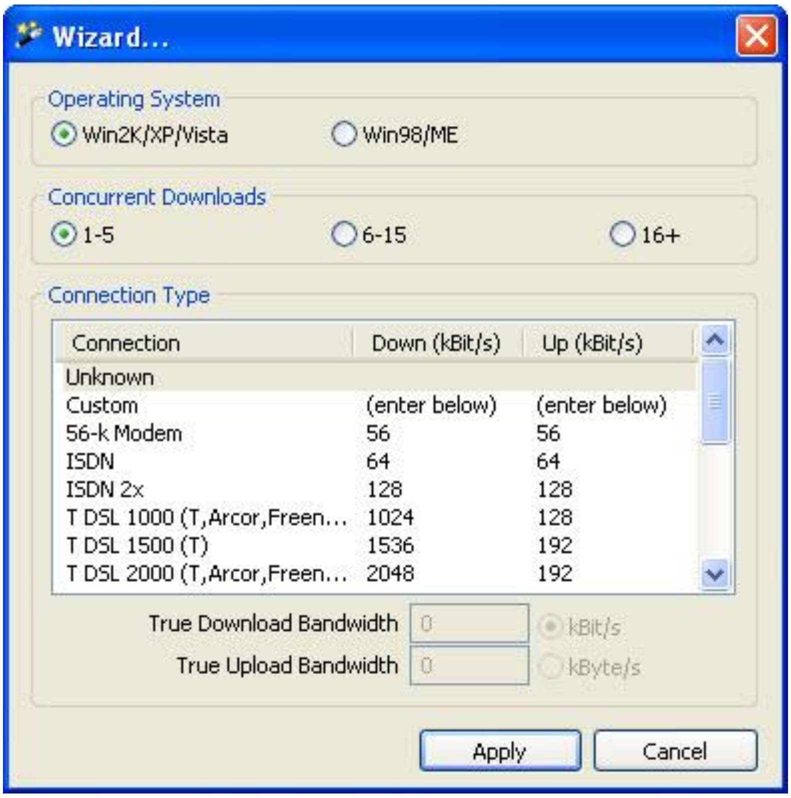
Completing the Wizard

You have now completed the first runtime wizard.

All these settings and more can be changed by clicking the Options icon. For explanations and support check out the help by pressing F1 in eMule!

To close this wizard, click Finish.

When you click on “Finish”, the programme starts up. Yet another set-up box appears:



Operating System

● Win2K/XP/Vista ○ Win98/ME

Concurrent Downloads

● 1-5 ○ 6-15 ○ 16+

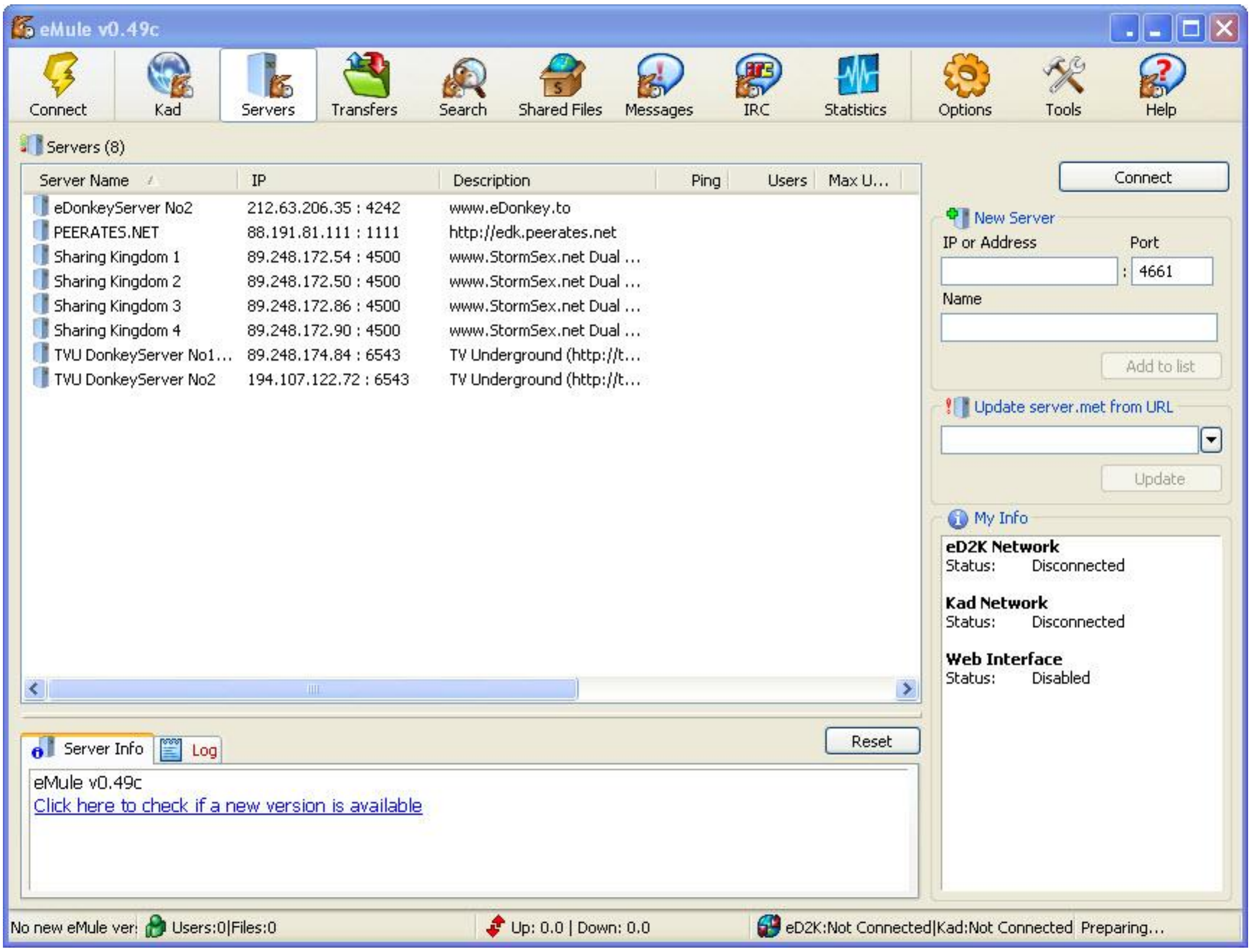
Connection Type

Connection	Down (kBit/s)	Up (kBit/s)
Unknown		
Custom	(enter below)	(enter below)
56-k Modem	56	56
ISDN	64	64
ISDN 2x	128	128
T DSL 1000 (T,Arcor,Freen...	1024	128
T DSL 1500 (T)	1536	192
T DSL 2000 (T,Arcor,Freen...	2048	192

True Download Bandwidth 0 ● kBit/s

True Upload Bandwidth 0 ○ kByte/s

When choices have been made in the box above, the start display appears:



Servers (8)

Server Name	IP	Description	Ping	Users	Max U...
eDonkeyServer No2	212.63.206.35 : 4242	www.eDonkey.to			
PEERATES.NET	88.191.81.111 : 1111	http://edk.peerates.net			
Sharing Kingdom 1	89.248.172.54 : 4500	www.StormSex.net Dual ...			
Sharing Kingdom 2	89.248.172.50 : 4500	www.StormSex.net Dual ...			
Sharing Kingdom 3	89.248.172.86 : 4500	www.StormSex.net Dual ...			
Sharing Kingdom 4	89.248.172.90 : 4500	www.StormSex.net Dual ...			
TVU DonkeyServer No1...	89.248.174.84 : 6543	TV Underground (http://t...			
TVU DonkeyServer No2	194.107.122.72 : 6543	TV Underground (http://t...			

IP or Address : Port 4661

Name

eD2K Network
Status: Disconnected

Kad Network
Status: Disconnected

Web Interface
Status: Disabled

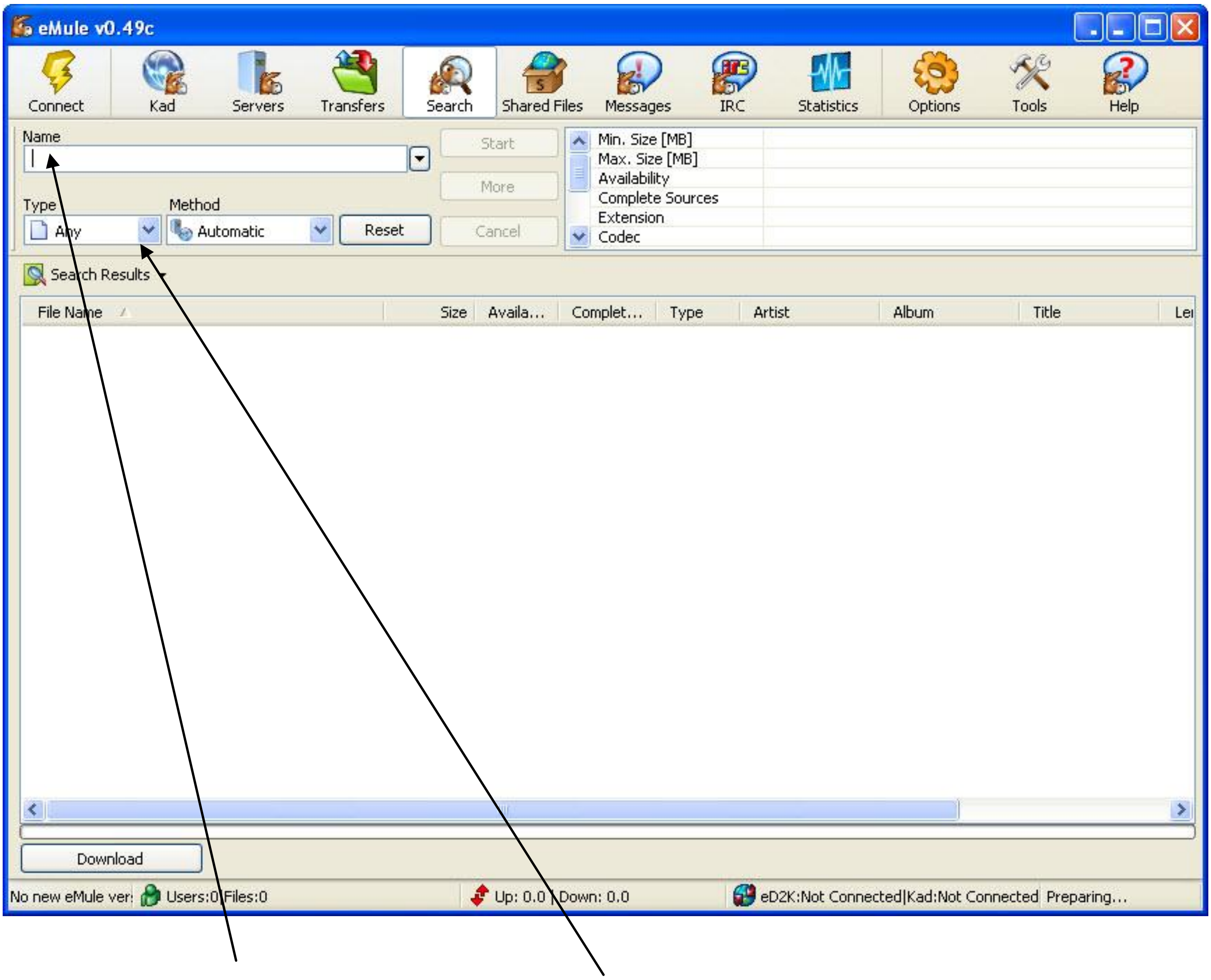
eMule v0.49c
Click here to check if a new version is available

No new eMule ver: Users:0|Files:0 Up: 0.0 | Down: 0.0 eD2K:Not Connected|Kad:Not Connected Preparing...

By clicking on ”Connect” the programme will go online.

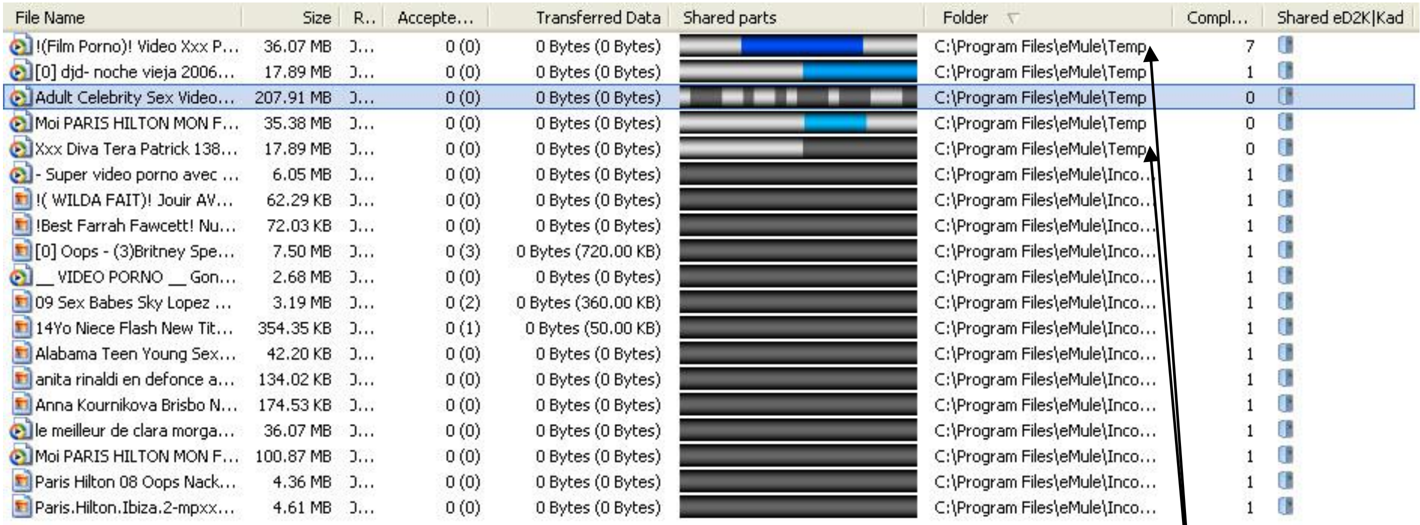
By clicking on the icons in the menu bar, we see the following pages:

Search function:



The search word is typed in the search field and a possible file type is chosen in the drop-down box.

Shared files



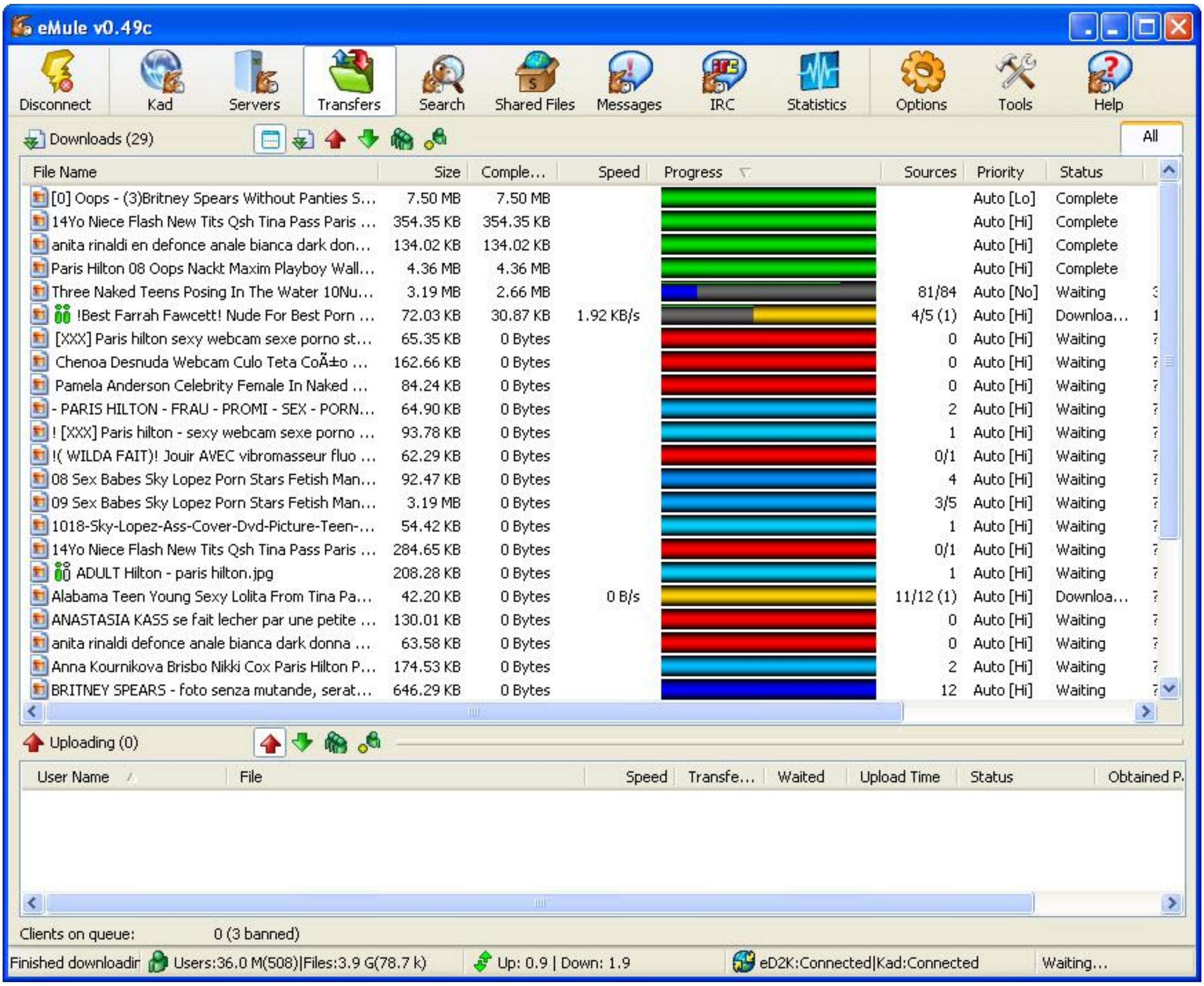
File Name	Size	R..	Accepte...	Transferred Data	Shared parts	Folder	Compl...	Shared eD2K|Kad
!(Film Porno)! Video Xxx P...	36.07 MB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Temp	7	
[0] djd- noche vieja 2006...	17.89 MB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Temp	1	
Adult Celebrity Sex Video...	207.91 MB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Temp	0	
Moi PARIS HILTON MON F...	35.38 MB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Temp	0	
Xxx Diva Tera Patrick 138...	17.89 MB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Temp	0	
- Super video porno avec ...	6.05 MB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco...	1	
!(WILDA FAIT)! Jouir AV...	62.29 KB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco...	1	
!Best Farrah Fawcett! Nu...	72.03 KB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco...	1	
[0] Oops - (3)Britney Spe...	7.50 MB	Ɔ...	0 (3)	0 Bytes (720.00 KB)		C:\Program Files\eMule\Inco...	1	
__ VIDEO PORNO __ Gon...	2.68 MB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco...	1	
09 Sex Babes Sky Lopez ...	3.19 MB	Ɔ...	0 (2)	0 Bytes (360.00 KB)		C:\Program Files\eMule\Inco...	1	
14Yo Niece Flash New Tit...	354.35 KB	Ɔ...	0 (1)	0 Bytes (50.00 KB)		C:\Program Files\eMule\Inco...	1	
Alabama Teen Young Sex...	42.20 KB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco...	1	
anita rinaldi en defonce a...	134.02 KB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco...	1	
Anna Kournikova Brisbo N...	174.53 KB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco...	1	
le meilleur de clara morga...	36.07 MB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco...	1	
Moi PARIS HILTON MON F...	100.87 MB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco...	1	
Paris Hilton 08 Oops Nack...	4.36 MB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco...	1	
Paris.Hilton.Ibiza.2-mpxx...	4.61 MB	Ɔ...	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco...	1	

(Here an example from a client that has been running for a while).

Notice the five files marked as being placed in the "Temp" folder. From these files sufficient material has been downloaded to share ("chunks larger than 9500 kb").

From the same display, you can see how many requests the network has sent for the individual shared files, how many requests have been accepted, and how many bytes material has been uploaded. All this information can be found in the file "known.met".

Downloads:



Downloads (29)

File Name	Size	Comple…	Speed	Progress	Sources	Priority	Status
[0] Oops - (3)Britney Spears Without Panties S…	7.50 MB	7.50 MB		🟩		Auto [Lo]	Complete
14Yo Niece Flash New Tits Qsh Tina Pass Paris …	354.35 KB	354.35 KB		🟩		Auto [Hi]	Complete
anita rinaldi en defonce anale bianca dark don…	134.02 KB	134.02 KB		🟩		Auto [Hi]	Complete
Paris Hilton 08 Oops Nackt Maxim Playboy Wall…	4.36 MB	4.36 MB		🟩		Auto [Hi]	Complete
Three Naked Teens Posing In The Water 10Nu…	3.19 MB	2.66 MB		🟦⬛	81/84	Auto [No]	Waiting
!Best Farrah Fawcett! Nude For Best Porn …	72.03 KB	30.87 KB	1.92 KB/s	⬛🟨	4/5 (1)	Auto [Hi]	Downloa…
[XXX] Paris hilton sexy webcam sexe porno st…	65.35 KB	0 Bytes		🟥	0	Auto [Hi]	Waiting
Chenoa Desnuda Webcam Culo Teta CoÃ±o …	162.66 KB	0 Bytes		🟥	0	Auto [Hi]	Waiting
Pamela Anderson Celebrity Female In Naked …	84.24 KB	0 Bytes		🟥	0	Auto [Hi]	Waiting
- PARIS HILTON - FRAU - PROMI - SEX - PORN…	64.90 KB	0 Bytes		🟦	2	Auto [Hi]	Waiting
! [XXX] Paris hilton - sexy webcam sexe porno …	93.78 KB	0 Bytes		🟦	1	Auto [Hi]	Waiting
!(WILDA FAIT)! Jouir AVEC vibromasseur fluo …	62.29 KB	0 Bytes		🟥	0/1	Auto [Hi]	Waiting
08 Sex Babes Sky Lopez Porn Stars Fetish Man…	92.47 KB	0 Bytes		🟦	4	Auto [Hi]	Waiting
09 Sex Babes Sky Lopez Porn Stars Fetish Man…	3.19 MB	0 Bytes		🟦	3/5	Auto [Hi]	Waiting
1018-Sky-Lopez-Ass-Cover-Dvd-Picture-Teen-…	54.42 KB	0 Bytes		🟦	1	Auto [Hi]	Waiting
14Yo Niece Flash New Tits Qsh Tina Pass Paris …	284.65 KB	0 Bytes		🟥	0/1	Auto [Hi]	Waiting
ADULT Hilton - paris hilton.jpg	208.28 KB	0 Bytes		🟦	1	Auto [Hi]	Waiting
Alabama Teen Young Sexy Lolita From Tina Pa…	42.20 KB	0 Bytes	0 B/s	🟨	11/12 (1)	Auto [Hi]	Downloa…
ANASTASIA KASS se fait lecher par une petite …	130.01 KB	0 Bytes		🟥	0	Auto [Hi]	Waiting
anita rinaldi defonce anale bianca dark donna …	63.58 KB	0 Bytes		🟥	0	Auto [Hi]	Waiting
Anna Kournikova Brisbo Nikki Cox Paris Hilton P…	174.53 KB	0 Bytes		🟦	2	Auto [Hi]	Waiting
BRITNEY SPEARS - foto senza mutande, serat…	646.29 KB	0 Bytes		🟦	12	Auto [Hi]	Waiting

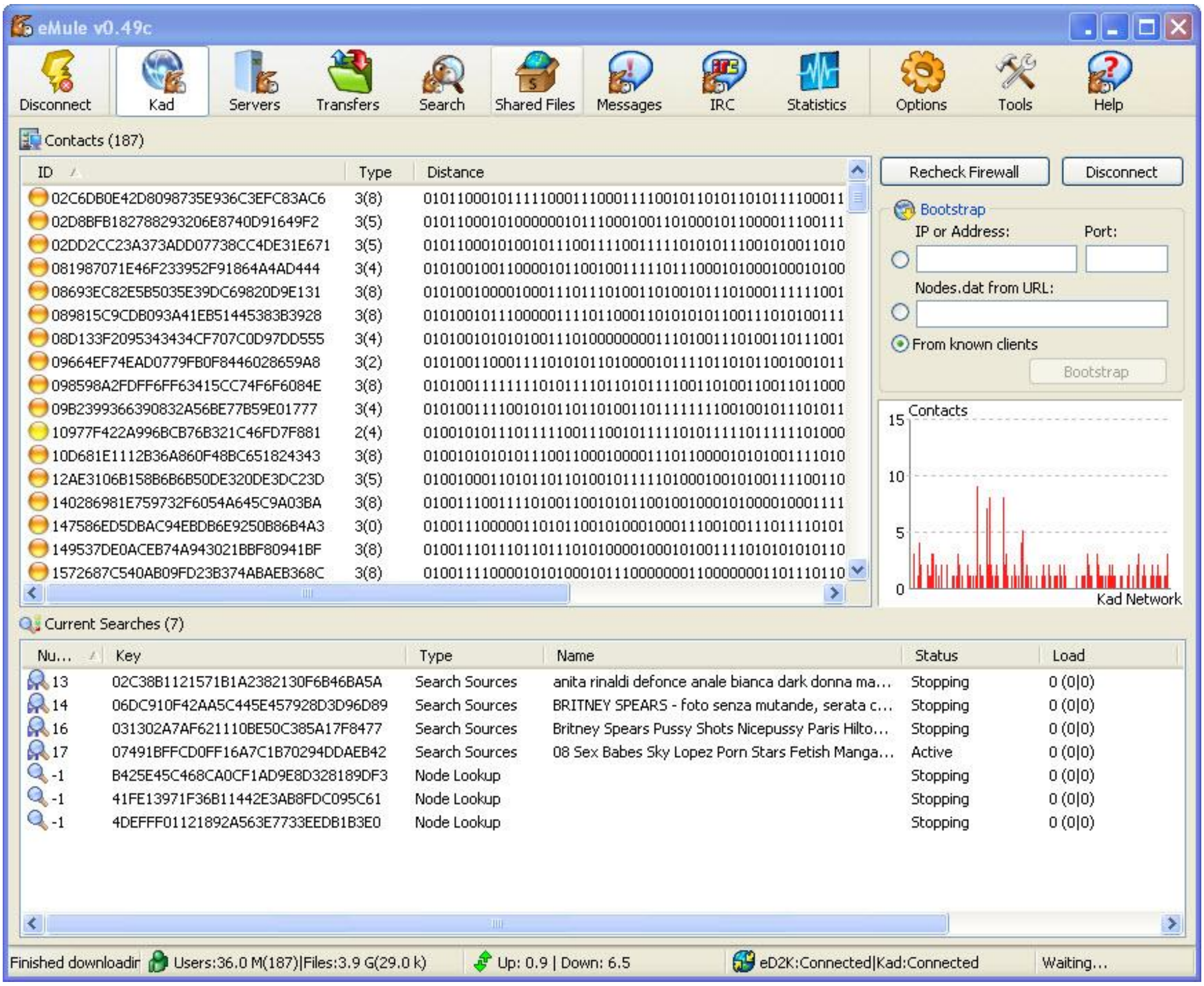
Uploading (0)

User Name	File	Speed	Transfe…	Waited	Upload Time	Status	Obtained P.

Clients on queue: 0 (3 banned)

Finished downloadir | Users:36.0 M(508)\|Files:3.9 G(78.7 k) | Up: 0.9 \| Down: 1.9 | eD2K:Connected\|Kad:Connected | Waiting…

KAD:



Contacts (187)

ID	Type	Distance
02C6DB0E42D8098735E936C3EFC83AC6	3(8)	0101100010111110001110001111001011010110101111100011
02D8BFB182788293206E8740D91649F2	3(5)	010110001010000001011100010011010001011000011100111
02DD2CC23A373ADD07738CC4DE31E671	3(5)	010110001010010111001111001111010101110010100110 10
081987071E46F233952F91864A4AD444	3(4)	010100100110000101100100111110111000101000100010100
08693EC82E5B5035E39DC69820D9E131	3(8)	010100100001000111011101001101001011101000111111001
089815C9CDB093A41EB51445383B3928	3(8)	010100101110000011110110001101010101100111010100111
08D133F2095343434CF707C0D97DD555	3(4)	010100101010100111010000000011101001110100110111001
09664EF74EAD0779FB0F8446028659A8	3(2)	010100110001111010101101000010111101101011001001011
098598A2FDFF6FF63415CC74F6F6084E	3(8)	010100111111110101111011010111100110100110011011000
09B2399366390832A56BE77B59E01777	3(4)	010100111100101011011010011011111111001001011101011
10977F422A996BCB76B321C46FD7F881	2(4)	010010101110111110011100101111101011111011111101000
10D681E1112B36A860F48BC651824343	3(8)	010010101010111001100010000111011000010101001111010
12AE3106B158B6B6B50DE320DE3DC23D	3(5)	010010001101011011010010111110100010010100111100110
140286981E759732F6054A645C9A03BA	3(8)	010011100111101001100101011001001000101000010001111
147586ED5DBAC94EBDB6E9250B86B4A3	3(0)	010011100000110101100101000100011100100111011110101
149537DE0ACEB74A943021BBF80941BF	3(8)	010011101110110111010100001000101001111010101010110
1572687C540AB09FD23B374ABAEB368C	3(8)	0100111100001010100010111000000001100000001101110110

Bootstrap

IP or Address: Port:

○ Nodes.dat from URL:

○

● From known clients

Bootstrap

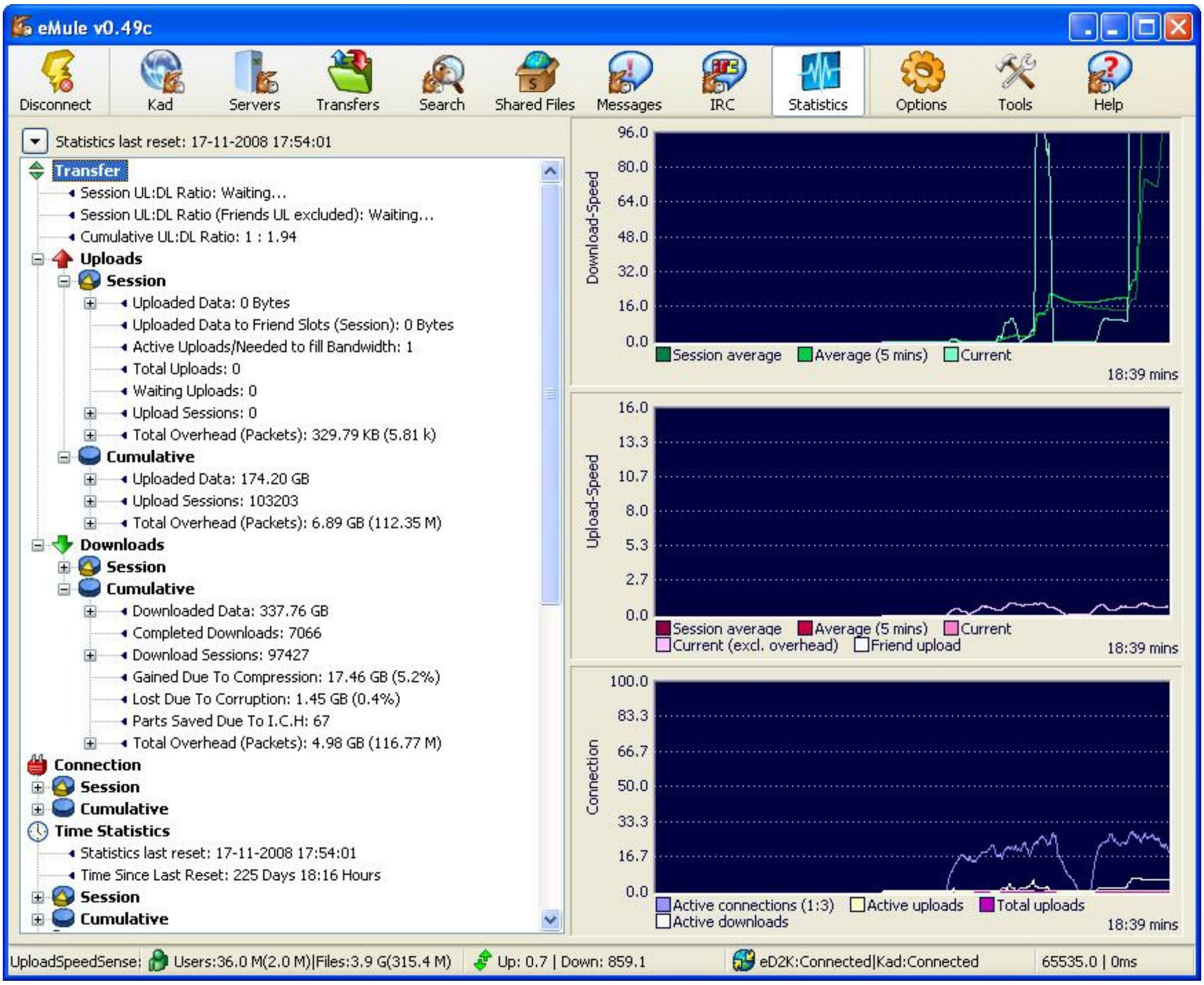
Current Searches (7)

Nu...	Key	Type	Name	Status	Load
13	02C38B1121571B1A2382130F6B46BA5A	Search Sources	anita rinaldi defonce anale bianca dark donna ma...	Stopping	0 (0|0)
14	06DC910F42AA5C445E457928D3D96D89	Search Sources	BRITNEY SPEARS - foto senza mutande, serata c...	Stopping	0 (0|0)
16	031302A7AF621110BE50C385A17F8477	Search Sources	Britney Spears Pussy Shots Nicepussy Paris Hilto...	Stopping	0 (0|0)
17	07491BFFCD0FF16A7C1B70294DDAEB42	Search Sources	08 Sex Babes Sky Lopez Porn Stars Fetish Manga...	Active	0 (0|0)
-1	B425E45C468CA0CF1AD9E8D328189DF3	Node Lookup		Stopping	0 (0|0)
-1	41FE13971F36B11442E3AB8FDC095C61	Node Lookup		Stopping	0 (0|0)
-1	4DEFFF01121892A563E7733EEDB1B3E0	Node Lookup		Stopping	0 (0|0)

Finished downloadir | Users:36.0 M(187)|Files:3.9 G(29.0 k) | Up: 0.9 | Down: 6.5 | eD2K:Connected|Kad:Connected | Waiting...

Shows the actual connection to the KAD network.

Statistics:



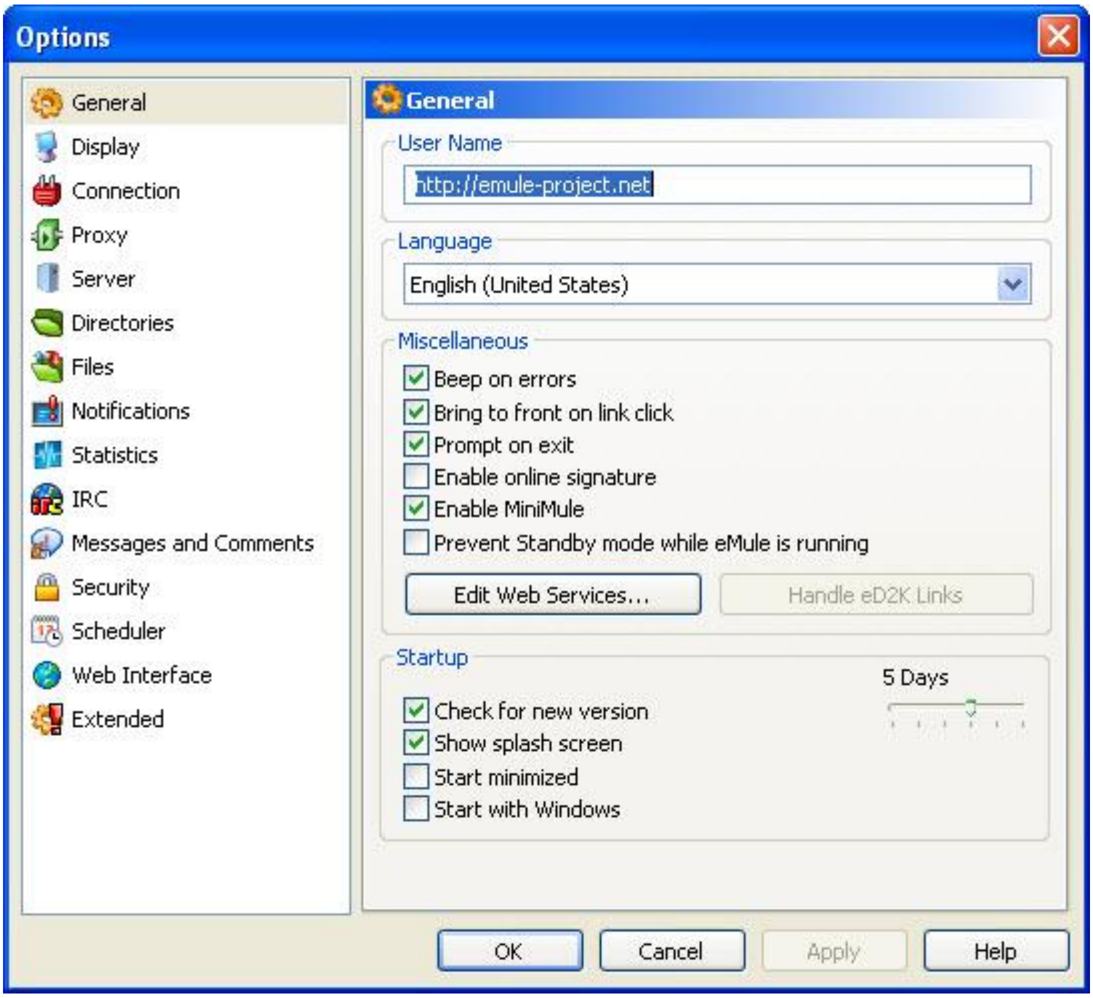
Statistics last reset: 17-11-2008 17:54:01

- Transfer
  - Session UL:DL Ratio: Waiting...
  - Session UL:DL Ratio (Friends UL excluded): Waiting...
  - Cumulative UL:DL Ratio: 1 : 1.94
  - Uploads
    - Session
      - Uploaded Data: 0 Bytes
      - Uploaded Data to Friend Slots (Session): 0 Bytes
      - Active Uploads/Needed to fill Bandwidth: 1
      - Total Uploads: 0
      - Waiting Uploads: 0
      - Upload Sessions: 0
      - Total Overhead (Packets): 329.79 KB (5.81 k)
    - Cumulative
      - Uploaded Data: 174.20 GB
      - Upload Sessions: 103203
      - Total Overhead (Packets): 6.89 GB (112.35 M)
  - Downloads
    - Session
    - Cumulative
      - Downloaded Data: 337.76 GB
      - Completed Downloads: 7066
      - Download Sessions: 97427
      - Gained Due To Compression: 17.46 GB (5.2%)
      - Lost Due To Corruption: 1.45 GB (0.4%)
      - Parts Saved Due To I.C.H: 67
      - Total Overhead (Packets): 4.98 GB (116.77 M)
- Connection
  - Session
  - Cumulative
- Time Statistics
  - Statistics last reset: 17-11-2008 17:54:01
  - Time Since Last Reset: 225 Days 18:16 Hours
  - Session
  - Cumulative

UploadSpeedSense: Users:36.0 M(2.0 M)|Files:3.9 G(315.4 M) Up: 0.7 | Down: 859.1 eD2K:Connected|Kad:Connected 65535.0 | 0ms

From the statistics picture, you can see the active traffic, accumulated data for downloads, uptime and so on. The content is constructed from the file “statistics.ini” – the page is just a graphic presentation of these data.

Settings:



User Name
http://emule-project.net

Language
English (United States)

Miscellaneous
☑ Beep on errors
☑ Bring to front on link click
☑ Prompt on exit
□ Enable online signature
☑ Enable MiniMule
□ Prevent Standby mode while eMule is running

Startup
5 Days
☑ Check for new version
☑ Show splash screen
□ Start minimized
□ Start with Windows

Under “Settings”, there are a number of possibilities, in which you can set up your client. It will, however, take too long to cover all functions.

Under ”Directories” , it will be shown, which folders the user actively has chosen to share.

Under “Extended” it will be indicated, whether the user has chosen to log traffic.

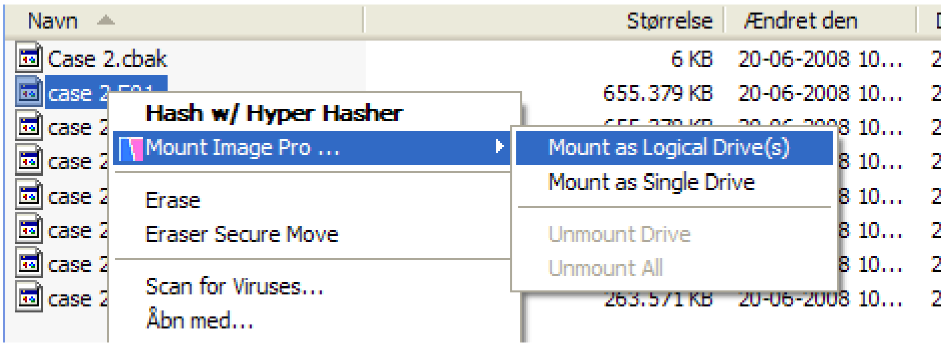
The Mounting of an Installed eMule Client

In connection with the examination of an installed client, it is possible to get the client running/started by mounting the evidence file containing the disk from the installed client.

You can mount the Evidence file in different ways – either by mounting it directly from EnCase or by using Mount Image Pro (which I recommend).

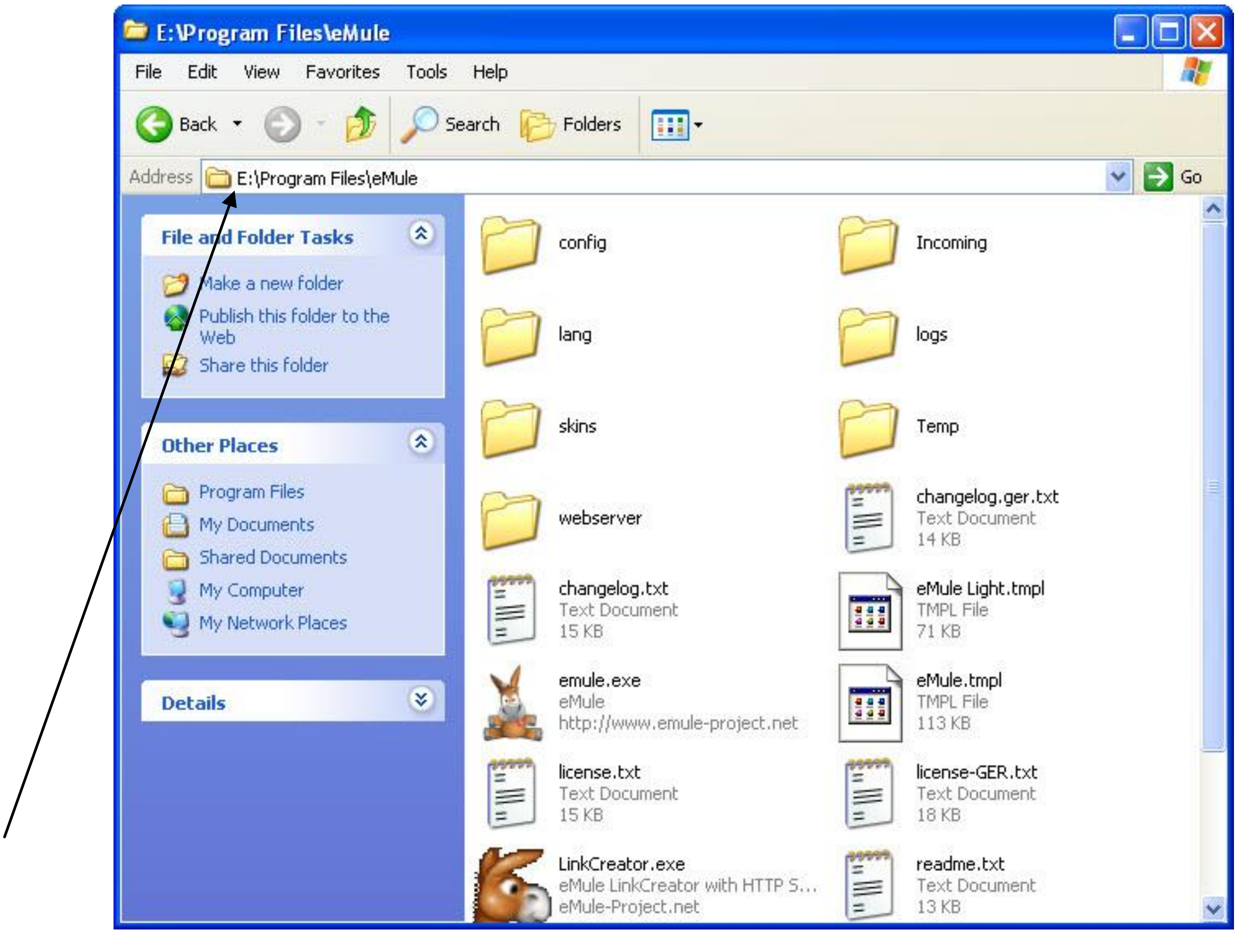
Mounting via Mount Image Pro takes place this way:

1. Open the folder containing the Evidence file that is to be mounted.
2. Right-click on the ”*.E01” file and choose ”Mount Image Pro ->Mount as Logical Drive(s)”.



3. The drive will now be available in ”Denne Computer” (This computer).

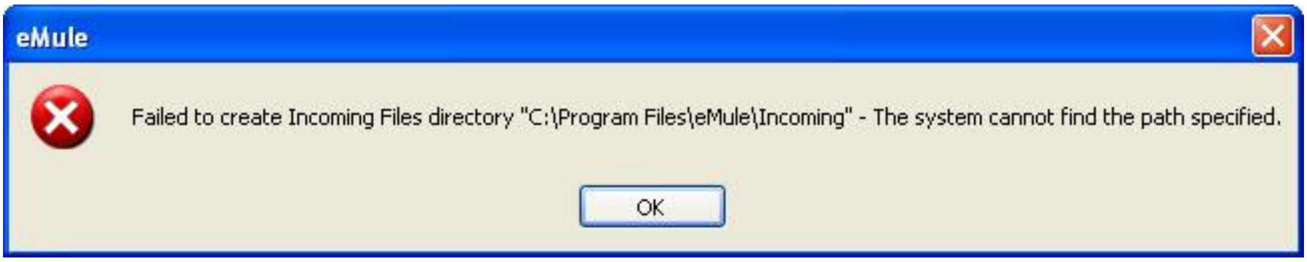
4. It is now possible to browse to the ”eMule mappen” (eMule folder) on the mounted drive.


E:\Program Files\eMule
File Edit View Favorites Tools Help
Back
Search
Folders
Address E:\Program Files\eMule
Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
Program Files
My Documents
Shared Documents
My Computer
My Network Places
Details
config
Incoming
lang
logs
skins
Temp
webserver
changelog.ger.txt Text Document 14 KB
changelog.txt Text Document 15 KB
eMule Light.tmpl TMPL File 71 KB
emule.exe eMule http://www.emule-project.net
eMule.tmpl TMPL File 113 KB
license.txt Text Document 15 KB
license-GER.txt Text Document 18 KB
LinkCreator.exe eMule LinkCreator with HTTP S... eMule-Project.net
readme.txt Text Document 13 KB

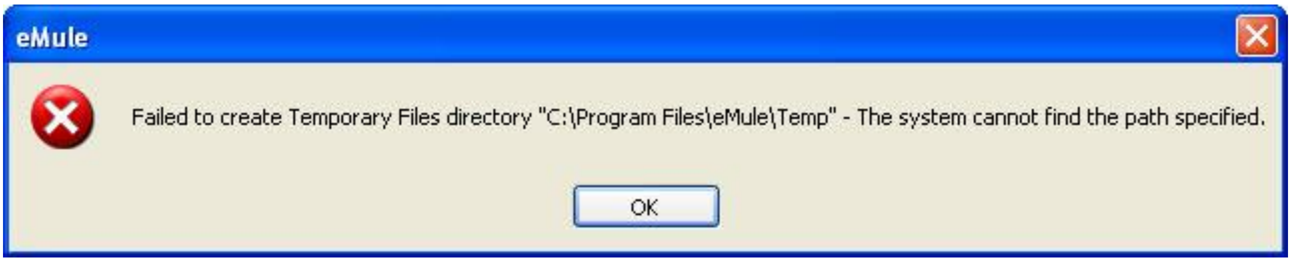
Notice, that the drive has got another drive letter. Originally, it would have had “C” as drive name.

5. Double-click on ”emule.exe”.

6. At start up of the programme, an error message will appear telling you that the folders ”C:\Programmer\eMule\incoming” and ”C:\Programmer\eMule\Temp” are not to be found.



Failed to create Incoming Files directory "C:\Program Files\eMule\Incoming" - The system cannot find the path specified.



eMule

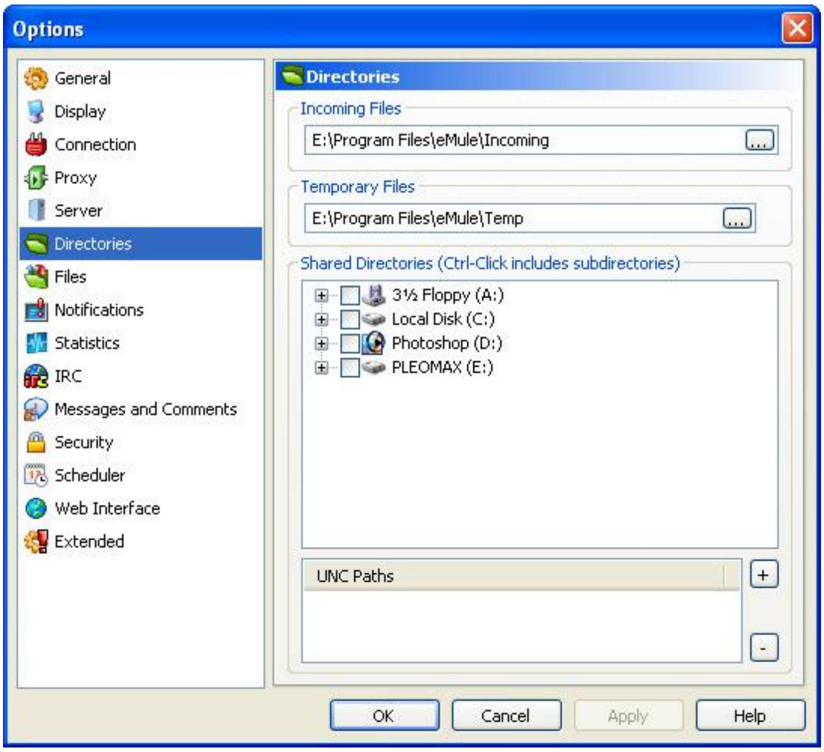
Failed to create Temporary Files directory "C:\Program Files\eMule\Temp" - The system cannot find the path specified.

As can be seen, the programme is unable to find the folders on the path. The path has to be corrected subsequently in the programme itself.

7. Click on “OK” for both error messages and open the programme’s user interface.

8. Go to ”\eMule\Config\shareddir.dat” and open this via Notepad. Read which possible folders have been shared by the user (notice that possible subfolders are not automatically shared).

9. Return to eMule’s user interface and choose the menu item ”Options” and the submenu ”Directories” . Correct the drive name to the drive letter, that the disk is mounted with, and mark possible user made folders as shared (the folders that are mentioned in ”shareddir.dat”).



Directories

Incoming Files: E:\Program Files\eMule\Incoming

Temporary Files: E:\Program Files\eMule\Temp

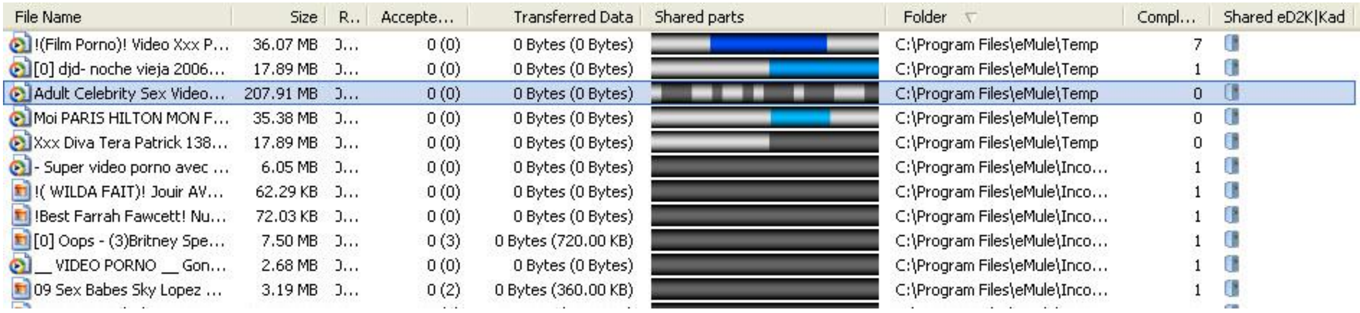
Shared Directories (Ctrl-Click includes subdirectories)

- ☐ 3½ Floppy (A:)
- ☐ Local Disk (C:)
- ☐ Photoshop (D:)
- ☐ PLEOMAX (E:)

10. Click “OK”.

11. Shut down and restart eMule.

12. It is now possible to see all shared files – including possible files that are about to be downloaded and where sufficient data has been downloaded for sharing.



File Name	Size	R..	Accepte…	Transferred Data	Shared parts	Folder	Compl…	Shared eD2K|Kad
!(Film Porno)! Video Xxx P…	36.07 MB	J…	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Temp	7	
[0] djd- noche vieja 2006…	17.89 MB	J…	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Temp	1	
Adult Celebrity Sex Video…	207.91 MB	J…	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Temp	0	
Moi PARIS HILTON MON F…	35.38 MB	J…	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Temp	0	
Xxx Diva Tera Patrick 138…	17.89 MB	J…	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Temp	0	
- Super video porno avec …	6.05 MB	J…	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco…	1	
!(WILDA FAIT)! Jouir AV…	62.29 KB	J…	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco…	1	
!Best Farrah Fawcett! Nu…	72.03 KB	J…	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco…	1	
[0] Oops - (3)Britney Spe…	7.50 MB	J…	0 (3)	0 Bytes (720.00 KB)		C:\Program Files\eMule\Inco…	1	
__VIDEO PORNO __Gon…	2.68 MB	J…	0 (0)	0 Bytes (0 Bytes)		C:\Program Files\eMule\Inco…	1	
09 Sex Babes Sky Lopez …	3.19 MB	J…	0 (2)	0 Bytes (360.00 KB)		C:\Program Files\eMule\Inco…	1	

13. In connection with this exercise, it is a good idea to document your discoveries with screen dumps. These pictures often say more than words and show how the user has seen his interface.

It is completely safe to use this method as the Evidence file is write protected, which means that possible changes only take place in RAM.

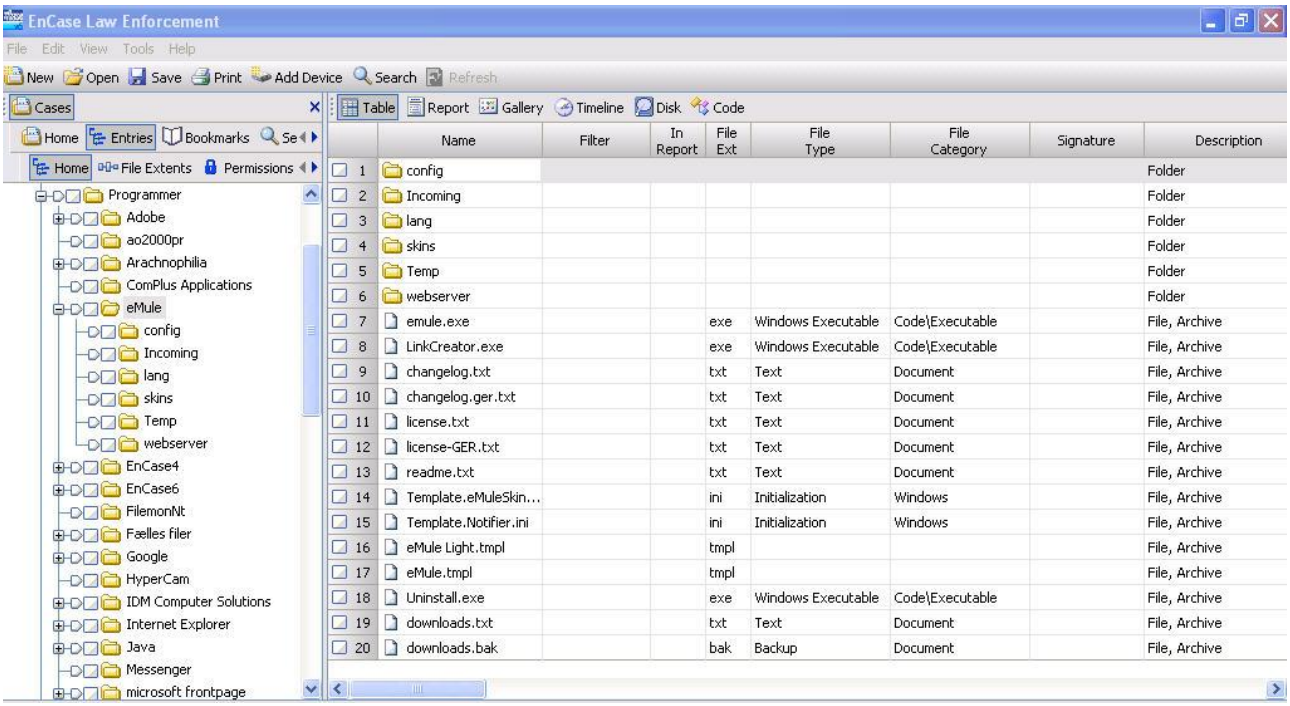
This method is relatively simple to carry out. Of course, you may also start the mounted disk through LiveView and VirtualMachine. This is, however, only possible if all shared folders are placed on the same physical hard disk, as it is not immediately possible to mount several disks at the same time and run them through LiveView.

By making use of the above-mentioned method, it is possible to mount a random number of disks and get the installation running across various disks.

Forensic Examination of eMule

Standard installation

The standard installation of eMule is found on "C:\Programmers\eMule”. The installation automatically sets up the folders “C:\Programmer\eMule\incoming" and "C:\Programmer\eMule\Temp" as shared with other users. As mentioned earlier, this “share” function cannot be switched off.
In EnCase it looks like this:



	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description
☐ 1	config							Folder
☐ 2	Incoming							Folder
☐ 3	lang							Folder
☐ 4	skins							Folder
☐ 5	Temp							Folder
☐ 6	webserver							Folder
☐ 7	emule.exe			exe	Windows Executable	Code\Executable		File, Archive
☐ 8	LinkCreator.exe			exe	Windows Executable	Code\Executable		File, Archive
☐ 9	changelog.txt			txt	Text	Document		File, Archive
☐ 10	changelog.ger.txt			txt	Text	Document		File, Archive
☐ 11	license.txt			txt	Text	Document		File, Archive
☐ 12	license-GER.txt			txt	Text	Document		File, Archive
☐ 13	readme.txt			txt	Text	Document		File, Archive
☐ 14	Template.eMuleSkin...			ini	Initialization	Windows		File, Archive
☐ 15	Template.Notifier.ini			ini	Initialization	Windows		File, Archive
☐ 16	eMule Light.tmpl			tmpl				File, Archive
☐ 17	eMule.tmpl			tmpl				File, Archive
☐ 18	Uninstall.exe			exe	Windows Executable	Code\Executable		File, Archive
☐ 19	downloads.txt			txt	Text	Document		File, Archive
☐ 20	downloads.bak			bak	Backup	Document		File, Archive

Windows registry

We find no information of any interest in the registry.

Information about shared folders/files

In the file "C:\Programmer\eMule\config\sharedir.dat", we find information about shared folders (apart from ”Incoming” and ”Temp”). The files can be opened by Notepad.

Other Files of Interest

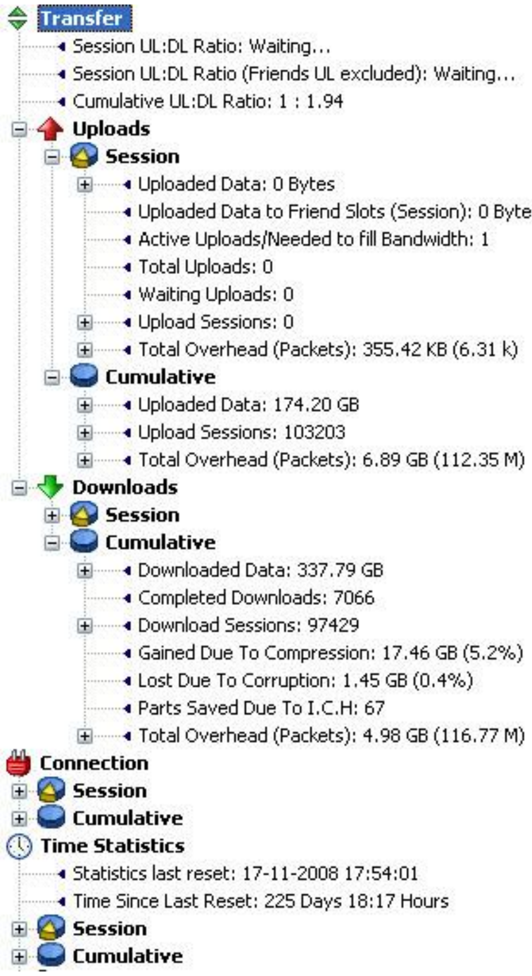
The files listed below are worth examining closer:

14. preferences.ini (Contains information about accumulated up-/download, among other things)
15. downloads.txt (Contains information about ongoing downloads)
16. AC_Searchstring.dat (Contains the last typed search words)
17. known.met (Information about files that have been shared – both present and former)

preferences.ini

The file is found in the folder ”C:\Programmer\eMule\config”.

The content of “preferences.ini” can be documented with advantage, by activating the client and having the content visually presented:



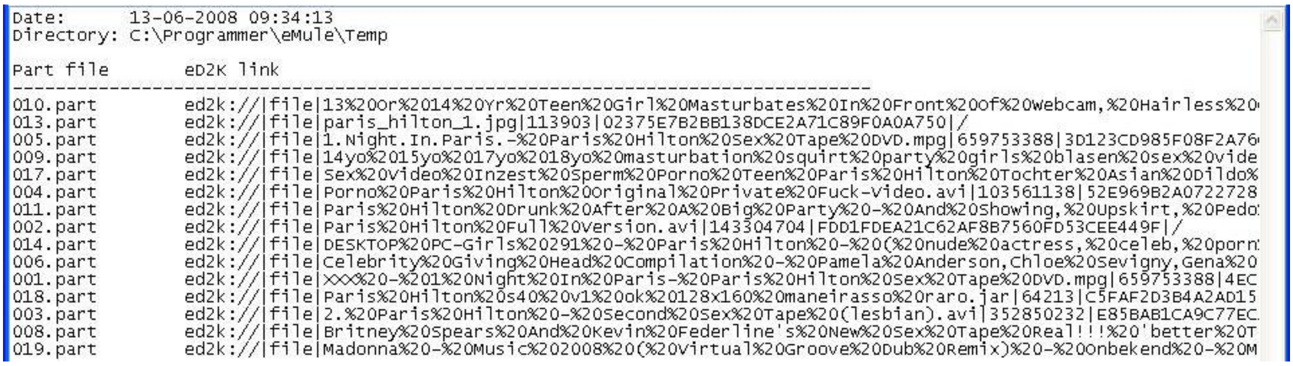
```
Transfer
    Session UL:DL Ratio: Waiting...
    Session UL:DL Ratio (Friends UL excluded): Waiting...
    Cumulative UL:DL Ratio: 1 : 1.94
  Uploads
    Session
      Uploaded Data: 0 Bytes
      Uploaded Data to Friend Slots (Session): 0 Bytes
      Active Uploads/Needed to fill Bandwidth: 1
      Total Uploads: 0
      Waiting Uploads: 0
      Upload Sessions: 0
      Total Overhead (Packets): 355.42 KB (6.31 k)
    Cumulative
      Uploaded Data: 174.20 GB
      Upload Sessions: 103203
      Total Overhead (Packets): 6.89 GB (112.35 M)
  Downloads
    Session
    Cumulative
      Downloaded Data: 337.79 GB
      Completed Downloads: 7066
      Download Sessions: 97429
      Gained Due To Compression: 17.46 GB (5.2%)
      Lost Due To Corruption: 1.45 GB (0.4%)
      Parts Saved Due To I.C.H: 67
      Total Overhead (Packets): 4.98 GB (116.77 M)
Connection
  Session
  Cumulative
Time Statistics
    Statistics last reset: 17-11-2008 17:54:01
    Time Since Last Reset: 225 Days 18:17 Hours
  Session
  Cumulative
```

downloads.txt

The file is found in the folder ”C:\Programmer\eMule\”.

This file contains information about the files that are being downloaded at present – that is the same information which is shown under the tab “Overførsler” (Transfer).

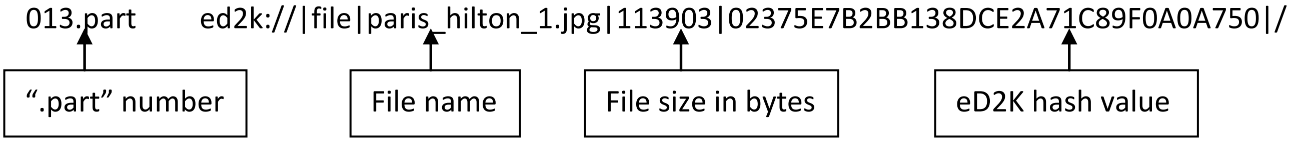
The content is readable in Notepad and will look like this:



```
Date:      13-06-2008 09:34:13
Directory: C:\Programmer\eMule\Temp

Part file       eD2K link
------------------------------------------------------------------------------------
010.part        ed2k://|file|13%20Or%2014%20Yr%20Teen%20Girl%20Masturbates%20In%20Front%20Of%20Webcam,%20Hairless%20
013.part        ed2k://|file|paris_hilton_1.jpg|113903|02375E7B2BB138DCE2A71C89F0A0A750|/
005.part        ed2k://|file|1.Night.In.Paris.-%20Paris%20Hilton%20Sex%20Tape%20DVD.mpg|659753388|3D123CD985F08F2A76
009.part        ed2k://|file|14yo%2015yo%2017yo%2018yo%20masturbation%20squirt%20party%20girls%20blasen%20sex%20vide
017.part        ed2k://|file|Sex%20Video%20Inzest%20Sperm%20Porno%20Teen%20Paris%20Hilton%20Tochter%20Asian%20Dildo%
004.part        ed2k://|file|Porno%20Paris%20Hilton%20Original%20Private%20Fuck-Video.avi|103561138|52E969B2A0722728
011.part        ed2k://|file|Paris%20Hilton%20Drunk%20After%20A%20Big%20Party%20-%20And%20Showing,%20Upskirt,%20Pedo
002.part        ed2k://|file|Paris%20Hilton%20Full%20Version.avi|143304704|FDD1FDEA21C62AF8B7560FD53CEE449F|/
014.part        ed2k://|file|DESKTOP%20PC-Girls%20291%20-%20Paris%20Hilton%20-%20(%20nude%20actress,%20celeb,%20porn
006.part        ed2k://|file|Celebrity%20Giving%20Head%20Compilation%20-%20Pamela%20Anderson,Chloe%20Sevigny,Gena%20
001.part        ed2k://|file|XXX%20-%201%20Night%20In%20Paris-%20Paris%20Hilton%20Sex%20Tape%20DVD.mpg|659753388|4EC
018.part        ed2k://|file|Paris%20Hilton%20s40%20v1%20ok%20128x160%20maneirasso%20raro.jar|64213|C5FAF2D3B4A2AD15
003.part        ed2k://|file|2.%20Paris%20Hilton%20-%20Second%20Sex%20Tape%20(lesbian).avi|352850232|E85BAB1CA9C77EC
008.part        ed2k://|file|Britney%20Spears%20And%20Kevin%20Federline's%20New%20Sex%20Tape%20Real!!!%20'better%20T
019.part        ed2k://|file|Madonna%20-%20Music%202008%20(%20Virtual%20Groove%20Dub%20Remix)%20-%20Onbekend%20-%20M
```

A line in “downloads.txt” could look something like this:



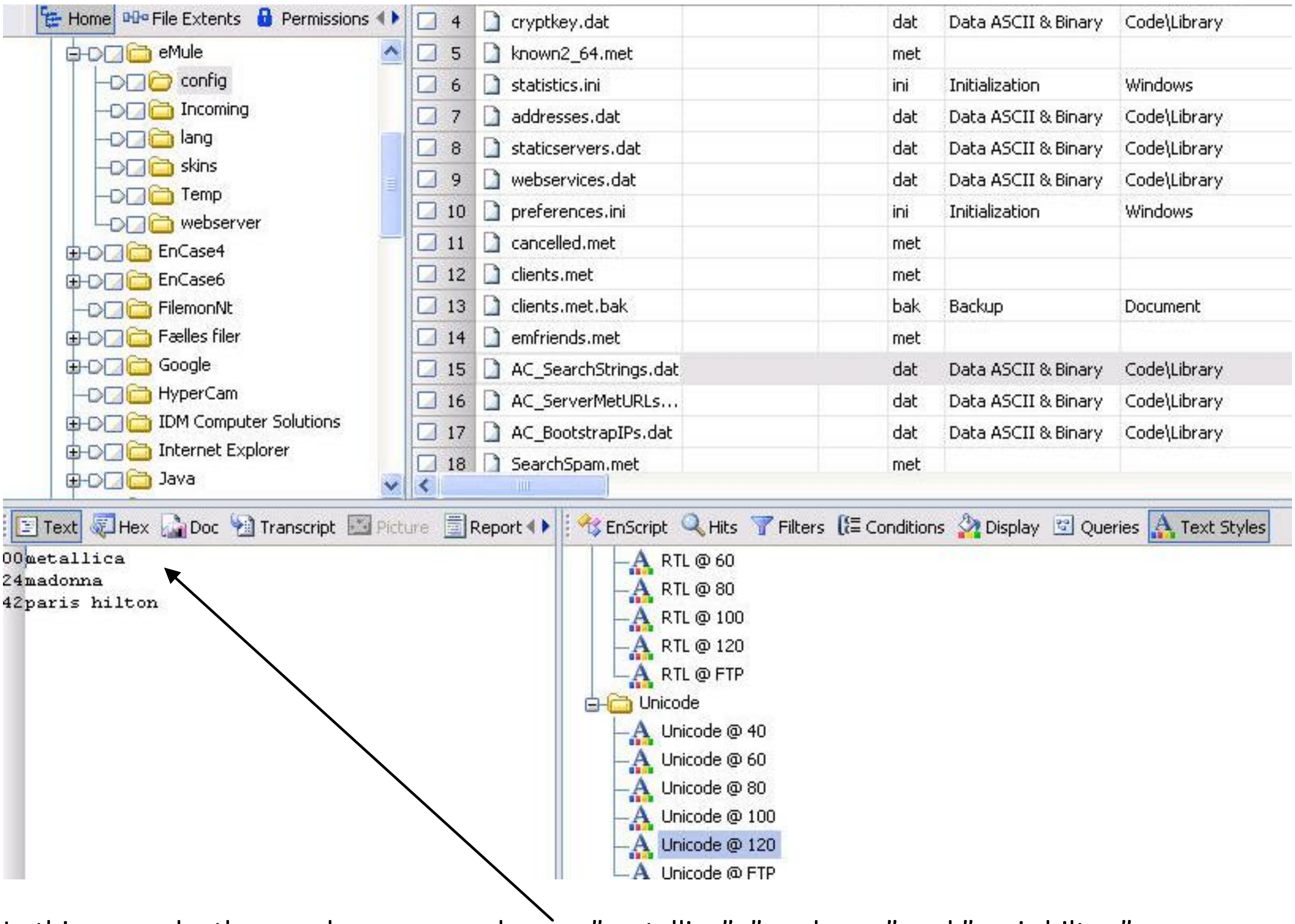
013.part   ed2k://|file|paris_hilton_1.jpg|113903|02375E7B2BB138DCE2A71C89F0A0A750|/

The line above is a fully valid eD2K link that can be copied directly into a browser, which then automatically opens an eMule and starts downloading this specific file.

AC_SearchStrings.dat

The file is found in the folder ”C:\Programmer\eMule\config”.

The file contains information about the search words last used. The words are given in Unicode. In EnCase, “Text Styles” may with advantage be set to Unicode:



4	cryptkey.dat	dat	Data ASCII & Binary	Code\Library
5	known2_64.met	met		
6	statistics.ini	ini	Initialization	Windows
7	addresses.dat	dat	Data ASCII & Binary	Code\Library
8	staticservers.dat	dat	Data ASCII & Binary	Code\Library
9	webservices.dat	dat	Data ASCII & Binary	Code\Library
10	preferences.ini	ini	Initialization	Windows
11	cancelled.met	met		
12	clients.met	met		
13	clients.met.bak	bak	Backup	Document
14	emfriends.met	met		
15	AC_SearchStrings.dat	dat	Data ASCII & Binary	Code\Library
16	AC_ServerMetURLs...	dat	Data ASCII & Binary	Code\Library
17	AC_BootstrapIPs.dat	dat	Data ASCII & Binary	Code\Library
18	SearchSpam.met	met		

```
00metallica
24madonna
42paris hilton
```

In this example, the user has run searches on ”metallica”, ”madonna” and ”paris hilton”.

known.met

The file is found in the folder ”C:\Programmer\eMule\config”.

“Known.met” is a virtual gold mine of data. The file contains information about all files that have been downloaded through the programme – or have been placed at the disposal of other clients by our user. It is possible to read out the data listed below:

- File name
- File size
- eD2K hash value
- When the date has last been changed
- Number of requests for the file from the network

- Number of requests accepted
- Number of bytes that have been uploaded
- The file’s upload priority
- “Last seen finished” date – that is, when has the file last been posted as available on the network from this installation (from version 0.48a).
  I will go into details with this later on.

An analyzis of "known.met"

When eMule is installed, the file “known.met” will not be created before connection has been made to the network. The first time eMule is shut down, the file will be created. If no material has been downloaded, the file will only contain 5 bytes of data. In HEX the file will look this way:

0E 00 00 00 00

The first byte (offset 0) contains the value 0E (NOTE: in newer versions it can be 0F), which is the file’s signature byte. Offset 1-4 contains information about the number of records in “known.met” and as can be seen above, no files have been downloaded.

If the first 5 bytes in ”known.met” contain the following data:

0E FF 00 00 00

You may deduce from this, that there are 256 entries in all, in this “known.met”, since the decimal value for “FF” is 256.

When examining ”known.met”, you can open it in Notepad, for instance, but the information is not very usable. It is only possible to deduce file name and type.

```
bôG$Ô•E§°ÍsñV(•ˆšäÏ••ýë•¾•‘Æ×°k†¬•ÃŒÒrÂ•ƒëüæ         ÓlÏ¤üÚ¾ò•••••••••%•Madonna
- Hung Up (Album Version).mp3
••••€PÎ
••••PÍ´Y••••T•••••••Q•••••••R•••••••••••••••'•OQ3KVGPW6JPLN2ZFYNCMSB7IIHUWMPJM
•••!•ÿõG •••"
••••••••••148.part•••ÓQ•••••••Ô@•••••••Ò•• Hung Up (Album Version)•••Ñ•Album
Version
```

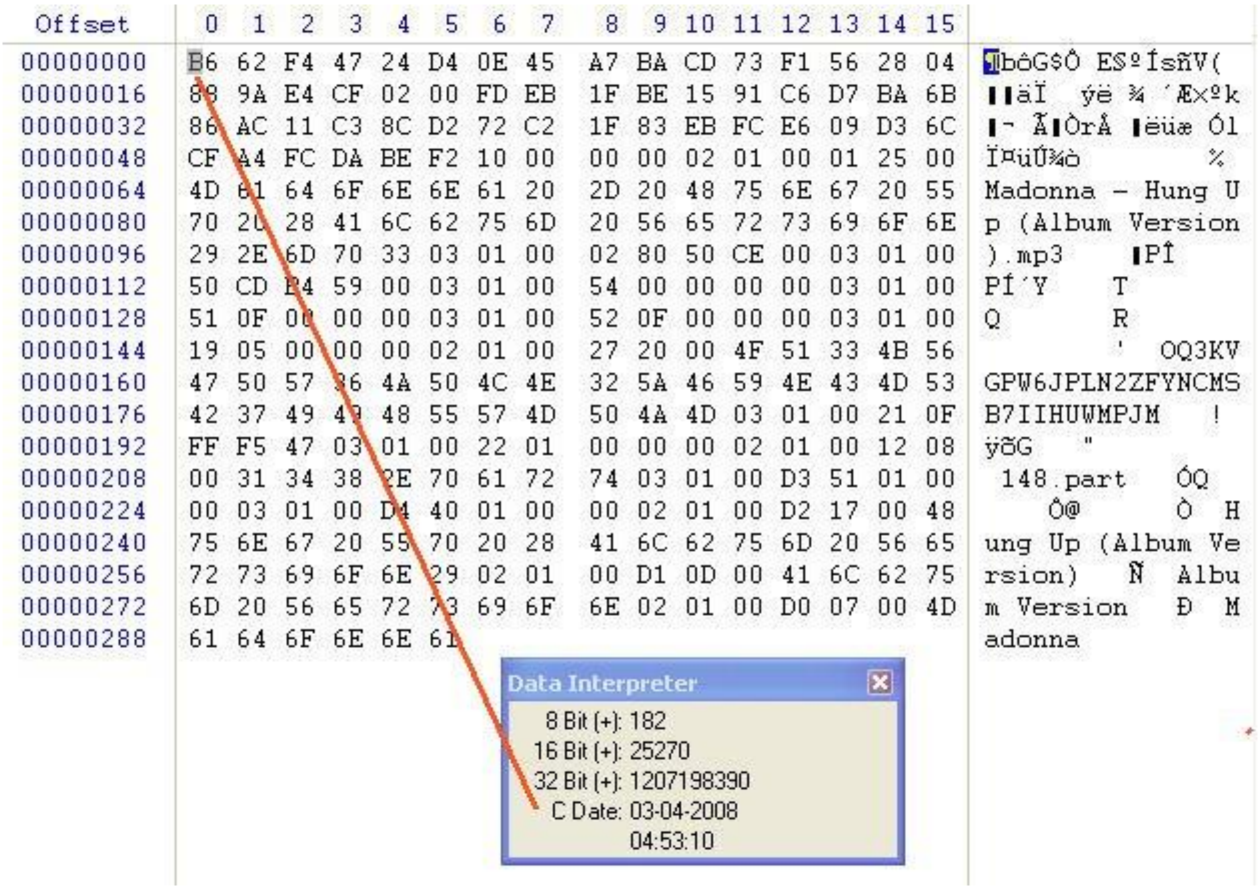
As can be seen, there are many “holes” in the data that can be read in text view.

In order to get more out of the data, you have to change to HEX View. The same posting looks this way:

```
B662F44724D40E45A7BACD73F1562804889AE4CF0200FDEB1FBE1591C6D7BA6B86AC11C38CD272C2
1F83EBFCE609D36CCFA4FCDABEF210000000020100012500 4D61646F6E6E61202D2048756E672055
702028416C62756D2056657273696F6E292E6D70330301000280 50CE0003010050CDB45900030100
540000000003010051 0F0000000301005 20F00000003010019050000000201002720004F51334B56
475057364A504C4E325A46594E434D5342374949485574 4D504A4D030100210FFFF5470301002201
0000000201001208003134382E70617274030100D351010000030100D44001000002 0100D2170048
756E672055702028416C62756D2056657273696F6E29020100D10D00416C62756D2056657273696F
6E020100D007004D61646F6E6E61
```

It is possible to interpret the data with EnCase, but an actual HEX viewer such as WinHEX is much more usable for the analysis. In WinHEX it is possible to interpret data up to 64 bytes onwards and give information, whether there are any possible time and date stamps and so on.

See the example below on the use of WinHEX.



```
Offset     0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15

00000000  B6 62 F4 47 24 D4 0E 45  A7 BA CD 73 F1 56 28 04  ¶bôG$Ô ESºÍsñV(
00000016  88 9A E4 CF 02 00 FD EB  1F BE 15 91 C6 D7 BA 6B  ▮▮äÏ  ýë ¾ ‘Æ×ºk
00000032  86 AC 11 C3 8C D2 72 C2  1F 83 EB FC E6 09 D3 6C  ▮¬ Ã▮ÒrÂ ▮ëüæ Ól
00000048  CF A4 FC DA BE F2 10 00  00 00 02 01 00 01 25 00  Ï¤üÚ¾ò        %
00000064  4D 61 64 6F 6E 6E 61 20  2D 20 48 75 6E 67 20 55  Madonna - Hung U
00000080  70 20 28 41 6C 62 75 6D  20 56 65 72 73 69 6F 6E  p (Album Version
00000096  29 2E 6D 70 33 03 01 00  02 80 50 CE 00 03 01 00  ).mp3    ▮PÎ
00000112  50 CD B4 59 00 03 01 00  54 00 00 00 00 03 01 00  PÍ´Y    T
00000128  51 0F 00 00 00 03 01 00  52 0F 00 00 00 03 01 00  Q       R
00000144  19 05 00 00 00 02 01 00  27 20 00 4F 51 33 4B 56          '  OQ3KV
00000160  47 50 57 36 4A 50 4C 4E  32 5A 46 59 4E 43 4D 53  GPW6JPLN2ZFYNCMS
00000176  42 37 49 49 48 55 57 4D  50 4A 4D 03 01 00 21 0F  B7IIHUWMPJM   !
00000192  FF F5 47 03 01 00 22 01  00 00 00 02 01 00 12 08  ÿõG   "
00000208  00 31 34 38 2E 70 61 72  74 03 01 00 D3 51 01 00   148.part   ÓQ
00000224  00 03 01 00 D4 40 01 00  00 02 01 00 D2 17 00 48      Ô@      Ò  H
00000240  75 6E 67 20 55 70 20 28  41 6C 62 75 6D 20 56 65  ung Up (Album Ve
00000256  72 73 69 6F 6E 29 02 01  00 D1 0D 00 41 6C 62 75  rsion)   Ñ  Albu
00000272  6D 20 56 65 72 73 69 6F  6E 02 01 00 D0 07 00 4D  m Version   Ð  M
00000288  61 64 6F 6E 6E 61                                 adonna
```

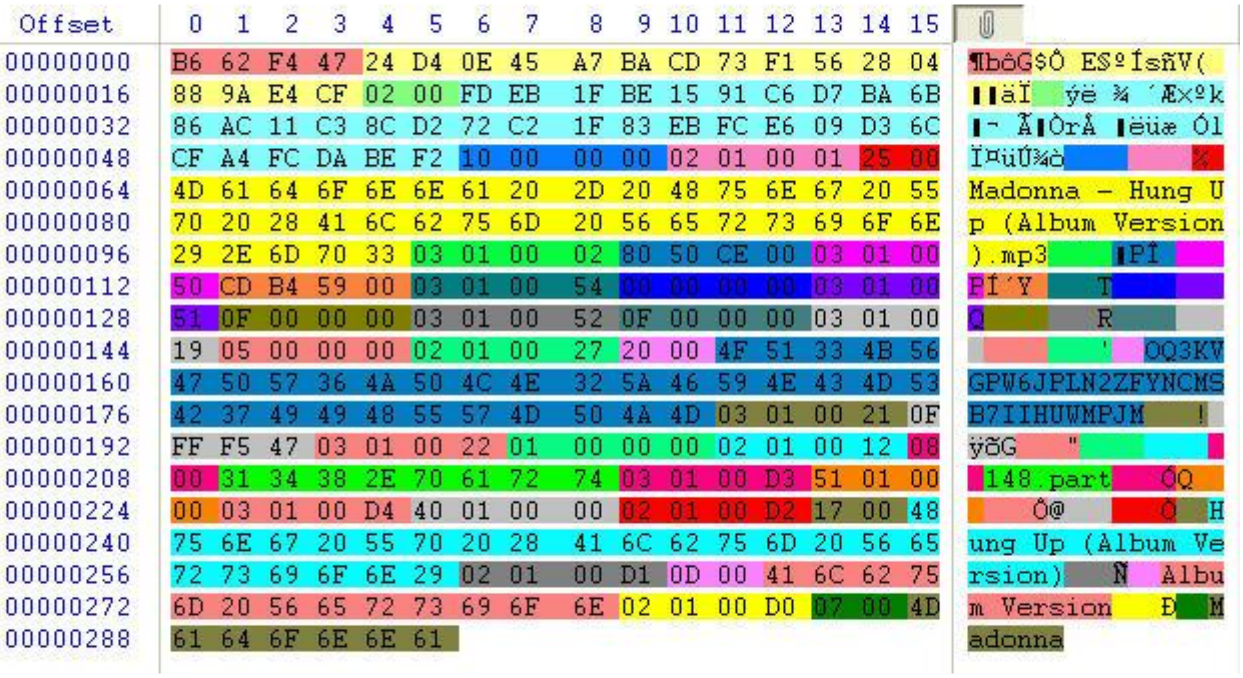
Data Interpreter

8 Bit (+): 182
16 Bit (+): 25270
32 Bit (+): 1207198390
C Date: 03-04-2008
04:53:10

Be aware of that the “Data Interpreter” interprets the data both as numbers and dates – for instance in this case where the 32 bits are interpreted both as numbers and UNIX date. You have to be aware of, that the interpretation is made from the existing data, which means that "false positives" could occur in relation to datings and so on. As a consequence of this, it is important to look at the data structures when analyzing in WinHEX.

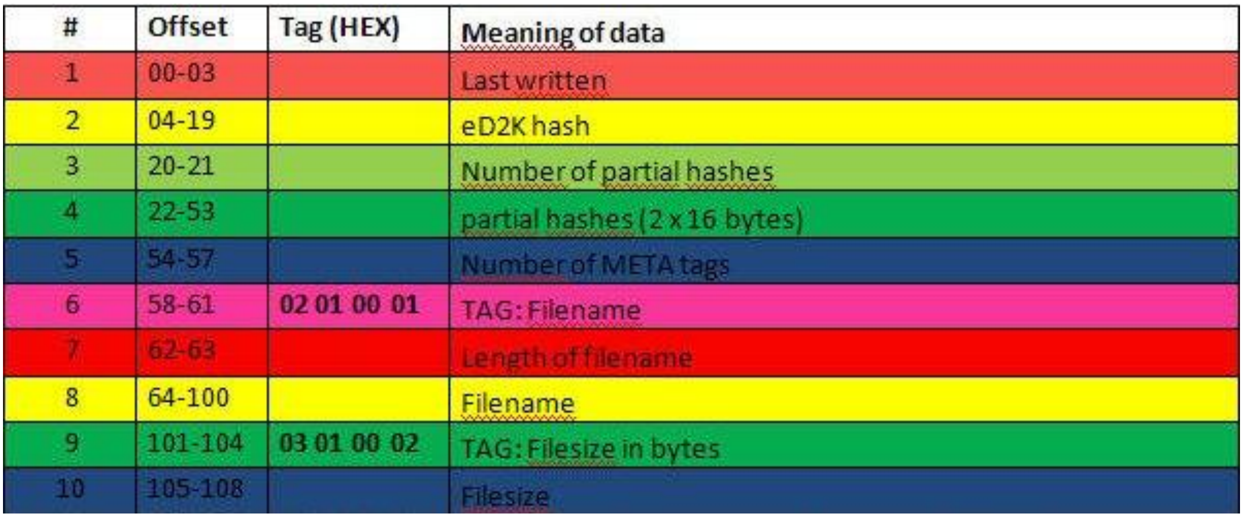
What do the different data mean?

In the example below, the meaning of the different data can be read out:

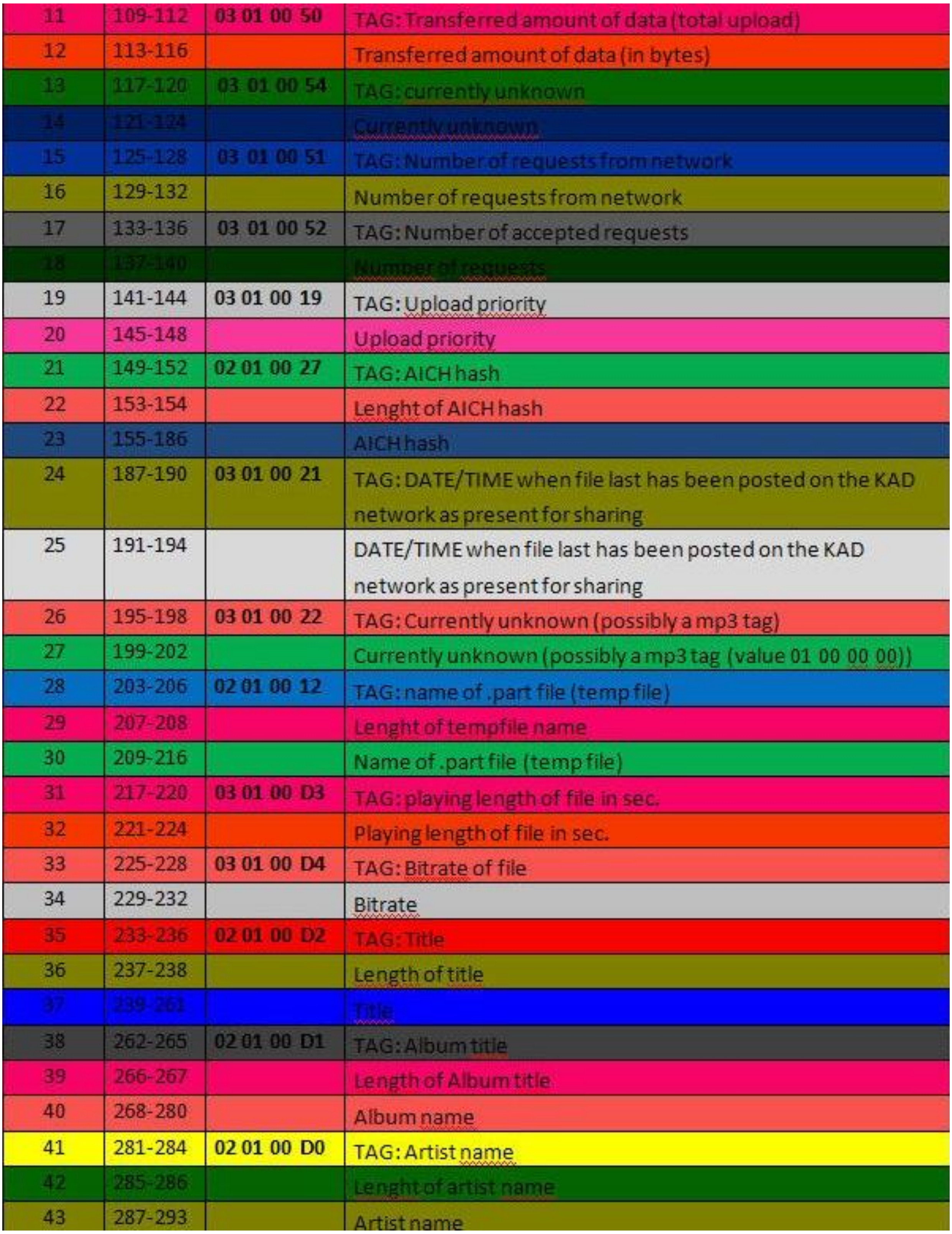


```
Offset     0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
00000000  B6 62 F4 47 24 D4 0E 45  A7 BA CD 73 F1 56 28 04  ¶bôG$Ô ESºÍsñV(
00000016  88 9A E4 CF 02 00 FD EB  1F BE 15 91 C6 D7 BA 6B  ▌▌äÏ  ýë ¾ ´Æ×ºk
00000032  86 AC 11 C3 8C D2 72 C2  1F 83 EB FC E6 09 D3 6C  ▌¬ Ã▌ÒrÅ ▌ëüæ Ól
00000048  CF A4 FC DA BE F2 10 00  00 00 02 01 00 01 25 00  Ï¤üÚ¾ò        %
00000064  4D 61 64 6F 6E 6E 61 20  2D 20 48 75 6E 67 20 55  Madonna - Hung U
00000080  70 20 28 41 6C 62 75 6D  20 56 65 72 73 69 6F 6E  p (Album Version
00000096  29 2E 6D 70 33 03 01 00  02 80 50 CE 00 03 01 00  ).mp3    ▌PÎ
00000112  50 CD B4 59 00 03 01 00  54 00 00 00 00 03 01 00  PÍ´Y    T
00000128  51 0F 00 00 00 03 01 00  52 0F 00 00 00 03 01 00  Q       R
00000144  19 05 00 00 00 02 01 00  27 20 00 4F 51 33 4B 56         '  OQ3KV
00000160  47 50 57 36 4A 50 4C 4E  32 5A 46 59 4E 43 4D 53  GPW6JPLN2ZFYNCMS
00000176  42 37 49 49 48 55 57 4D  50 4A 4D 03 01 00 21 0F  B7IIHUWMPJM   !
00000192  FF F5 47 03 01 00 22 01  00 00 00 02 01 00 12 08  ÿõG   "
00000208  00 31 34 38 2E 70 61 72  74 03 01 00 D3 51 01 00   148.part   ÓQ
00000224  00 03 01 00 D4 40 01 00  00 02 01 00 D2 17 00 48      Ô@     Ò  H
00000240  75 6E 67 20 55 70 20 28  41 6C 62 75 6D 20 56 65  ung Up (Album Ve
00000256  72 73 69 6F 6E 29 02 01  00 D1 0D 00 41 6C 62 75  rsion)   Ñ  Albu
00000272  6D 20 56 65 72 73 69 6F  6E 02 01 00 D0 07 00 4D  m Version    Ð M
00000288  61 64 6F 6E 6E 61                                 adonna
```

Below here, you see the meaning of the individual markings.



#	Offset	Tag (HEX)	Meaning of data
1	00-03		Last written
2	04-19		eD2K hash
3	20-21		Number of partial hashes
4	22-53		partial hashes (2 x 16 bytes)
5	54-57		Number of META tags
6	58-61	02 01 00 01	TAG: Filename
7	62-63		Length of filename
8	64-100		Filename
9	101-104	03 01 00 02	TAG: Filesize in bytes
10	105-108		Filesize



11	109-112	03 01 00 50	TAG: Transferred amount of data (total upload)
12	113-116		Transferred amount of data (in bytes)
13	117-120	03 01 00 54	TAG: currently unknown
14	121-124		Currently unknown
15	125-128	03 01 00 51	TAG: Number of requests from network
16	129-132		Number of requests from network
17	133-136	03 01 00 52	TAG: Number of accepted requests
18	137-140		Number of requests
19	141-144	03 01 00 19	TAG: Upload priority
20	145-148		Upload priority
21	149-152	02 01 00 27	TAG: AICH hash
22	153-154		Lenght of AICH hash
23	155-186		AICH hash
24	187-190	03 01 00 21	TAG: DATE/TIME when file last has been posted on the KAD network as present for sharing
25	191-194		DATE/TIME when file last has been posted on the KAD network as present for sharing
26	195-198	03 01 00 22	TAG: Currently unknown (possibly a mp3 tag)
27	199-202		Currently unknown (possibly a mp3 tag (value 01 00 00 00))
28	203-206	02 01 00 12	TAG: name of .part file (temp file)
29	207-208		Lenght of tempfile name
30	209-216		Name of .part file (temp file)
31	217-220	03 01 00 D3	TAG: playing length of file in sec.
32	221-224		Playing length of file in sec.
33	225-228	03 01 00 D4	TAG: Bitrate of file
34	229-232		Bitrate
35	233-236	02 01 00 D2	TAG: Title
36	237-238		Length of title
37	239-261		Title
38	262-265	02 01 00 D1	TAG: Album title
39	266-267		Length of Album title
40	268-280		Album name
41	281-284	02 01 00 D0	TAG: Artist name
42	285-286		Lenght of artist name
43	287-293		Artist name

Every record may contain a number of different META-tags and all tags are not always represented. Moreover, it has not been possible to interpret all tags completely.

In general, META-tags can be divided into two groups:

- Strings
- Numerical values

Strings:

The META-tag for strings has the format “02 01 00 xx”, in which “xx” represents the ”value” of the tag. Immediately after the tag, the 2 bytes are placed that contain the length of the string.

Numerical values:

The META-tag for numerical values has the format “03 01 00 xx”, in which “xx” represents the ”value” of the tag. The subsequent 4 bytes contain the numerical value or a date/time value (UNIX/C-date).

Examples of different META-tags.

TAG	**Meaning**
02 01 00 01	File name
02 01 00 12	Temp file name (.part)
02 01 00 27	AICH hash *)
02 01 00 D0	Artist name
02 01 00 D1	Album
02 01 00 D2	Title
03 01 00 02	File size
03 01 00 19	Upload priority **)
03 01 00 21	File dating (date/time when file has last been posted on KAD ***)
03 01 00 22	Currently unknown (possibly a mp3 tag)
03 01 00 50	Transferred amount of data (total upload)
03 01 00 D3	Playing length of file in sec.
03 01 00 51	Number of requests from network
03 01 00 52	Number of accepted requests
03 01 00 D4	Bit rate
03 01 00 54	Currently unknown

*) This hash value is an Advanced Intelligent Corruption Handler hash value. It helps you

determine whether parts (“chunks”) of downloaded data are corrupt. Each “chunk” is divided into 53 (52x 180KB and 1x 140KB (9500 KB)) and each of these parts is hashed with SHA1. Each of these hashes is called a “block hash”. By combining a couple of “block hashes” – each part with the part next to it, for instance – eMule gets a complete “tree” of hash values. This “hash tree” of “block hashes” is called the AICH hash set.

**) The upload priority is automatically set to the value ”05” (Auto), but it can be changed by the user. This is done in the window “Shared Files”, wherein each file can be set manually to the desired value.

Upload priority:

00 00 00 00: Low
01 00 00 00: Normal
02 00 00 00: High
03 00 00 00: Release
04 00 00 00: Very Low
05 00 00 00: Auto

***) This time and date stamp is rather special and demands an explanation:

When eMule connects to the network, the programme checks whether the individual file is still in the shared folders. If the file is present, eMule will try to post the file on the KAD network. If the file in question has insufficient sources, the file will be posted and the actual date/time (in GMT) will be updated. On the other hand, if there are insufficient sources on the KAD network, the file will not be posted (in order to prevent flooding). Instead the file is given a time and date stamp (“reposting time”) which is actual time + 5 hours (GMT). When the new time comes, the process will be repeated. If there is a shortage of sources, the file is posted with the actual time (GMT) or else the file will get a new “reposting time”, which again is actual time + 5 hours.

This means that when examining “known.met” it is possible to determine for how long time the individual file has been shared (+/- 5hours) – even if the file has been removed or deleted from the shared folders. You can work out the period in which the file has been shared by deducting the posting time from “last changed” time (Notice that this is ONLY when the file has been downloaded through eMule – more about this later on).

How do we determine whether a file has been downloaded via eMule or the user has placed it at the disposal of the network?

In the file ”C:\Programmer\eMule\config\shareddir.dat” paths are found to the current shared folders (”incoming” and ”Temp” are not mentioned here).

If other folders have been shared, all files in the folders will be added to “known.met”, but the individual files will not have references to a ”.part” file. This means that NO tag exists for this information (02 01 00 12) in this record.

A quick way to check this is to read out the number of records in “known.met” (offset 1-4), and then carry out a search on the HEX values 02 01 00 12 and compare them with the number of records that have been read out earlier. If there is a difference, single files will have been shared by the user (NOTE: If the user chooses to delete the old program before installing a new – or the known.met file has been deleted/corrupted - there will be no referenced to the “.part” file – even if the file had been downloaded by the previous program installation. Do a thorough examination on this prior to saying, that the user has set the files shared by him self)

The content of the”Temp” folder

When examining the folder "C:\Programmer\eMule\Temp", we see that this folder contains the partly downloaded files.

During download, a file is divided into 3 separate files:

- “xx.part” file
- “xx.part.met” file
- “xx.part.met.bak” file

"xx.part" file contains the actual file data. The file has the same size as the complete file (possible missing file parts are being marked with ”00”).

"xx.part.met" contains "meta-data" for the file, such as file name, file size, data chunks downloaded, AICH hash of chunks downloaded and so on.

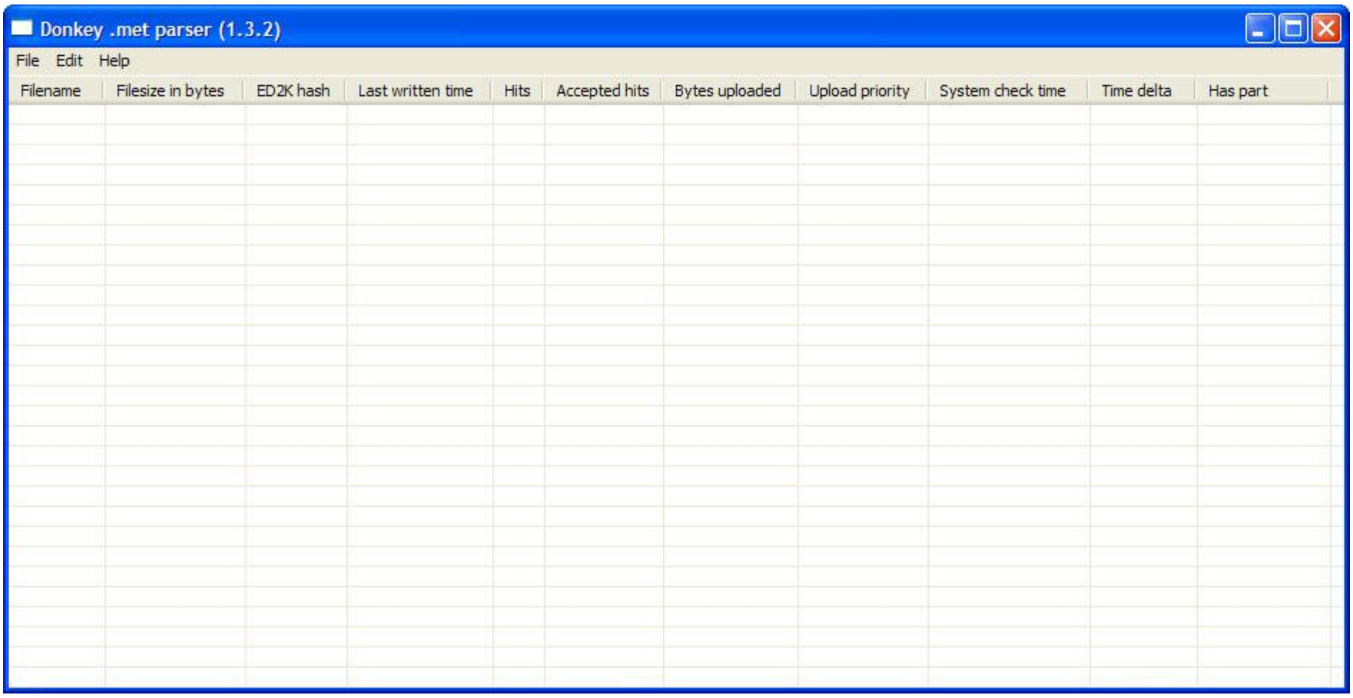
"xx.part.met.bak" is a backup of "xx.part.met".

If a partly downloaded file contains a video sequence, you can often play it in MediaPlayer or in VirtualDub, for instance.

Analysis tool for ”known.met”

Instructions on using ”DonkeyMetParser v. 1.3.3”

The GUI of the the parser:

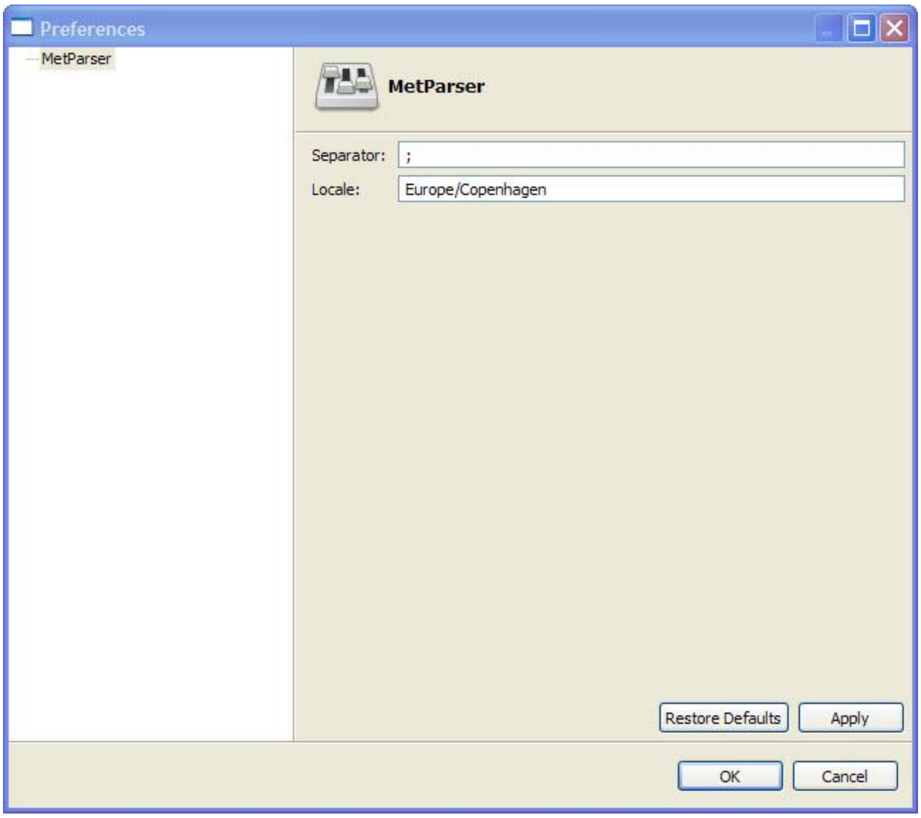


Filename	Filesize in bytes	ED2K hash	Last written time	Hits	Accepted hits	Bytes uploaded	Upload priority	System check time	Time delta	Has part

How to use:

Prior to the first use, you have to update the program with your current timezone:

1. Open <Edit> -> <Preferences>



Separator: ;

Locale: Europe/Copenhagen

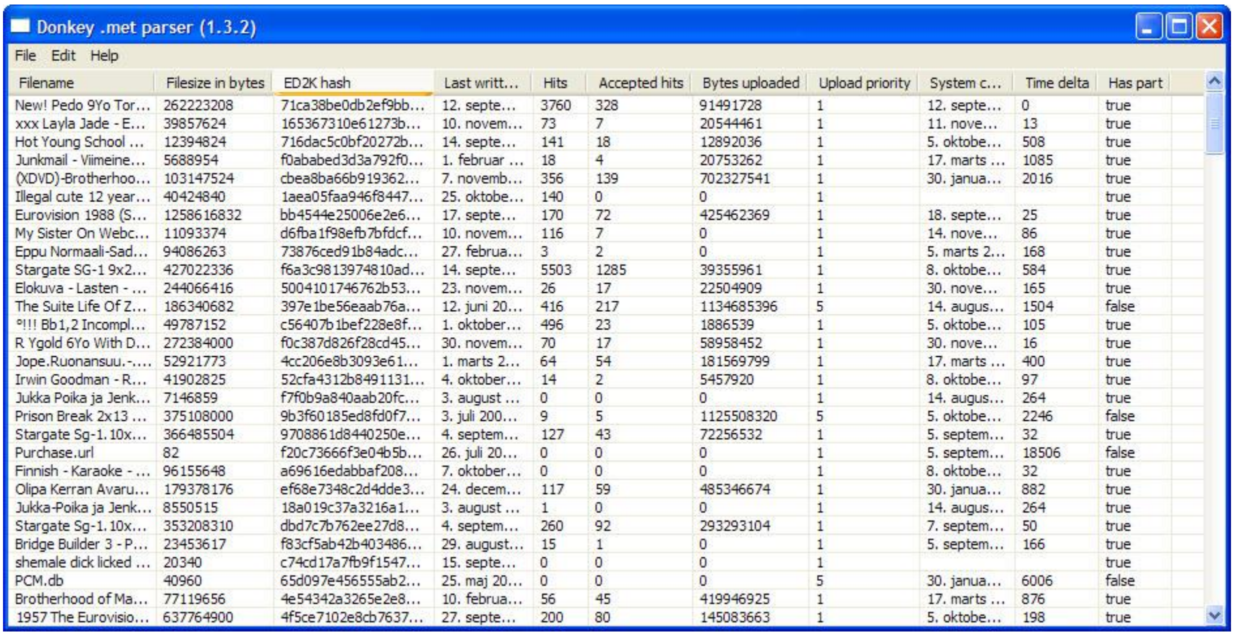
2. Fill in the desired separator for the CSV file (";" is the default separator in Excel (Europe)) - this way you can directly open the file in Excel just by double-clicking it

3. Fill in your locale time zone (find the right time zone table below. By filling in the right zone instead of the GMT offset, you'll have the right change of DST (Daylight saving time))

4. Click Apply

5. Go to <File> -> <Open> to browse to the desired "known.met" file and click "Open"

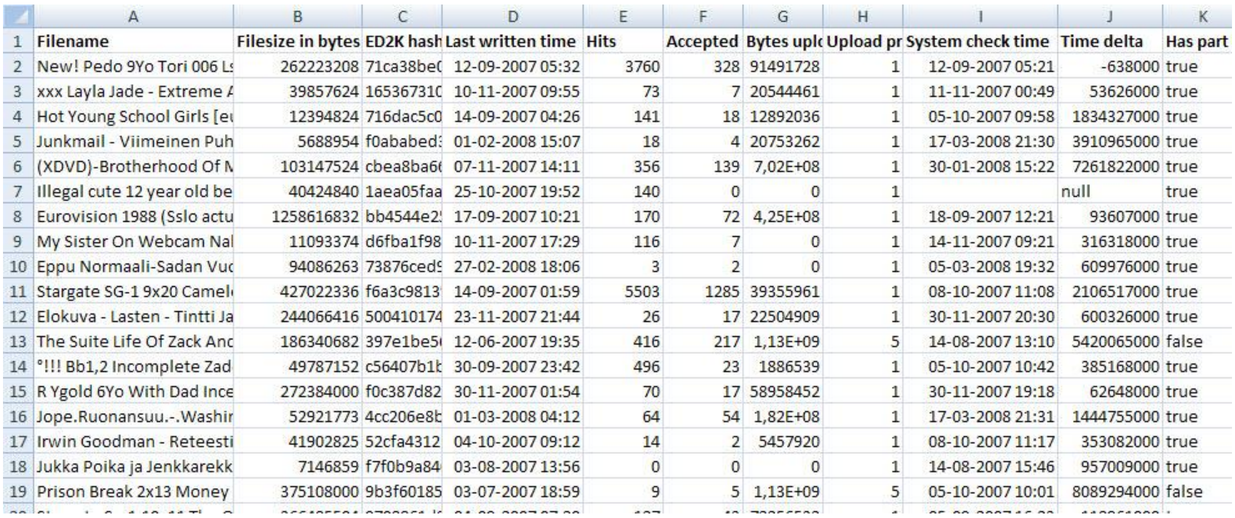
6. The parsed data will be shown in the grid



Filename	Filesize in bytes	ED2K hash	Last writt…	Hits	Accepted hits	Bytes uploaded	Upload priority	System c…	Time delta	Has part
New! Pedo 9Yo Tor…	262223208	71ca38be0db2ef9bb…	12. septe…	3760	328	91491728	1	12. septe…	0	true
xxx Layla Jade - E…	39857624	165367310e61273b…	10. novem…	73	7	20544461	1	11. nove…	13	true
Hot Young School …	12394824	716dac5c0bf20272b…	14. septe…	141	18	12892036	1	5. oktobe…	508	true
Junkmail - Viimeine…	5688954	f0ababed3d3a792f0…	1. februar …	18	4	20753262	1	17. marts …	1085	true
(XDVD)-Brotherhoo…	103147524	cbea8ba66b919362…	7. novemb…	356	139	702327541	1	30. janua…	2016	true
Illegal cute 12 year…	40424840	1aea05faa946f8447…	25. oktobe…	140	0	0	1			true
Eurovision 1988 (S…	1258616832	bb4544e25006e2e6…	17. septe…	170	72	425462369	1	18. septe…	25	true
My Sister On Webc…	11093374	d6fba1f98efb7bfdcf…	10. novem…	116	7	0	1	14. nove…	86	true
Eppu Normaali-Sad…	94086263	73876ced91b84adc…	27. februa…	3	2	0	1	5. marts 2…	168	true
Stargate SG-1 9x2…	427022336	f6a3c9813974810ad…	14. septe…	5503	1285	39355961	1	8. oktobe…	584	true
Elokuva - Lasten - …	244066416	5004101746762b53…	23. novem…	26	17	22504909	1	30. nove…	165	true
The Suite Life Of Z…	186340682	397e1be56eaab76a…	12. juni 20…	416	217	1134685396	5	14. augus…	1504	false
°!!! Bb1,2 Incompl…	49787152	c56407b1bef228e8f…	1. oktober…	496	23	1886539	1	5. oktobe…	105	true
R Ygold 6Yo With D…	272384000	f0c387d826f28cd45…	30. novem…	70	17	58958452	1	30. nove…	16	true
Jope.Ruonansuu.-.…	52921773	4cc206e8b3093e61…	1. marts 2…	64	54	181569799	1	17. marts …	400	true
Irwin Goodman - R…	41902825	52cfa4312b8491131…	4. oktober…	14	2	5457920	1	8. oktobe…	97	true
Jukka Poika ja Jenk…	7146859	f7f0b9a840aab20fc…	3. august …	0	0	0	1	14. augus…	264	true
Prison Break 2x13 …	375108000	9b3f60185ed8fd0f7…	3. juli 200…	9	5	1125508320	5	5. oktobe…	2246	false
Stargate Sg-1.10x…	366485504	970886 1d8440250e…	4. septem…	127	43	72256532	1	5. septem…	32	true
Purchase.url	82	f20c73666f3e04b5b…	26. juli 20…	0	0	0	1	5. septem…	18506	false
Finnish - Karaoke - …	96155648	a69616edabbaf208…	7. oktober…	0	0	0	1	8. oktobe…	32	true
Olipa Kerran Avaru…	179378176	ef68e7348c2d4dde3…	24. decem…	117	59	485346674	1	30. janua…	882	true
Jukka-Poika ja Jenk…	8550515	18a019c37a3216a1…	3. august …	1	0	0	1	14. augus…	264	true
Stargate Sg-1.10x…	353208310	dbd7c7b762ee27d8…	4. septem…	260	92	293293104	1	7. septem…	50	true
Bridge Builder 3 - P…	23453617	f83cf5ab42b403486…	29. august…	15	1	0	1	5. septem…	166	true
shemale dick licked …	20340	c74cd17a7fb9f1547…	15. septe…	0	0	0	1			true
PCM.db	40960	65d097e456555ab2…	25. maj 20…	0	0	0	5	30. janua…	6006	false
Brotherhood of Ma…	77119656	4e54342a3265e2e8…	10. februa…	56	45	419946925	1	17. marts …	876	true
1957 The Eurovisio…	637764900	4f5ce7102e8cb7637…	27. septe…	200	80	145083663	1	5. oktobe…	198	true

7. Choose <File> -> <Export> - Select filename and path, and click "Save"

8. Double click the new CSV file and view the data



	A	B	C	D	E	F	G	H	I	J	K
1	Filename	Filesize in bytes	ED2K hash	Last written time	Hits	Accepted	Bytes uplc	Upload pr	System check time	Time delta	Has part
2	New! Pedo 9Yo Tori 006 Ls	262223208	71ca38be(	12-09-2007 05:32	3760	328	91491728	1	12-09-2007 05:21	-638000	true
3	xxx Layla Jade - Extreme A	39857624	16536731C	10-11-2007 09:55	73	7	20544461	1	11-11-2007 00:49	53626000	true
4	Hot Young School Girls [eu	12394824	716dac5c0	14-09-2007 04:26	141	18	12892036	1	05-10-2007 09:58	1834327000	true
5	Junkmail - Viimeinen Puh	5688954	f0ababed3	01-02-2008 15:07	18	4	20753262	1	17-03-2008 21:30	3910965000	true
6	(XDVD)-Brotherhood Of N	103147524	cbea8ba6(	07-11-2007 14:11	356	139	7,02E+08	1	30-01-2008 15:22	7261822000	true
7	Illegal cute 12 year old be	40424840	1aea05faa	25-10-2007 19:52	140	0	0	1		null	true
8	Eurovision 1988 (Sslo actu	1258616832	bb4544e2!	17-09-2007 10:21	170	72	4,25E+08	1	18-09-2007 12:21	93607000	true
9	My Sister On Webcam Nal	11093374	d6fba1f98	10-11-2007 17:29	116	7	0	1	14-11-2007 09:21	316318000	true
10	Eppu Normaali-Sadan Vuc	94086263	73876ced9	27-02-2008 18:06	3	2	0	1	05-03-2008 19:32	609976000	true
11	Stargate SG-1 9x20 Camel	427022336	f6a3c9813	14-09-2007 01:59	5503	1285	39355961	1	08-10-2007 11:08	2106517000	true
12	Elokuva - Lasten - Tintti Ja	244066416	500410174	23-11-2007 21:44	26	17	22504909	1	30-11-2007 20:30	600326000	true
13	The Suite Life Of Zack Anc	186340682	397e1be5(	12-06-2007 19:35	416	217	1,13E+09	5	14-08-2007 13:10	5420065000	false
14	°!!! Bb1,2 Incomplete Zad	49787152	c56407b1b	30-09-2007 23:42	496	23	1886539	1	05-10-2007 10:42	385168000	true
15	R Ygold 6Yo With Dad Ince	272384000	f0c387d82	30-11-2007 01:54	70	17	58958452	1	30-11-2007 19:18	62648000	true
16	Jope.Ruonansuu.-.Washir	52921773	4cc206e8b	01-03-2008 04:12	64	54	1,82E+08	1	17-03-2008 21:31	1444755000	true
17	Irwin Goodman - Reteesti	41902825	52cfa4312	04-10-2007 09:12	14	2	5457920	1	08-10-2007 11:17	353082000	true
18	Jukka Poika ja Jenkkarekk	7146859	f7f0b9a84	03-08-2007 13:56	0	0	0	1	14-08-2007 15:46	957009000	true
19	Prison Break 2x13 Money	375108000	9b3f60185	03-07-2007 18:59	9	5	1,13E+09	5	05-10-2007 10:01	8089294000	false

Please notice that the parser shows the "TimeDelta" in minutes - while Excell shows the same time in seconds (this due to an internal calculation mode within Excell)

Explanation to the different fields

Fieldname	Meaning	Notes
Filename	The name of the file, that the user has clicked on when searching	
File size in bytes	Size of file in bytes	
eD2K Hash value	The eDonkey hash value of the file	For files smaller than 9500 bytes, this value is the same as the MD4 hash value of the file
Last Written	The time when the file was fully downloaded	If the file has been shared "manually" by the user, will this time/date be the original "Last Written" timestamp - see further under the "Has Part" part later on
Hits	The number of hits on the file from the eD2K/KAD network	
Accepted hits	Number of accepted hits, where the eDonkey client "grants" access to download data from the desired file	
Bytes uploadet	The accumulated (total) upload from this specific file	
Upload priority	The upload priority of the file (05 - Auto is default)	00 00 00 00: Low 01 00 00 00: Normal 02 00 00 00: High 03 00 00 00: Release 04 00 00 00: Very Low 05 00 00 00: Auto

		If the Upload priority has been changed from Auto, it shows, that the user has done this manually to the file (in the "Shared files" pane he has selected the file, right-clicked it and changed the priority)
SystemCheckTime	When eMule connects to the network, the program checks whether the individual file is still in the shared folders. If the file is present, eMule will try to post the file on the KAD network. If the file in question has insufficient sources, the file will be posted and the actual date/time (in GMT) will be updated. On the other hand, if there are insufficient sources on the KAD network, the file will not be posted (in order to prevent flooding). Instead the file is given a time and date stamp (“reposting time”) which is actual time + 5 hours (GMT). When the new time comes, the process will be repeated. If there is a shortage of sources, the file is posted with the actual time (GMT) or else the file will get a new “reposting time”, which again is actual time + 5 hours. This means that when examining “known.met” it is possible to determine for how long time the individual file has been shared (+/- 5 hours) – even if the file has been removed or deleted from the shared folders.	
TimeDelta	The amount of time, that the file has been shared	When transferring the data from the parser to the CSV file, and opening it, the shown amount of time will change from minutes to seconds. In rare cases you will get a negative amount of time - see note further down

Has Part	When a file is downloaded through eMule, the entry in "known.met" will contain a reference to the temporary ".part" file. If this entry not is present, the file has not been downloaded through eMule (at least not the present installation)	True/false indicates whether there is a reference to the ".part" file

Ocurrence of "negative TimeDelta"

In rare cases occurrences of negative values will appear, when parsing af "known.met" file. This happens when a larger file is being downloaded. When sufficient data is available ("chunks") they are shared on the network in the same way as full downloaded files. The available "chunks" gets a "SystemCheckTime" stamp, while the "LastWritten" timestamp NOT is present in the "known.met" file until the full file has been downloaded.

Scenario:

The user selects a 500 Mb file for download at 13:00 GMT present day. During the download he obtains several full "data chunks" that are set as shared. Every time the file gets a "SystemCheckTime" timestamp. At 15:30 GMT present day the file gets the last "SystemCheckTime", and at 16:00 GMT the file is fully downloaded. The entry in the "known.met" file is created with "Last Written" as 16:00 GMT present day. The user removes the file from the shared folder before next "SystemCheckTime" is stamped into the file.

When parsing this file the "TimeDelta" will be negative as it is calculated as a subtraction of the "LastWritten" from "SystemCheckTime".

Even if you have a negative "TimeDelta" you can have a large amount of hits, accepted hits and upload of data

Finding data of interest in unallocated clusters

When you are making an examination - try to use the following GREP search (EnCase version)

```
\x03\x01\x00\x51.{4,4}\x03\x01\x00\x52
```

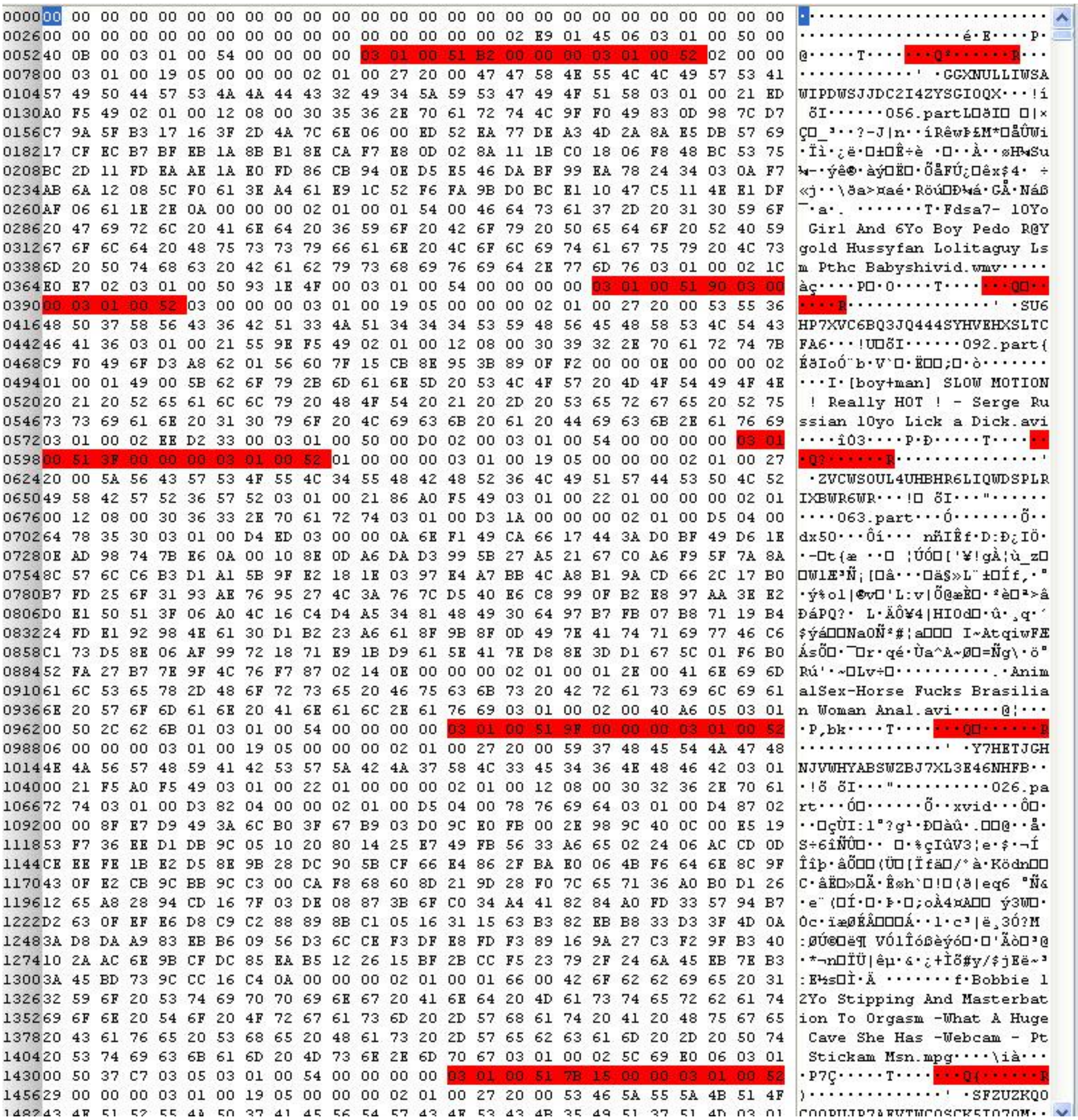
This GREP searches for parts of the entries in "known.met"

This search is specifically searching for the "Number of hits from the network" (the tag 03010051) - then followed by the actual number of hits - which is stated in the next 4 bytes (unknown data) and then followed by the "Number of accepted hits" (the tag 03010052)

When you have finished this search, you might get a lot of hits (as each entry in the known.met file has these tags).

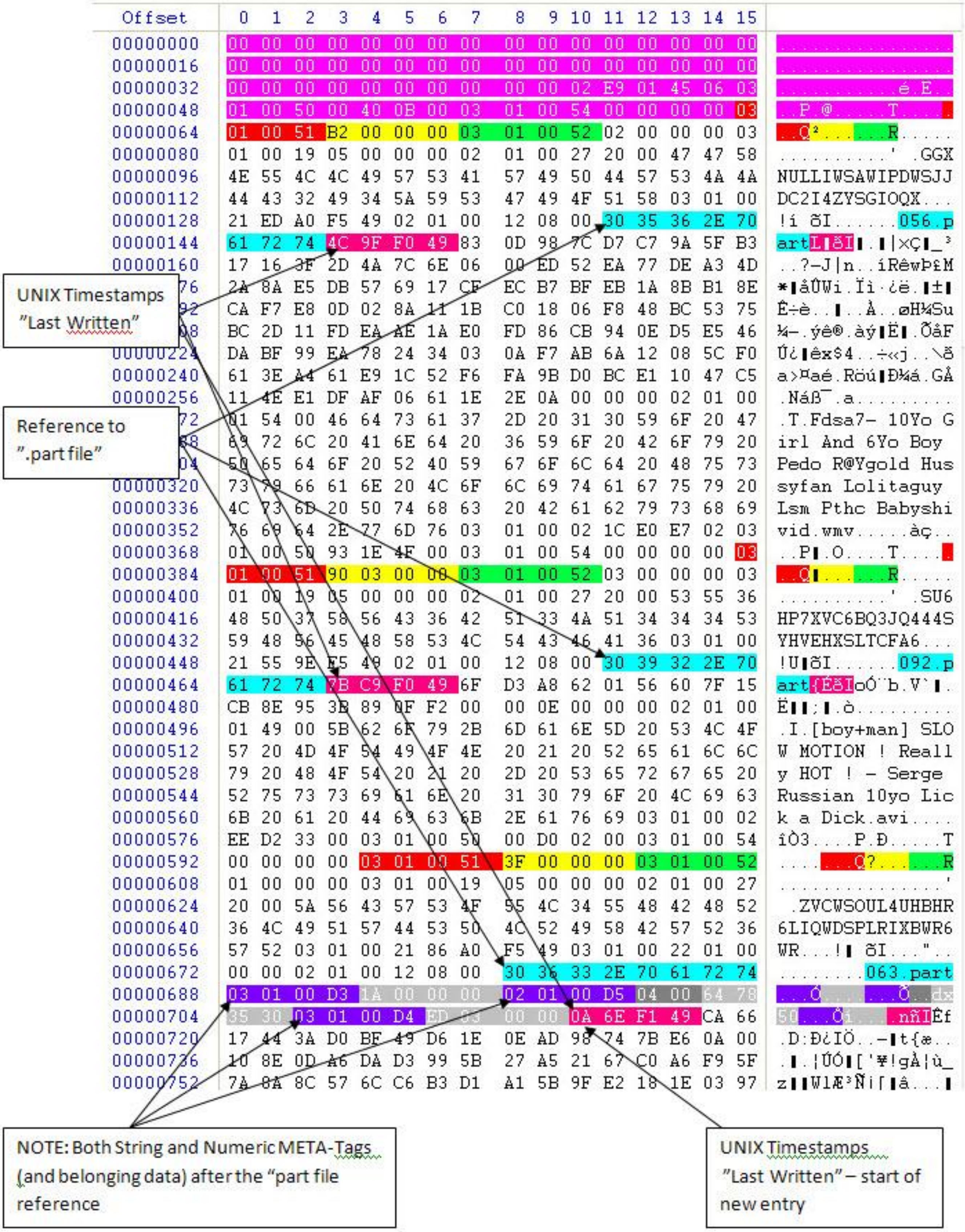
How to analyze data found in unallocated clusters

Using EnCase you might get searchhits like below when using the GREP search shown above:



```
000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ··························
002600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 E9 01 45 06 03 01 00 50 00  ················é·E····P·
005240 0B 00 03 01 00 54 00 00 00 00 03 01 00 51 B2 00 00 00 03 01 00 52 02 00 00  @·····T······Q²······R···
007800 03 01 00 19 05 00 00 00 02 01 00 27 20 00 47 47 58 4E 55 4C 4C 49 57 53 41  ·············' ·GGXNULLIWSA
010457 49 50 44 57 53 4A 4A 44 43 32 49 34 5A 59 53 47 49 4F 51 58 03 01 00 21 ED  WIPDWSJJDC2I4ZYSGIOQX···!í
0130A0 F5 49 02 01 00 12 08 00 30 35 36 2E 70 61 72 74 4C 9F F0 49 83 0D 98 7C D7   õI······056.partL□ðI□ □|×
0156C7 9A 5F B3 17 16 3F 2D 4A 7C 6E 06 00 ED 52 EA 77 DE A3 4D 2A 8A E5 DB 57 69  Ç□_³··?-J|n··íRêwÞ£M*□åÛWi
018217 CF EC B7 BF EB 1A 8B B1 8E CA F7 E8 0D 02 8A 11 1B C0 18 06 F8 48 BC 53 75  ·Ïì·¿ë·□±□Ê÷è ·□··À··øH¼Su
0208BC 2D 11 FD EA AE 1A E0 FD 86 CB 94 0E D5 E5 46 DA BF 99 EA 78 24 34 03 0A F7  ¼-·ýê®·àý□Ë□·ÕåFÚ¿□êx$4· ÷
0234AB 6A 12 08 5C F0 61 3E A4 61 E9 1C 52 F6 FA 9B D0 BC E1 10 47 C5 11 4E E1 DF  «j··\ða>¤aé·Röú□Ð¼á·GÅ·Náß
0260AF 06 61 1E 2E 0A 00 00 00 02 01 00 01 54 00 46 64 73 61 37 2D 20 31 30 59 6F  ¯·a·. ·······T·Fdsa7- 10Yo
028620 47 69 72 6C 20 41 6E 64 20 36 59 6F 20 42 6F 79 20 50 65 64 6F 20 52 40 59   Girl And 6Yo Boy Pedo R@Y
031267 6F 6C 64 20 48 75 73 73 79 66 61 6E 20 4C 6F 6C 69 74 61 67 75 79 20 4C 73  gold Hussyfan Lolitaguy Ls
03386D 20 50 74 68 63 20 42 61 62 79 73 68 69 76 69 64 2E 77 6D 76 03 01 00 02 1C  m Pthc Babyshivid.wmv·····
0364E0 E7 02 03 01 00 50 93 1E 4F 00 03 01 00 54 00 00 00 00 03 01 00 51 90 03 00  àç····P□·O····T······Q□··
039000 03 01 00 52 03 00 00 00 03 01 00 19 05 00 00 00 02 01 00 27 20 00 53 55 36  ····R···············' ·SU6
041648 50 37 58 56 43 36 42 51 33 4A 51 34 34 34 53 59 48 56 45 48 58 53 4C 54 43  HP7XVC6BQ3JQ444SYHVEHXSLTC
044246 41 36 03 01 00 21 55 9E F5 49 02 01 00 12 08 00 30 39 32 2E 70 61 72 74 7B  FA6···!U□õI······092.part{
0468C9 F0 49 6F D3 A8 62 01 56 60 7F 15 CB 8E 95 3B 89 0F F2 00 00 0E 00 00 00 02  ÉðIoÓ¨b·V`□·Ë□□;□·ò·······
049401 00 01 49 00 5B 62 6F 79 2B 6D 61 6E 5D 20 53 4C 4F 57 20 4D 4F 54 49 4F 4E  ···I·[boy+man] SLOW MOTION
052020 21 20 52 65 61 6C 6C 79 20 48 4F 54 20 21 20 2D 20 53 65 72 67 65 20 52 75   ! Really HOT ! - Serge Ru
054673 73 69 61 6E 20 31 30 79 6F 20 4C 69 63 6B 20 61 20 44 69 63 6B 2E 61 76 69  ssian 10yo Lick a Dick.avi
057203 01 00 02 EE D2 33 00 03 01 00 50 00 D0 02 00 03 01 00 54 00 00 00 00 03 01  ····îÒ3····P·Ð·····T······
059800 51 3F 00 00 00 03 01 00 52 01 00 00 00 03 01 00 19 05 00 00 00 02 01 00 27  ·Q?······R···············'
062420 00 5A 56 43 57 53 4F 55 4C 34 55 48 42 48 52 36 4C 49 51 57 44 53 50 4C 52   ·ZVCWSOUL4UHBHR6LIQWDSPLR
065049 58 42 57 52 36 57 52 03 01 00 21 86 A0 F5 49 03 01 00 22 01 00 00 00 02 01  IXBWR6WR···!□ õI···"······
067600 12 08 00 30 36 33 2E 70 61 72 74 03 01 00 D3 1A 00 00 00 02 01 00 D5 04 00  ····063.part···Ó·······Õ··
070264 78 35 30 03 01 00 D4 ED 03 00 00 0A 6E F1 49 CA 66 17 44 3A D0 BF 49 D6 1E  dx50···Ôí··· nñIÊf·D:Ð¿IÖ·
07280E AD 98 74 7B E6 0A 00 10 8E 0D A6 DA D3 99 5B 27 A5 21 67 C0 A6 F9 5F 7A 8A  ·-□t{æ ··□ ¦ÚÓ□['¥!gÀ¦ù_z□
07548C 57 6C C6 B3 D1 A1 5B 9F E2 18 1E 03 97 E4 A7 BB 4C A8 B1 9A CD 66 2C 17 B0  □WlÆ³Ñ¡[□â···□ä§»L¨±□Íf,·°
0780B7 FD 25 6F 31 93 AE 76 95 27 4C 3A 76 7C D5 40 E6 C8 99 0F B2 E8 97 AA 3E E2  ·ý%o1|®v□'L:v|Õ@æÈ□·²è□ª>â
0806D0 E1 50 51 3F 06 A0 4C 16 C4 D4 A5 34 81 48 49 30 64 97 B7 FB 07 B8 71 19 B4  ÐáPQ?· L·ÄÔ¥4|HI0d□·û·¸q·´
083224 FD E1 92 98 4E 61 30 D1 B2 23 A6 61 8F 9B 8F 0D 49 7E 41 74 71 69 77 46 C6  $ýá□□Na0Ñ²#¦a□□□ I~AtqiwFÆ
0858C1 73 D5 8E 06 AF 99 72 18 71 E9 1B D9 61 5E 41 7E D8 8E 3D D1 67 5C 01 F6 B0  ÁsÕ□·¯□r·qé·Ùa^A~Ø□=Ñg\·ö°
088452 FA 27 B7 7E 9F 4C 76 F7 87 02 14 0E 00 00 00 02 01 00 01 2E 00 41 6E 69 6D  Rú'·~□Lv÷□··········.·Anim
091061 6C 53 65 78 2D 48 6F 72 73 65 20 46 75 63 6B 73 20 42 72 61 73 69 6C 69 61  alSex-Horse Fucks Brasilia
09366E 20 57 6F 6D 61 6E 20 41 6E 61 6C 2E 61 76 69 03 01 00 02 00 40 A6 05 03 01  n Woman Anal.avi·····@¦···
096200 50 2C 62 6B 01 03 01 00 54 00 00 00 00 03 01 00 51 9F 00 00 00 03 01 00 52  ·P,bk····T······Q□······R
098806 00 00 00 03 01 00 19 05 00 00 00 02 01 00 27 20 00 59 37 48 45 54 4A 47 48  ···············' ·Y7HETJGH
10144E 4A 56 57 48 59 41 42 53 57 5A 42 4A 37 58 4C 33 45 34 36 4E 48 46 42 03 01  NJVWHYABSWZBJ7XL3E46NHFB··
104000 21 F5 A0 F5 49 03 01 00 22 01 00 00 00 02 01 00 12 08 00 30 32 36 2E 70 61  ·!õ õI···"··········026.pa
106672 74 03 01 00 D3 82 04 00 00 02 01 00 D5 04 00 78 76 69 64 03 01 00 D4 87 02  rt···Ó□······Õ··xvid···Ô□·
109200 00 8F E7 D9 49 3A 6C B0 3F 67 B9 03 D0 9C E0 FB 00 2E 98 9C 40 0C 00 E5 19  ··□çÙI:l°?g¹·Ð□àû·.□□@··å·
111853 F7 36 EE D1 DB 9C 05 10 20 80 14 25 E7 49 FB 56 33 A6 65 02 24 06 AC CD 0D  S÷6îÑÛ□·· □·%çIûV3¦e·$·¬Í
1144CE EE FE 1B E2 D5 8E 9B 28 DC 90 5B CF 66 E4 86 2F BA E0 06 4B F6 64 6E 8C 9F  Îîþ·âÕ□□(Ü□[Ïfä□/º à·Ködn□□
117043 0F E2 CB 9C BB 9C C3 00 CA F8 68 60 8D 21 9D 28 F0 7C 65 71 36 A0 B0 D1 26  C·âË□»□Ã·Êøh`□!□(ð|eq6 °Ñ&
119612 65 A8 28 94 CD 16 7F 03 DE 08 87 3B 6F C0 34 A4 41 82 84 A0 FD 33 57 94 B7  ·e¨(□Í·□·Þ·□;oÀ4¤A□□ ý3W□·
1222D2 63 0F EF E6 D8 C9 C2 88 89 8B C1 05 16 31 15 63 B3 82 EB B8 33 D3 3F 4D 0A  Òc·ïæØÉÂ□□□Á··1·c³|ë¸3Ó?M
12483A D8 DA A9 83 EB B6 09 56 D3 6C CE F3 DF E8 FD F3 89 16 9A 27 C3 F2 9F B3 40  :ØÚ©□ë¶ VÓlÎóßèýó□·□'Ãò□³@
127410 2A AC 6E 9B CF DC 85 EA B5 12 26 15 BF 2B CC F5 23 79 2F 24 6A 45 EB 7E B3  ·*¬n□ÏÜ|êµ·&·¿+Ìõ#y/$jEë~³
13003A 45 BD 73 9C CC 16 C4 0A 00 00 00 02 01 00 01 66 00 42 6F 62 62 69 65 20 31  :E½s□Ì·Ä ·······f·Bobbie 1
132632 59 6F 20 53 74 69 70 70 69 6E 67 20 41 6E 64 20 4D 61 73 74 65 72 62 61 74  2Yo Stipping And Masterbat
135269 6F 6E 20 54 6F 20 4F 72 67 61 73 6D 20 2D 57 68 61 74 20 41 20 48 75 67 65  ion To Orgasm -What A Huge
137820 43 61 76 65 20 53 68 65 20 48 61 73 20 2D 57 65 62 63 61 6D 20 2D 20 50 74   Cave She Has -Webcam - Pt
140420 53 74 69 63 6B 61 6D 20 4D 73 6E 2E 6D 70 67 03 01 00 02 5C 69 E0 06 03 01   Stickam Msn.mpg····\ià···
143000 50 37 C7 03 05 03 01 00 54 00 00 00 00 03 01 00 51 7B 15 00 00 03 01 00 52  ·P7Ç·····T······Q{······R
145629 00 00 00 03 01 00 19 05 00 00 00 02 01 00 27 20 00 53 46 5A 55 5A 4B 51 4F  )···············' ·SFZUZKQO
148243 4F 51 52 55 4A 50 37 41 45 56 54 57 43 4F 53 43 4B 35 49 51 37 51 4D 03 01  COQRUJP7AEVTWCOSCK5IQ7QM··
```

Same data shown in WinHEX - the GREP search is here shown in red/yellow/green



```
Offset     0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
00000000  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000016  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000032  00 00 00 00 00 00 00 00  00 00 02 E9 01 45 06 03  ............é.E.
00000048  01 00 50 00 40 0B 00 03  01 00 54 00 00 00 00 03  ..P.@.....T.....
00000064  01 00 51 B2 00 00 00 03  01 00 52 02 00 00 00 03  ..Q².......R....
00000080  01 00 19 05 00 00 00 02  01 00 27 20 00 47 47 58  ..........' .GGX
00000096  4E 55 4C 4C 49 57 53 41  57 49 50 44 57 53 4A 4A  NULLIWSAWIPDWSJJ
00000112  44 43 32 49 34 5A 59 53  47 49 4F 51 58 03 01 00  DC2I4ZYSGIOQX...
00000128  21 ED A0 F5 49 02 01 00  12 08 00 30 35 36 2E 70  !í õI......056.p
00000144  61 72 74 4C 9F F0 49 83  0D 98 7C D7 C7 9A 5F B3  artL▮ðI▮.▮|×Ç▮_³
00000160  17 16 3F 2D 4A 7C 6E 06  00 ED 52 EA 77 DE A3 4D  ..?-J|n..íRêwÞ£M
      76  2A 8A E5 DB 57 69 17 CF  EC B7 BF EB 1A 8B B1 8E  *▮åÛWi.Ïì·¿ë.▮±▮
      92  CA F7 E8 0D 02 8A 11 1B  C0 18 06 F8 48 BC 53 75  Ê÷è..▮..À..øH¼Su
      08  BC 2D 11 FD EA AE 1A E0  FD 86 CB 94 0E D5 E5 46  ¼-.ýê®.àý▮Ë▮.ÕåF
00000224  DA BF 99 EA 78 24 34 03  0A F7 AB 6A 12 08 5C F0  Ú¿▮êx$4..÷«j..\ð
00000240  61 3E A4 61 E9 1C 52 F6  FA 9B D0 BC E1 10 47 C5  a>¤aé.Röú▮Ð¼á.GÅ
00000256  11 4E E1 DF AF 06 61 1E  2E 0A 00 00 00 02 01 00  .Náß¯.a.........
      72  01 54 00 46 64 73 61 37  2D 20 31 30 59 6F 20 47  .T.Fdsa7- 10Yo G
      88  69 72 6C 20 41 6E 64 20  36 59 6F 20 42 6F 79 20  irl And 6Yo Boy 
      04  50 65 64 6F 20 52 40 59  67 6F 6C 64 20 48 75 73  Pedo R@Ygold Hus
00000320  73 79 66 61 6E 20 4C 6F  6C 69 74 61 67 75 79 20  syfan Lolitaguy 
00000336  4C 73 6D 20 50 74 68 63  20 42 61 62 79 73 68 69  Lsm Pthc Babyshi
00000352  76 69 64 2E 77 6D 76 03  01 00 02 1C E0 E7 02 03  vid.wmv.....àç..
00000368  01 00 50 93 1E 4F 00 03  01 00 54 00 00 00 00 03  ..P▮.O....T.....
00000384  01 00 51 90 03 00 00 03  01 00 52 03 00 00 00 03  ..Q▮.......R....
00000400  01 00 19 05 00 00 00 02  01 00 27 20 00 53 55 36  ..........' .SU6
00000416  48 50 37 58 56 43 36 42  51 33 4A 51 34 34 34 53  HP7XVC6BQ3JQ444S
00000432  59 48 56 45 48 58 53 4C  54 43 46 41 36 03 01 00  YHVEHXSLTCFA6...
00000448  21 55 9E F5 49 02 01 00  12 08 00 30 39 32 2E 70  !U▮õI......092.p
00000464  61 72 74 7B C9 F0 49 6F  D3 A8 62 01 56 60 7F 15  art{ÉðIoÓ¨b.V`▮.
00000480  CB 8E 95 3B 89 0F F2 00  00 0E 00 00 00 02 01 00  Ë▮▮;▮.ò.........
00000496  01 49 00 5B 62 6F 79 2B  6D 61 6E 5D 20 53 4C 4F  .I.[boy+man] SLO
00000512  57 20 4D 4F 54 49 4F 4E  20 21 20 52 65 61 6C 6C  W MOTION ! Reall
00000528  79 20 48 4F 54 20 21 20  2D 20 53 65 72 67 65 20  y HOT ! - Serge 
00000544  52 75 73 73 69 61 6E 20  31 30 79 6F 20 4C 69 63  Russian 10yo Lic
00000560  6B 20 61 20 44 69 63 6B  2E 61 76 69 03 01 00 02  k a Dick.avi....
00000576  EE D2 33 00 03 01 00 50  00 D0 02 00 03 01 00 54  îÒ3....P.Ð.....T
00000592  00 00 00 00 03 01 00 51  3F 00 00 00 03 01 00 52  .......Q?......R
00000608  01 00 00 00 03 01 00 19  05 00 00 00 02 01 00 27  ...............'
00000624  20 00 5A 56 43 57 53 4F  55 4C 34 55 48 42 48 52   .ZVCWSOUL4UHBHR
00000640  36 4C 49 51 57 44 53 50  4C 52 49 58 42 57 52 36  6LIQWDSPLRIXBWR6
00000656  57 52 03 01 00 21 86 A0  F5 49 03 01 00 22 01 00  WR...!▮ õI..."..
00000672  00 00 02 01 00 12 08 00  30 36 33 2E 70 61 72 74  ........063.part
00000688  03 01 00 D3 1A 00 00 00  02 01 00 D5 04 00 64 78  ...Ó.......Õ..dx
00000704  35 30 03 01 00 D4 ED 03  00 00 0A 6E F1 49 CA 66  50...Ôí....nñIÊf
00000720  17 44 3A D0 BF 49 D6 1E  0E AD 98 74 7B E6 0A 00  .D:Ð¿IÖ..-▮t{æ..
00000736  10 8E 0D A6 DA D3 99 5B  27 A5 21 67 C0 A6 F9 5F  .▮.¦ÚÓ▮['¥!gÀ¦ù_
00000752  7A 8A 8C 57 6C C6 B3 D1  A1 5B 9F E2 18 1E 03 97  z▮▮WlÆ³Ñ¡[▮â...▮
```

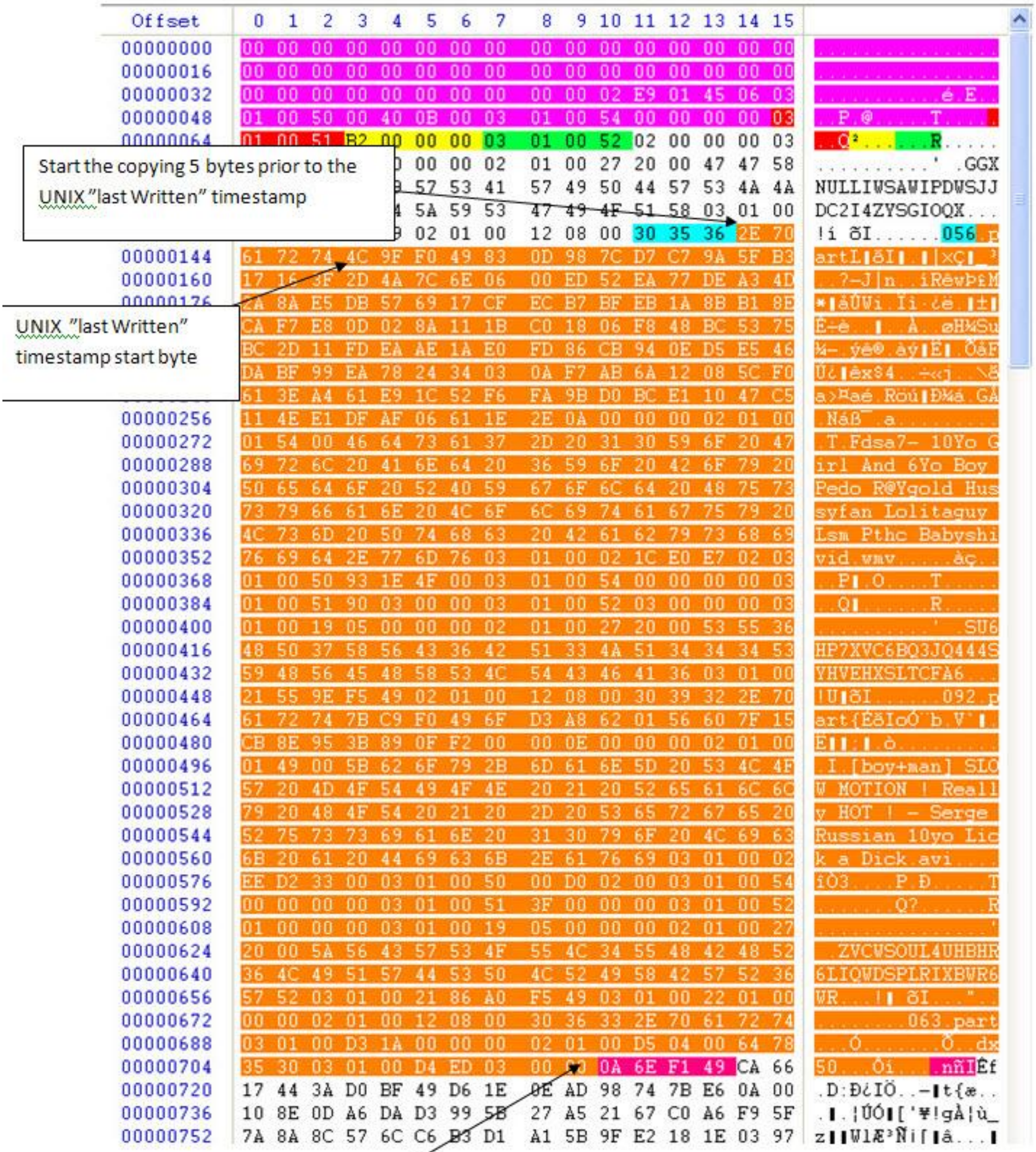
UNIX Timestamps ”Last Written”

Reference to ”.part file”

NOTE: Both String and Numeric META-Tags (and belonging data) after the “part file reference

UNIX Timestamps ”Last Written” – start of new entry

Which data to copy out?



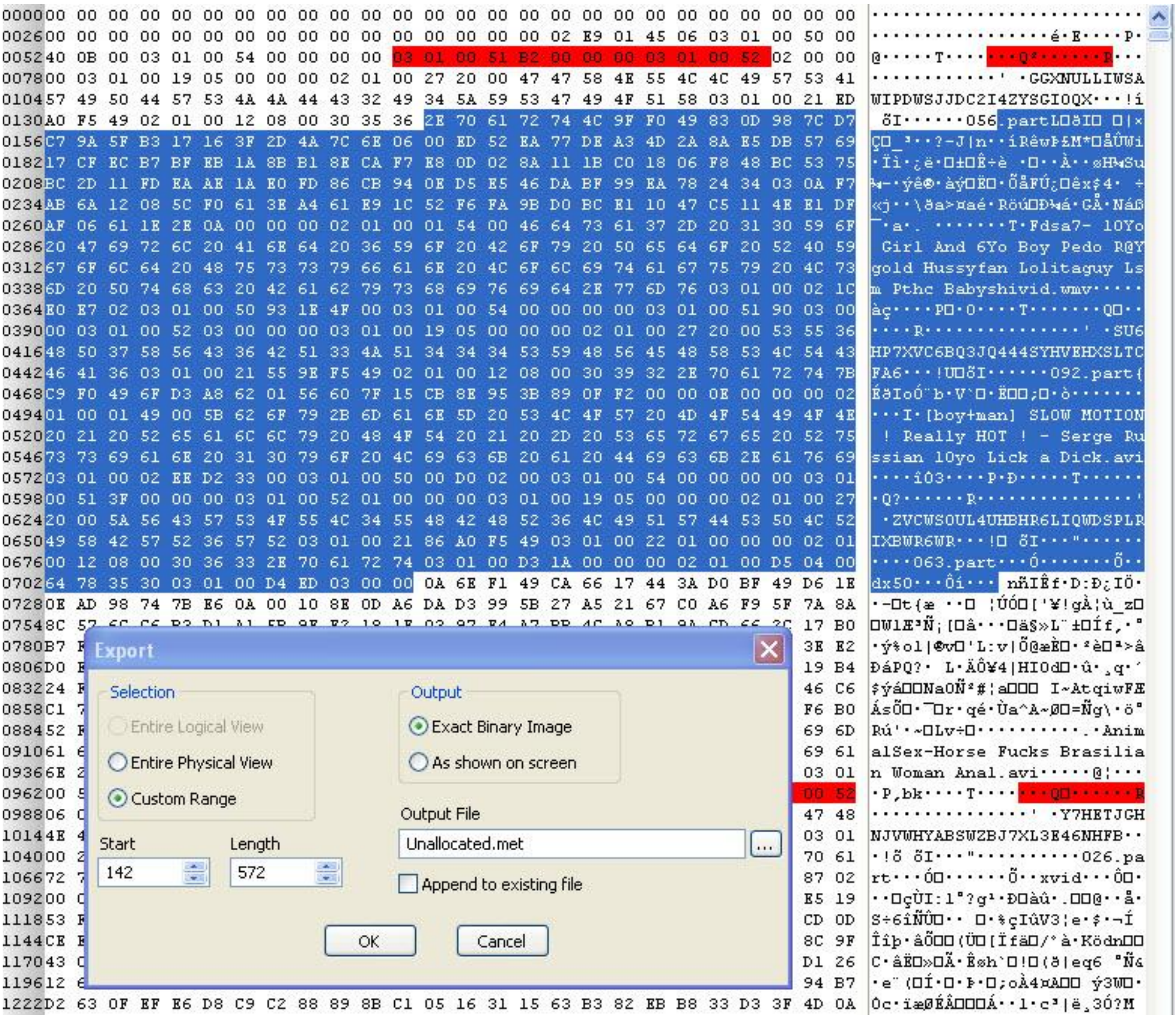
```
  Offset     0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
00000000    00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000016    00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000032    00 00 00 00 00 00 00 00  00 00 02 E9 01 45 06 03   ..........é.E..
00000048    01 00 50 00 40 0B 00 03  01 00 54 00 00 00 00 03   ..P.@.....T.....
00000064    01 00 51 B2 00 00 00 03  01 00 52 02 00 00 00 03   ..Q²......R.....
                        0 00 00 02  01 00 27 20 00 47 47 58   ...........' .GGX
                        3 57 53 41  57 49 50 44 57 53 4A 4A   NULLIWSAWIPDWSJJ
                        4 5A 59 53  47 49 4F 51 58 03 01 00   DC2I4ZYSGIOQX...
                        9 02 01 00  12 08 00 30 35 36 2E 70   !í õI......056.p
00000144    61 72 74 4C 9F F0 49 83  0D 98 7C D7 C7 9A 5F B3   artL▌ðI▌.▌|×Ç▌_³
00000160    17 16 3F 2D 4A 7C 6E 06  00 ED 52 EA 77 DE A3 4D   ..?-J|n..íRêwÞ£M
00000176    2A 8A E5 DB 57 69 17 CF  EC B7 BF EB 1A 8B B1 8E   *▌åÛWi.Ïì·¿ë.▌±▌
            CA F7 E8 0D 02 8A 11 1B  C0 18 06 F8 48 BC 53 75   Ê÷è..▌..À..øH¼Su
            BC 2D 11 FD EA AE 1A E0  FD 86 CB 94 0E D5 E5 46   ¼-.ýê®.àý▌Ë▌.ÕåF
            DA BF 99 EA 78 24 34 03  0A F7 AB 6A 12 08 5C F0   Ú¿▌êx$4..÷«j..\ð
            61 3E A4 61 E9 1C 52 F6  FA 9B D0 BC E1 10 47 C5   a>¤aé.Röú▌Ð¼á.GÅ
00000256    11 4E E1 DF AF 06 61 1E  2E 0A 00 00 00 02 01 00   .Náß¯.a.........
00000272    01 54 00 46 64 73 61 37  2D 20 31 30 59 6F 20 47   .T.Fdsa7- 10Yo G
00000288    69 72 6C 20 41 6E 64 20  36 59 6F 20 42 6F 79 20   irl And 6Yo Boy 
00000304    50 65 64 6F 20 52 40 59  67 6F 6C 64 20 48 75 73   Pedo R@Ygold Hus
00000320    73 79 66 61 6E 20 4C 6F  6C 69 74 61 67 75 79 20   syfan Lolitaguy 
00000336    4C 73 6D 20 50 74 68 63  20 42 61 62 79 73 68 69   Lsm Pthc Babyshi
00000352    76 69 64 2E 77 6D 76 03  01 00 02 1C E0 E7 02 03   vid.wmv.....àç..
00000368    01 00 50 93 1E 4F 00 03  01 00 54 00 00 00 00 03   ..P▌.O....T.....
00000384    01 00 51 90 03 00 00 03  01 00 52 03 00 00 00 03   ..Q▌......R.....
00000400    01 00 19 05 00 00 00 02  01 00 27 20 00 53 55 36   ..........' .SU6
00000416    48 50 37 58 56 43 36 42  51 33 4A 51 34 34 34 53   HP7XVC6BQ3JQ444S
00000432    59 48 56 45 48 58 53 4C  54 43 46 41 36 03 01 00   YHVEHXSLTCFA6...
00000448    21 55 9E F5 49 02 01 00  12 08 00 30 39 32 2E 70   !U▌õI......092.p
00000464    61 72 74 7B C9 F0 49 6F  D3 A8 62 01 56 60 7F 15   art{ÉðIoÓ¨b.V`▌.
00000480    CB 8E 95 3B 89 0F F2 00  00 0E 00 00 00 02 01 00   Ë▌▌;▌.ò.........
00000496    01 49 00 5B 62 6F 79 2B  6D 61 6E 5D 20 53 4C 4F   .I.[boy+man] SLO
00000512    57 20 4D 4F 54 49 4F 4E  20 21 20 52 65 61 6C 6C   W MOTION ! Reall
00000528    79 20 48 4F 54 20 21 20  2D 20 53 65 72 67 65 20   y HOT ! - Serge 
00000544    52 75 73 73 69 61 6E 20  31 30 79 6F 20 4C 69 63   Russian 10yo Lic
00000560    6B 20 61 20 44 69 63 6B  2E 61 76 69 03 01 00 02   k a Dick.avi....
00000576    EE D2 33 00 03 01 00 50  00 D0 02 00 03 01 00 54   îÒ3....P.Ð.....T
00000592    00 00 00 00 03 01 00 51  3F 00 00 00 03 01 00 52   .......Q?......R
00000608    01 00 00 00 03 01 00 19  05 00 00 00 02 01 00 27   ...............'
00000624    20 00 5A 56 43 57 53 4F  55 4C 34 55 48 42 48 52    .ZVCWSOUL4UHBHR
00000640    36 4C 49 51 57 44 53 50  4C 52 49 58 42 57 52 36   6LIQWDSPLRIXBWR6
00000656    57 52 03 01 00 21 86 A0  F5 49 03 01 00 22 01 00   WR...!▌ õI..."..
00000672    00 00 02 01 00 12 08 00  30 36 33 2E 70 61 72 74   ........063.part
00000688    03 01 00 D3 1A 00 00 00  02 01 00 D5 04 00 64 78   ...Ó.......Õ..dx
00000704    35 30 03 01 00 D4 ED 03  00 00 0A 6E F1 49 CA 66   50...Ôí....nñIÊf
00000720    17 44 3A D0 BF 49 D6 1E  0E AD 98 74 7B E6 0A 00   .D:Ð¿IÖ..-▌t{æ..
00000736    10 8E 0D A6 DA D3 99 5B  27 A5 21 67 C0 A6 F9 5F   .▌.¦ÚÓ▌['¥!gÀ¦ù_
00000752    7A 8A 8C 57 6C C6 B3 D1  A1 5B 9F E2 18 1E 03 97   z▌▌WlÆ³Ñ¡[▌â...▌
```

Start the copying 5 bytes prior to the UNIX "last Written" timestamp

UNIX "last Written" timestamp start byte

Stop copying prior the last found UNIX "last written" timestamp. Right before this timestamp you either find a reference to a ".part" file – or data belonging to a META-tag (in this case the META tag is "030100D4" and the belonging data is "ED030000"

How to export the data into a new file



```
000000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
002600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 E9 01 45 06 03 01 00 50 00
005240 0B 00 03 01 00 54 00 00 00 00 03 01 00 51 B2 00 00 00 03 01 00 52 02 00 00
007800 03 01 00 19 05 00 00 00 02 01 00 27 20 00 47 47 58 4E 55 4C 4C 49 57 53 41
010457 49 50 44 57 53 4A 4A 44 43 32 49 34 5A 59 53 47 49 4F 51 58 03 01 00 21 ED
0130A0 F5 49 02 01 00 12 08 00 30 35 36 2E 70 61 72 74 4C 9F F0 49 83 0D 98 7C D7
0156C7 9A 5F B3 17 16 3F 2D 4A 7C 6E 06 00 ED 52 EA 77 DE A3 4D 2A 8A E5 DB 57 69
018217 CF EC B7 BF EB 1A 8B B1 8E CA F7 E8 0D 02 8A 11 1B C0 18 06 F8 48 BC 53 75
0208BC 2D 11 FD EA AE 1A E0 FD 86 CB 94 0E D5 E5 46 DA BF 99 EA 78 24 34 03 0A F7
0234AB 6A 12 08 5C F0 61 3E A4 61 E9 1C 52 F6 FA 9B D0 BC E1 10 47 C5 11 4E E1 DF
0260AF 06 61 1E 2E 0A 00 00 00 02 01 00 01 54 00 46 64 73 61 37 2D 20 31 30 59 6F
028620 47 69 72 6C 20 41 6E 64 20 36 59 6F 20 42 6F 79 20 50 65 64 6F 20 52 40 59
031267 6F 6C 64 20 48 75 73 73 79 66 61 6E 20 4C 6F 6C 69 74 61 67 75 79 20 4C 73
03386D 20 50 74 68 63 20 42 61 62 79 73 68 69 76 69 64 2E 77 6D 76 03 01 00 02 1C
0364E0 E7 02 03 01 00 50 93 1E 4F 00 03 01 00 54 00 00 00 00 03 01 00 51 90 03 00
039000 03 01 00 52 03 00 00 00 03 01 00 19 05 00 00 00 02 01 00 27 20 00 53 55 36
041648 50 37 58 56 43 36 42 51 33 4A 51 34 34 34 53 59 48 56 45 48 58 53 4C 54 43
044246 41 36 03 01 00 21 55 9E F5 49 02 01 00 12 08 00 30 39 32 2E 70 61 72 74 7B
0468C9 F0 49 6F D3 A8 62 01 56 60 7F 15 CB 8E 95 3B 89 0F F2 00 00 0E 00 00 00 02
049401 00 01 49 00 5B 62 6F 79 2B 6D 61 6E 5D 20 53 4C 4F 57 20 4D 4F 54 49 4F 4E
052020 21 20 52 65 61 6C 6C 79 20 48 4F 54 20 21 20 2D 20 53 65 72 67 65 20 52 75
054673 73 69 61 6E 20 31 30 79 6F 20 4C 69 63 6B 20 61 20 44 69 63 6B 2E 61 76 69
057203 01 00 02 EE D2 33 00 03 01 00 50 00 D0 02 00 03 01 00 54 00 00 00 00 03 01
059800 51 3F 00 00 00 03 01 00 52 01 00 00 00 03 01 00 19 05 00 00 00 02 01 00 27
062420 00 5A 56 43 57 53 4F 55 4C 34 55 48 42 48 52 36 4C 49 51 57 44 53 50 4C 52
065049 58 42 57 52 36 57 52 03 01 00 21 86 A0 F5 49 03 01 00 22 01 00 00 00 02 01
067600 12 08 00 30 36 33 2E 70 61 72 74 03 01 00 D3 1A 00 00 00 02 01 00 D5 04 00
070264 78 35 30 03 01 00 D4 ED 03 00 00 0A 6E F1 49 CA 66 17 44 3A D0 BF 49 D6 1E
07280E AD 98 74 7B E6 0A 00 10 8E 0D A6 DA D3 99 5B 27 A5 21 67 C0 A6 F9 5F 7A 8A
07548C                                                                      17 B0
0780B7                                                                      3E E2
0806D0                                                                      19 B4
083224                                                                      46 C6
0858C1                                                                      F6 B0
088452                                                                      69 6D
091061                                                                      69 61
09366E                                                                      03 01
096200                                                                      00 52
098806                                                                      47 48
10144E                                                                      03 01
104000                                                                      70 61
106672                                                                      87 02
109200                                                                      E5 19
111853                                                                      CD 0D
1144CE                                                                      8C 9F
117043                                                                      D1 26
119612                                                                      94 B7
1222D2 63 0F EF E6 D8 C9 C2 88 89 8B C1 05 16 31 15 63 B3 82 EB B8 33 D3 3F 4D 0A
```

Selection

○ Entire Logical View

○ Entire Physical View

● Custom Range

Start: 142

Length: 572

Output

● Exact Binary Image

○ As shown on screen

Output File: Unallocated.met

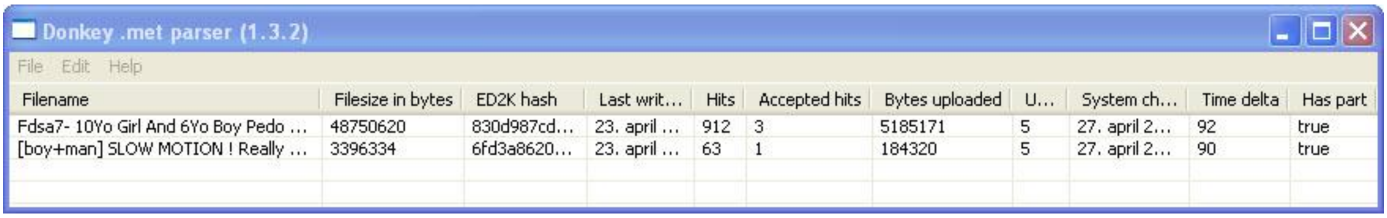
□ Append to existing file

Right-click the selected data and choose "Export"

Choose the Output file and path (somthing.met) and click "ok"

The data will now be exported into a ".met" file.

Open DonkeyMet Parser, and parse the new file



Donkey .met parser (1.3.2)

Filename	Filesize in bytes	ED2K hash	Last writ...	Hits	Accepted hits	Bytes uploaded	U...	System ch...	Time delta	Has part
Fdsa7- 10Yo Girl And 6Yo Boy Pedo ...	48750620	830d987cd...	23. april ...	912	3	5185171	5	27. april 2...	92	true
[boy+man] SLOW MOTION ! Really ...	3396334	6fd3a8620...	23. april ...	63	1	184320	5	27. april 2...	90	true

This is how to parse data found in unallocated clusters

It's possible to use other tools to extract the binary data - find your own way to use these tools :-)

LimeWire

What version of LimeWire is examined?

The following information is based on examination of LimWire v. 5.1.3 – basic version. This is the current newest version of LimeWire (june 2009) – and it has some significant changes compared to the 4.x versions. The differences to earlier versions will not be mentioned.

LimeWire is a P2P client connecting to the Gnutella network.

The client comes in 2 different versions:

- LimeWire Basic
- LimeWire Pro

The “Basic version” is free, while the “Pro version” costs aprox. 35 UD$ a year

The text given below has been taken directly from the official homepage of LimeWire on www.limewire.com

About LimeWire

LimeWire is the world's most popular peer-to-peer file-sharing program. With over 70 million unique monthly users, the software is downloaded hundreds of thousands of times every day and boasts millions of active users at any given moment. LimeWire uses the BitTorrent protocol and the Gnutella network to provide an unparalleled searches and download speed to the user. As always, LimeWire takes the security of its users very seriously and will never bundle spyware, adware, or viruses

The Company

Founded in 2000 by CEO Mark Gorton, Lime Wire is a leader of innovative peer-to-peer software development and solutions in the file sharing industry. We develop powerful, sophisticated software offering an unparalleled user experience. Our signature products, LimeWire BASIC and

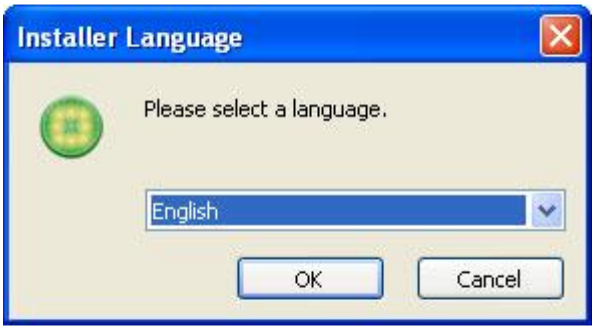
LimeWire PRO, run on the decentralized Gnutella Network and are among the world's most popular peer-to-peer file sharing applications. More recently we've launched the LimeWire Store, a digital media store, and are working on a number of projects to help further connect Lime Wire's peer-to-peer community. Interested in joining Lime Wire? Read about our open positions here.

What is LimeWire?

LimeWire is a peer-to-peer file sharing program that connects to the Gnutella network and enables users to search for and download files from other users. It is not a web site or a service, and Lime Wire does not provide any of the content found on the network. LimeWire enables you to share your files with millions of other LimeWire users, and vice versa, so there is always a diverse selection of files available.

Installation

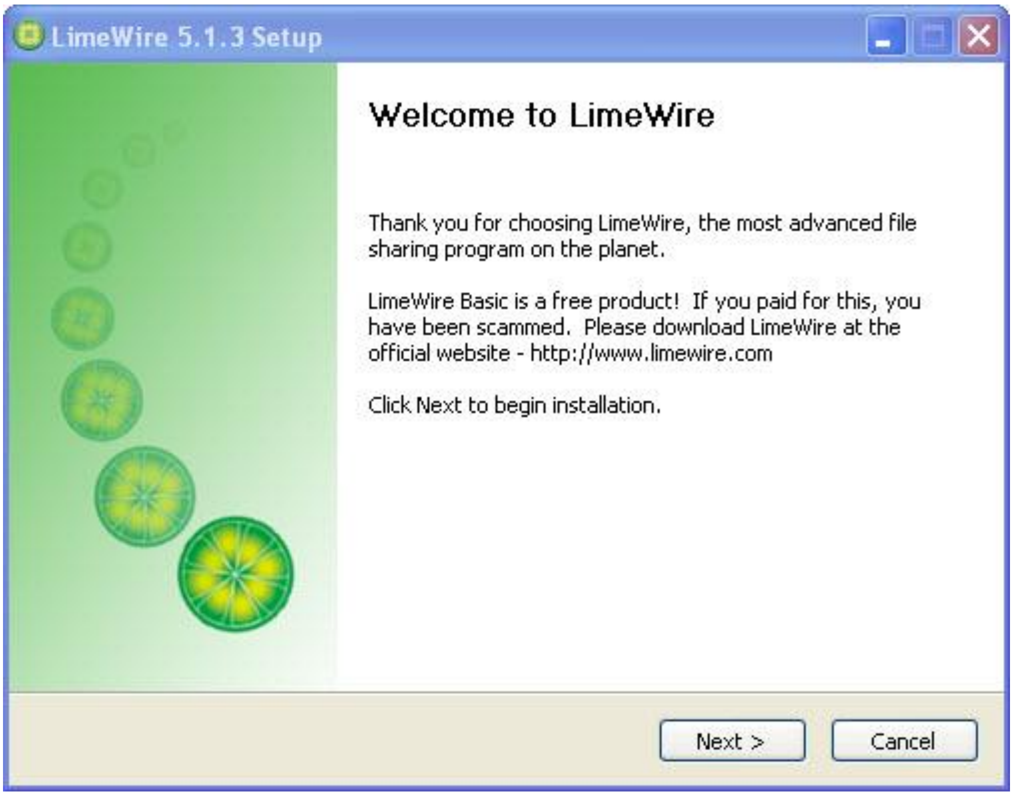
The following screenshots shows a standard installation of LimeWire 5.1.3 Basic version (free)



Installer Language

Please select a language.

English

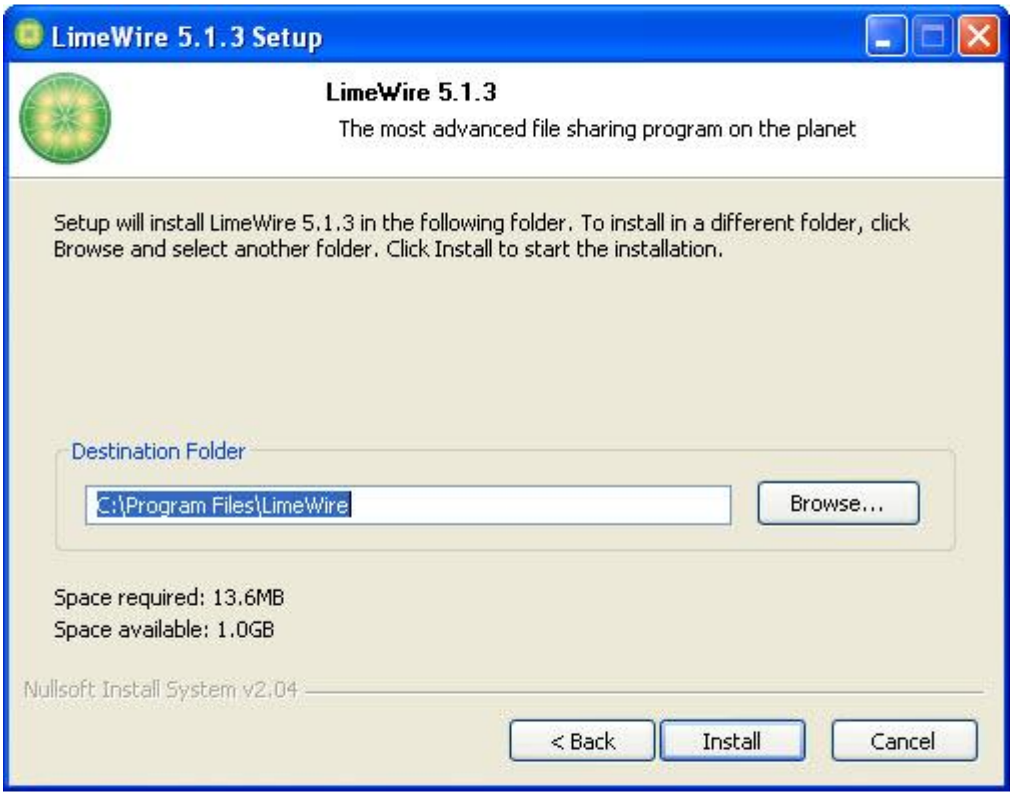


Welcome to LimeWire

Thank you for choosing LimeWire, the most advanced file sharing program on the planet.

LimeWire Basic is a free product! If you paid for this, you have been scammed. Please download LimeWire at the official website - http://www.limewire.com

Click Next to begin installation.



LimeWire 5.1.3

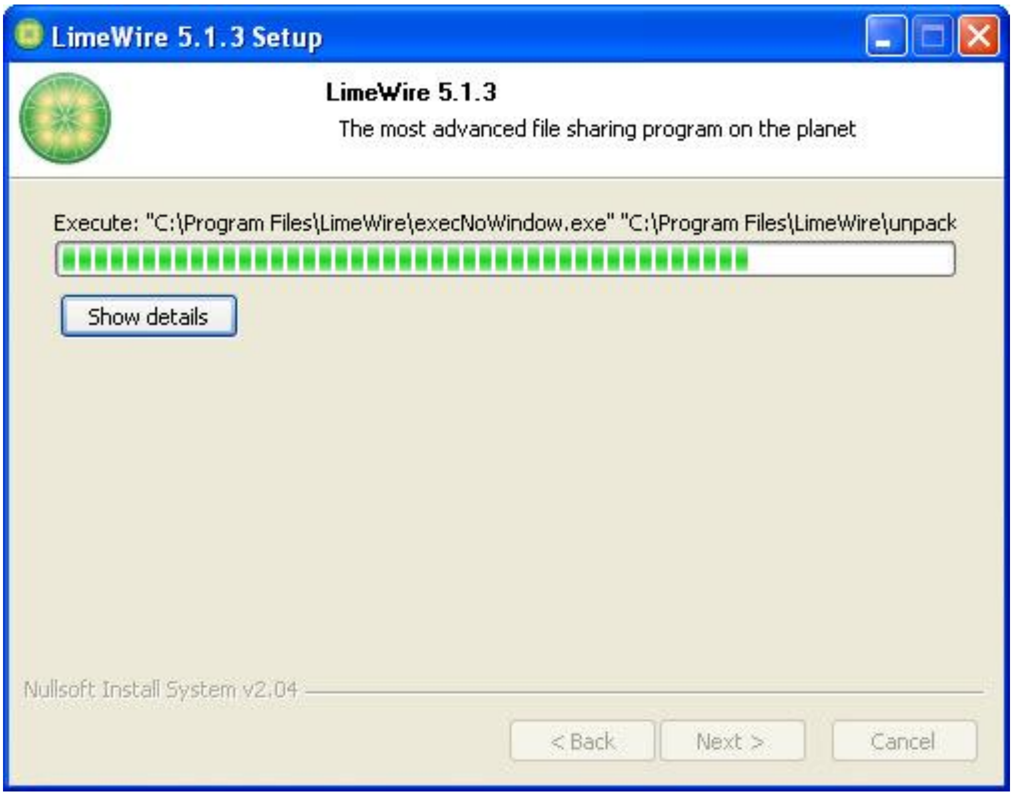
The most advanced file sharing program on the planet

Setup will install LimeWire 5.1.3 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files\LimeWire

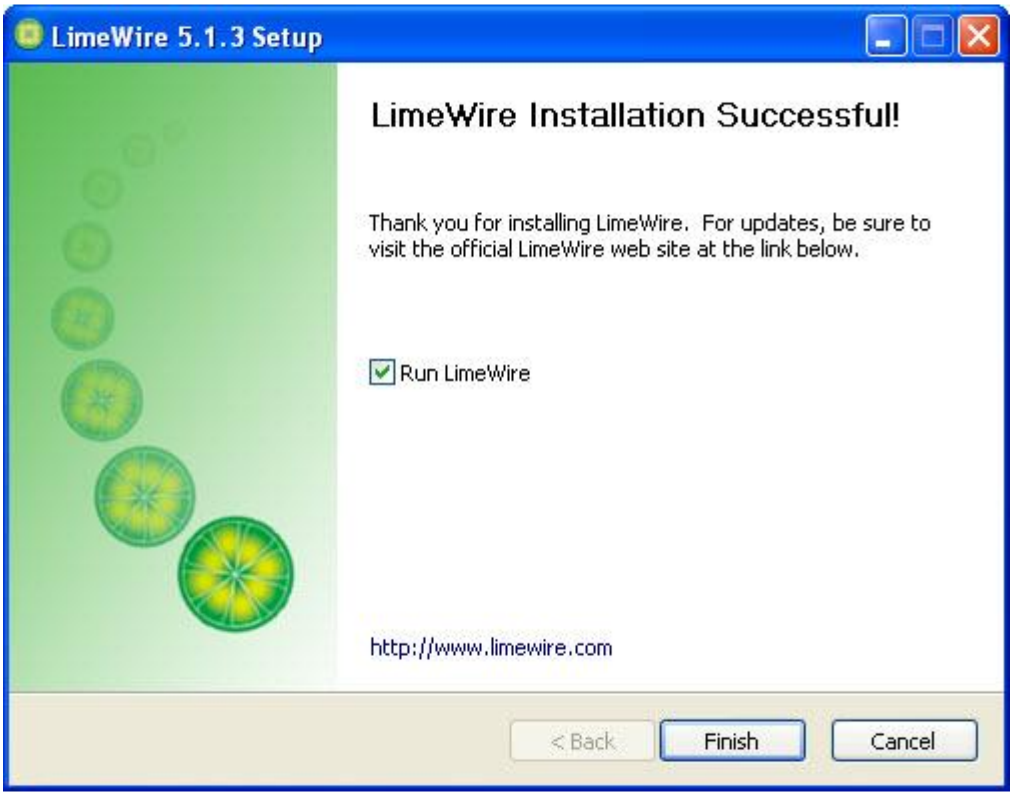
Space required: 13.6MB

Space available: 1.0GB


LimeWire 5.1.3 Setup
LimeWire 5.1.3
The most advanced file sharing program on the planet

Execute: "C:\Program Files\LimeWire\execNoWindow.exe" "C:\Program Files\LimeWire\unpack

Show details
Nullsoft Install System v2.04
< Back
Next >
Cancel

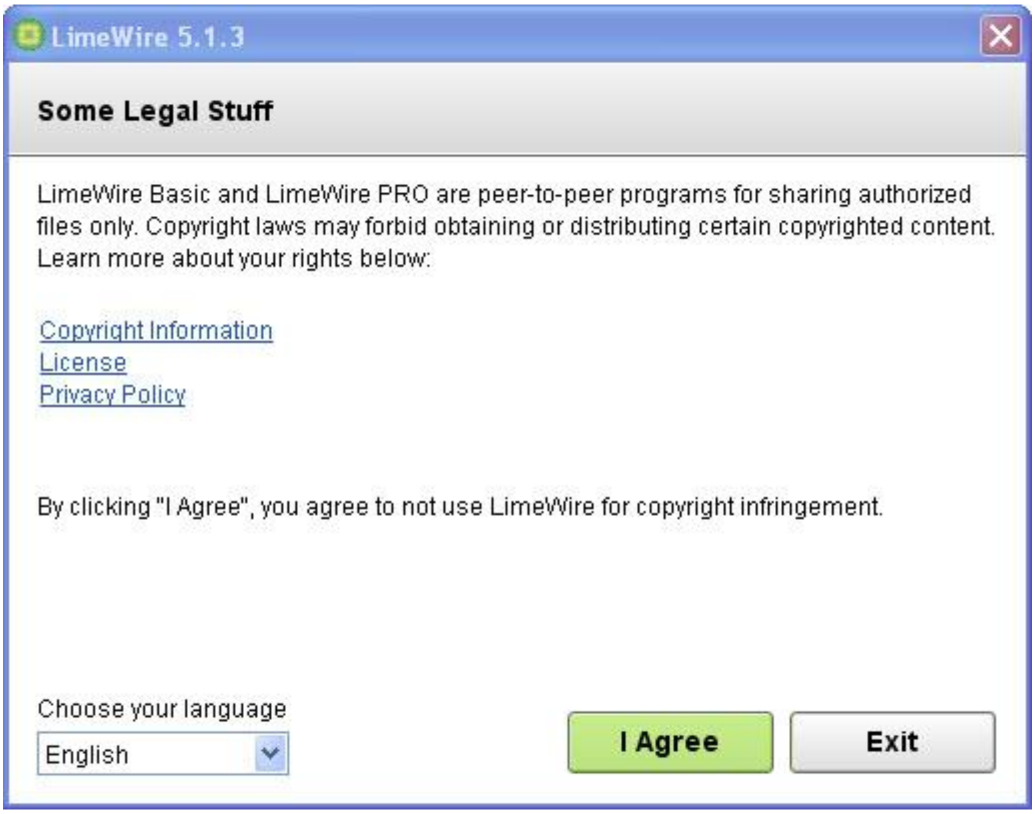


LimeWire Installation Successful!

Thank you for installing LimeWire. For updates, be sure to visit the official LimeWire web site at the link below.

☑ Run LimeWire

http://www.limewire.com



Some Legal Stuff

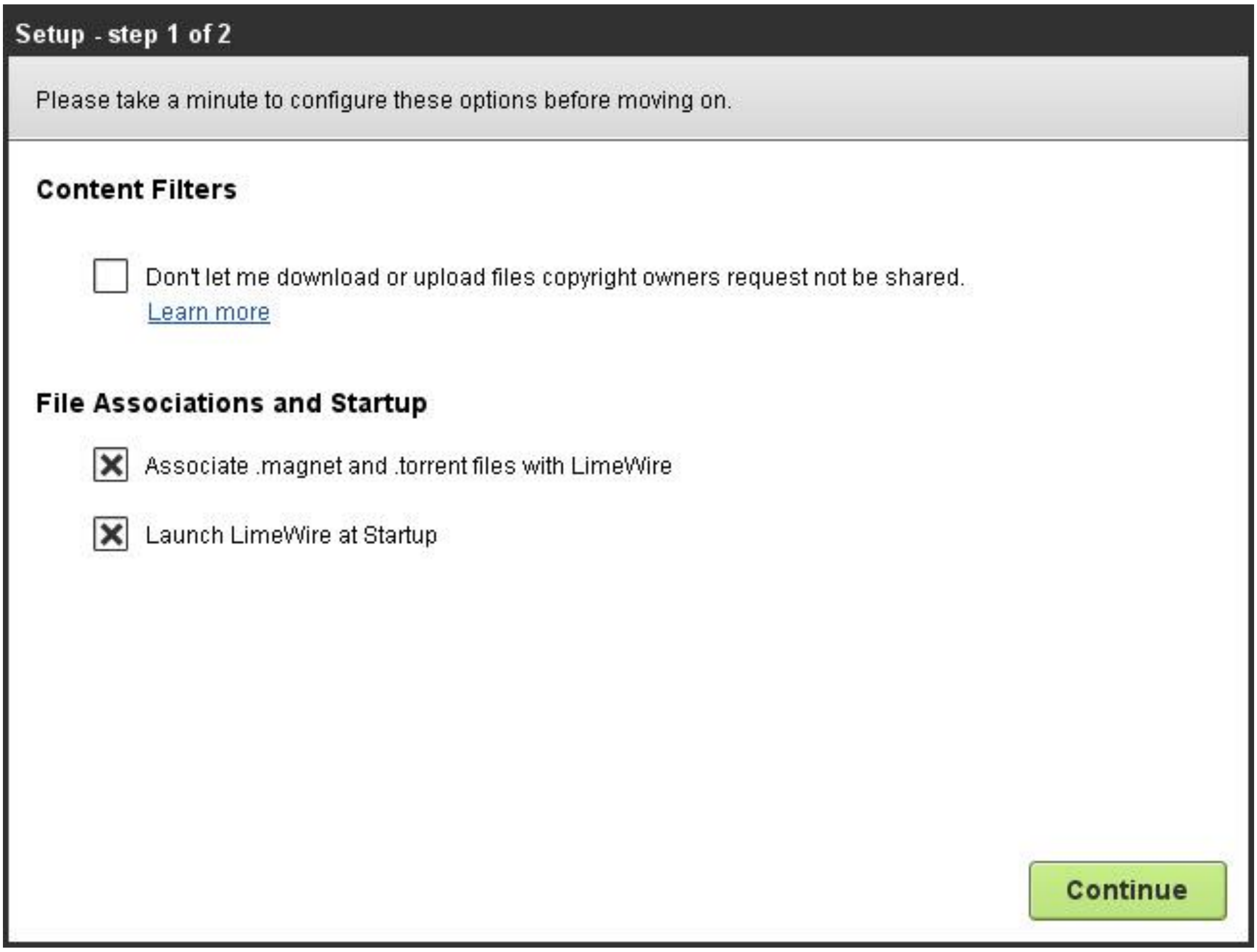
LimeWire Basic and LimeWire PRO are peer-to-peer programs for sharing authorized files only. Copyright laws may forbid obtaining or distributing certain copyrighted content. Learn more about your rights below:

Copyright Information
License
Privacy Policy

By clicking "I Agree", you agree to not use LimeWire for copyright infringement.

Choose your language: English

Scouring NYC for Limes...



Setup - step 1 of 2

Please take a minute to configure these options before moving on.

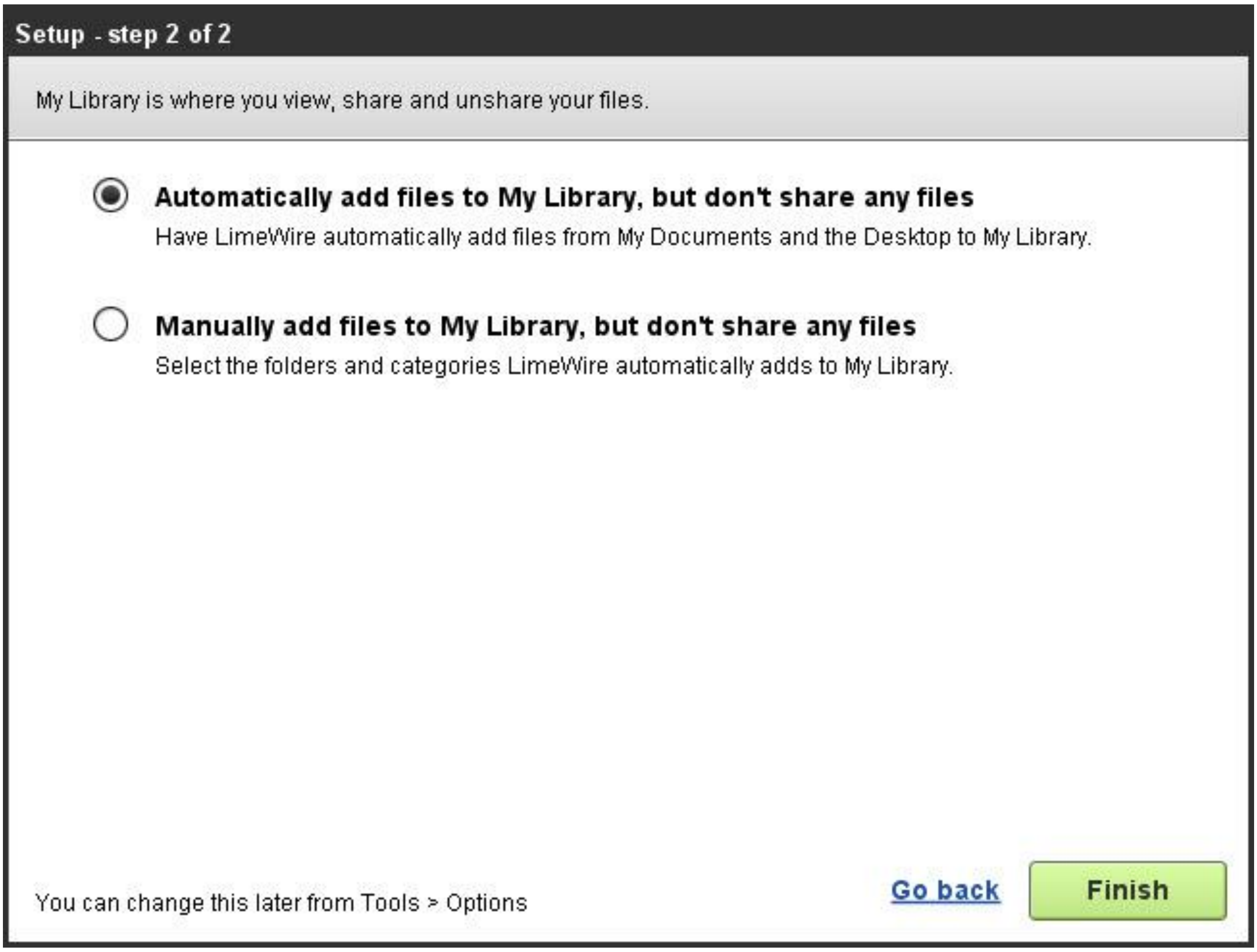
Content Filters

☐ Don't let me download or upload files copyright owners request not be shared.
Learn more

File Associations and Startup

☒ Associate .magnet and .torrent files with LimeWire

☒ Launch LimeWire at Startup



Setup - step 2 of 2

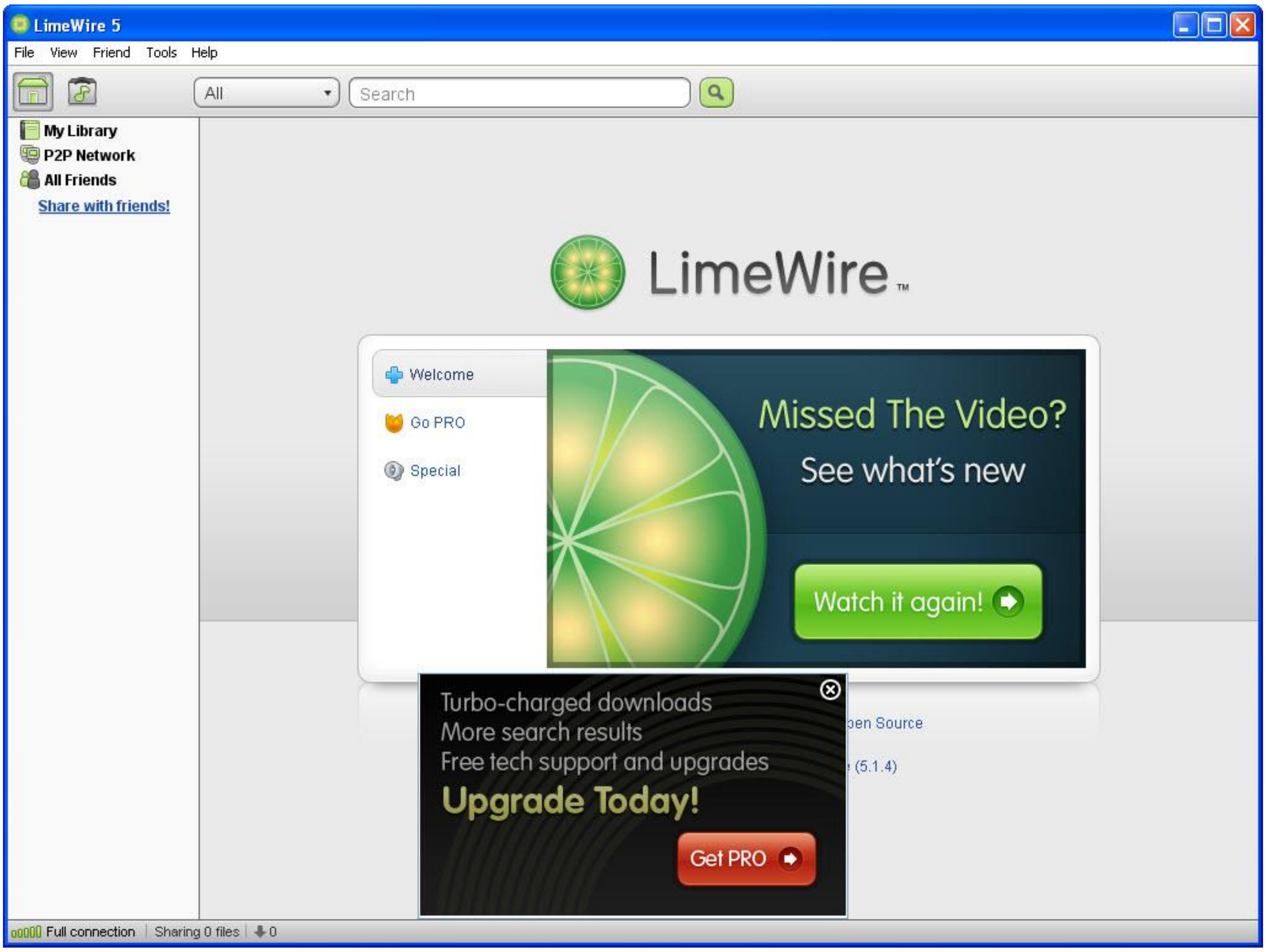
My Library is where you view, share and unshare your files.

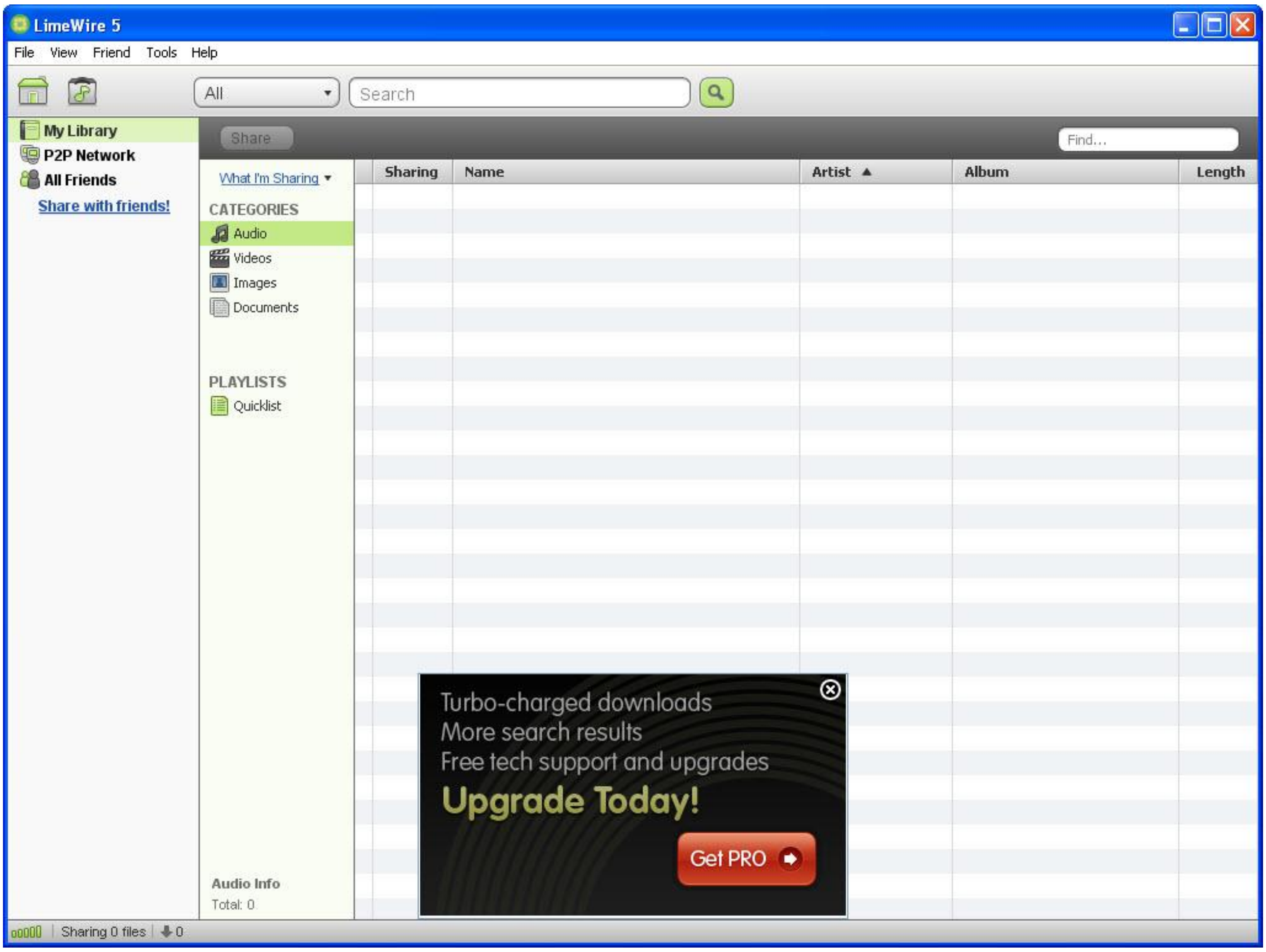
● **Automatically add files to My Library, but don't share any files**
Have LimeWire automatically add files from My Documents and the Desktop to My Library.

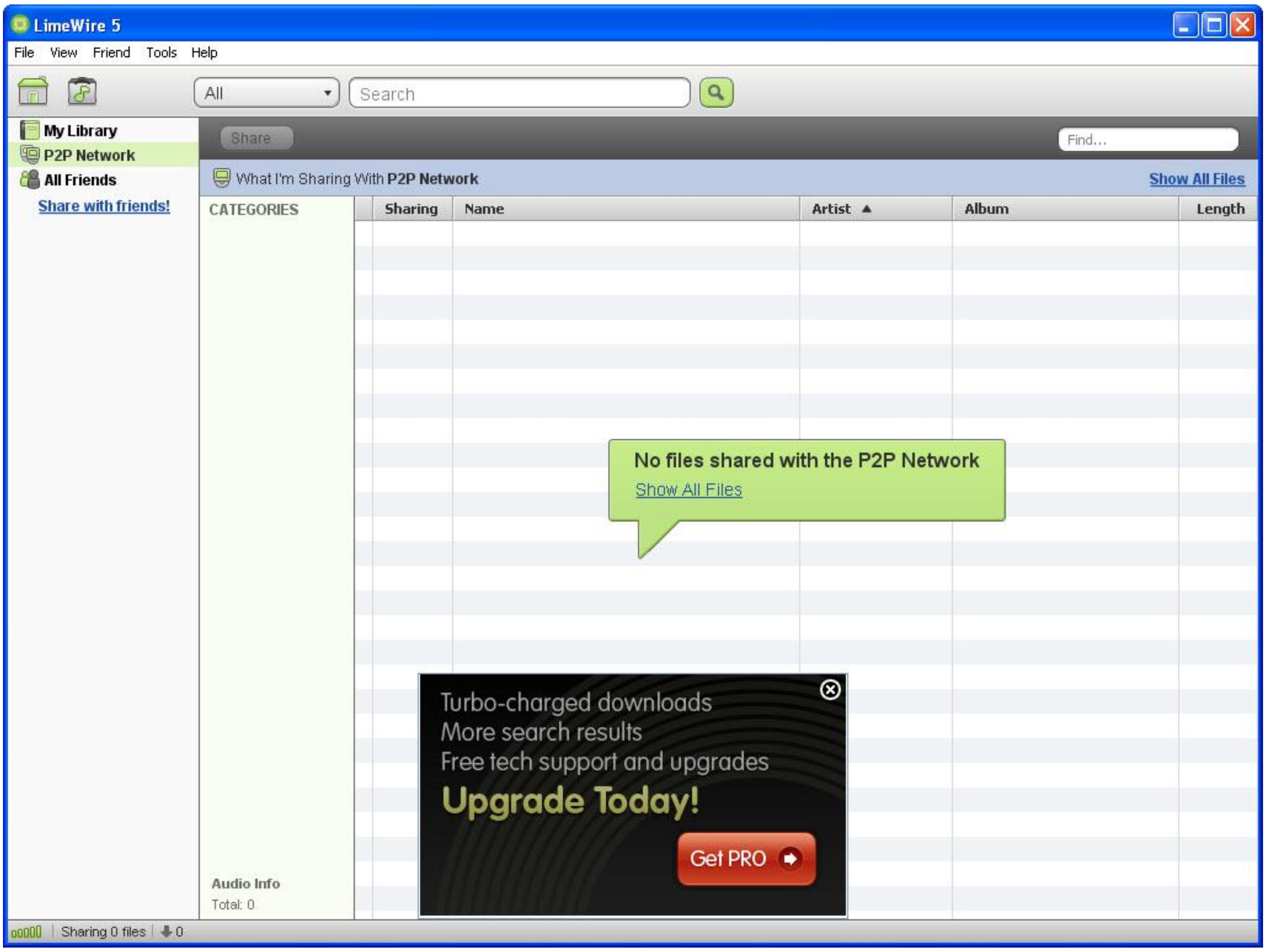
○ **Manually add files to My Library, but don't share any files**
Select the folders and categories LimeWire automatically adds to My Library.

You can change this later from Tools > Options

NOTE: Files downloaded with LimeWire are automatically shared on the P2P network – in spite of the setting shown !!

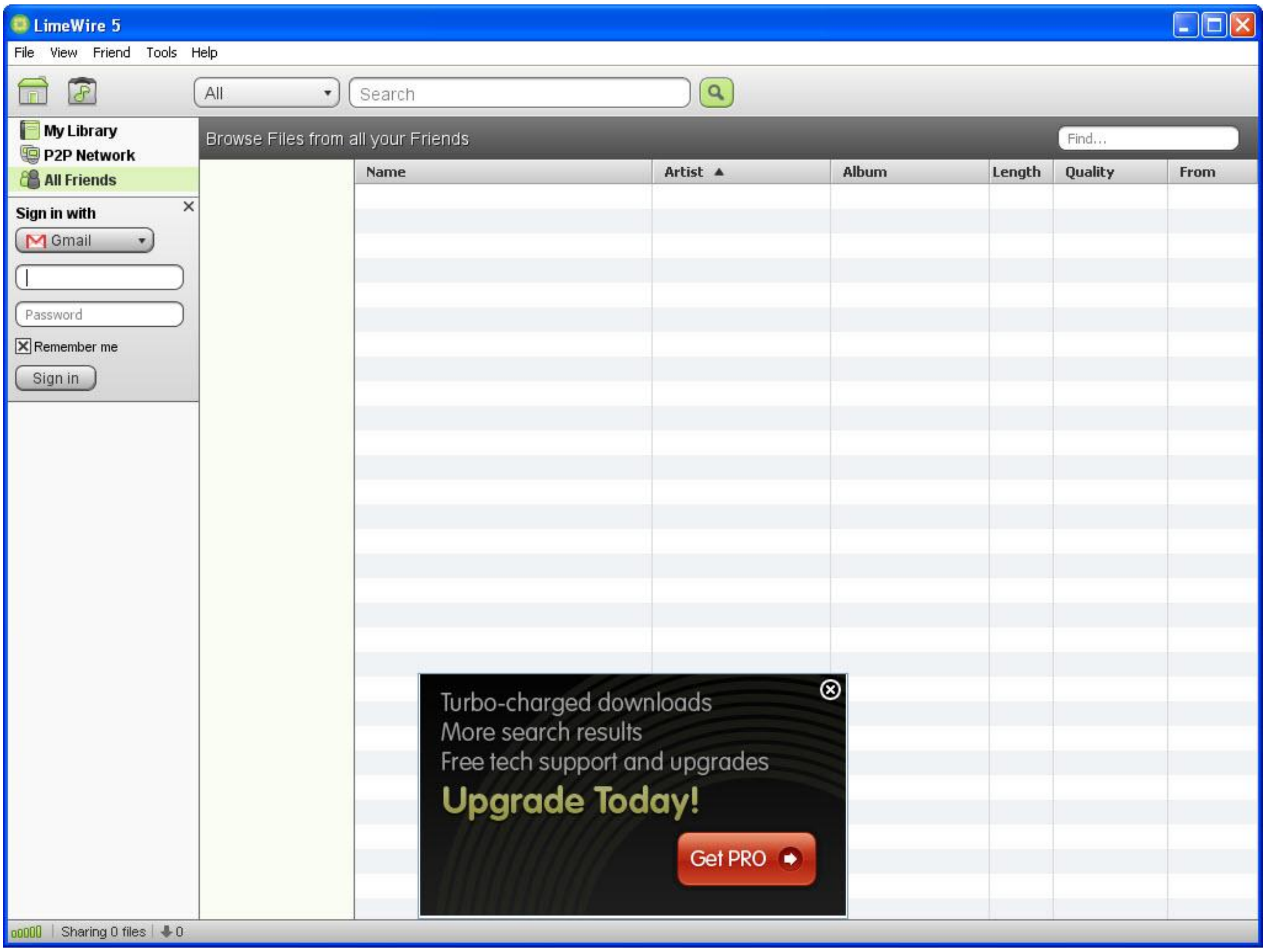

LimeWire 5
File View Friend Tools Help
All
Search
My Library
P2P Network
All Friends
Share with friends!
LimeWire
Welcome
Go PRO
Special
Missed The Video?
See what's new
Watch it again!
Turbo-charged downloads
More search results
Free tech support and upgrades
Upgrade Today!
Get PRO
pen Source
(5.1.4)
Full connection
Sharing 0 files
0


LimeWire 5
File View Friend Tools Help
All
Search
My Library
P2P Network
All Friends
Share with friends!
Share
Find...
What I'm Sharing
CATEGORIES
Audio
Videos
Images
Documents
PLAYLISTS
Quicklist
Audio Info
Total: 0
Sharing
Name
Artist
Album
Length
Turbo-charged downloads
More search results
Free tech support and upgrades
Upgrade Today!
Get PRO
Sharing 0 files
0



No files shared with the P2P Network

Show All Files

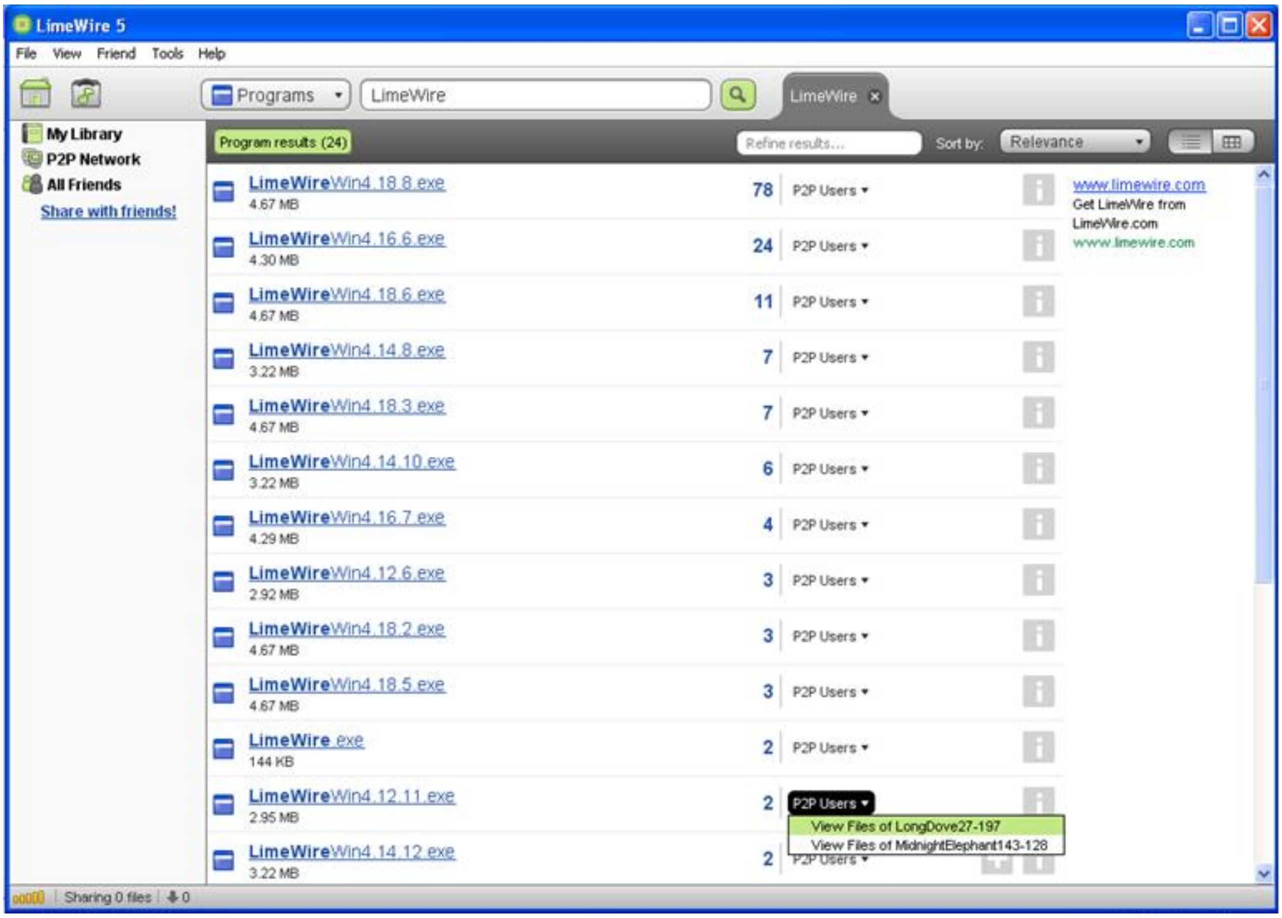


WIKI information from the LimeWire website

The following information is taken from the LimeWire WIKI (http://wiki.limewire.org/index.php?title=Main_Page)

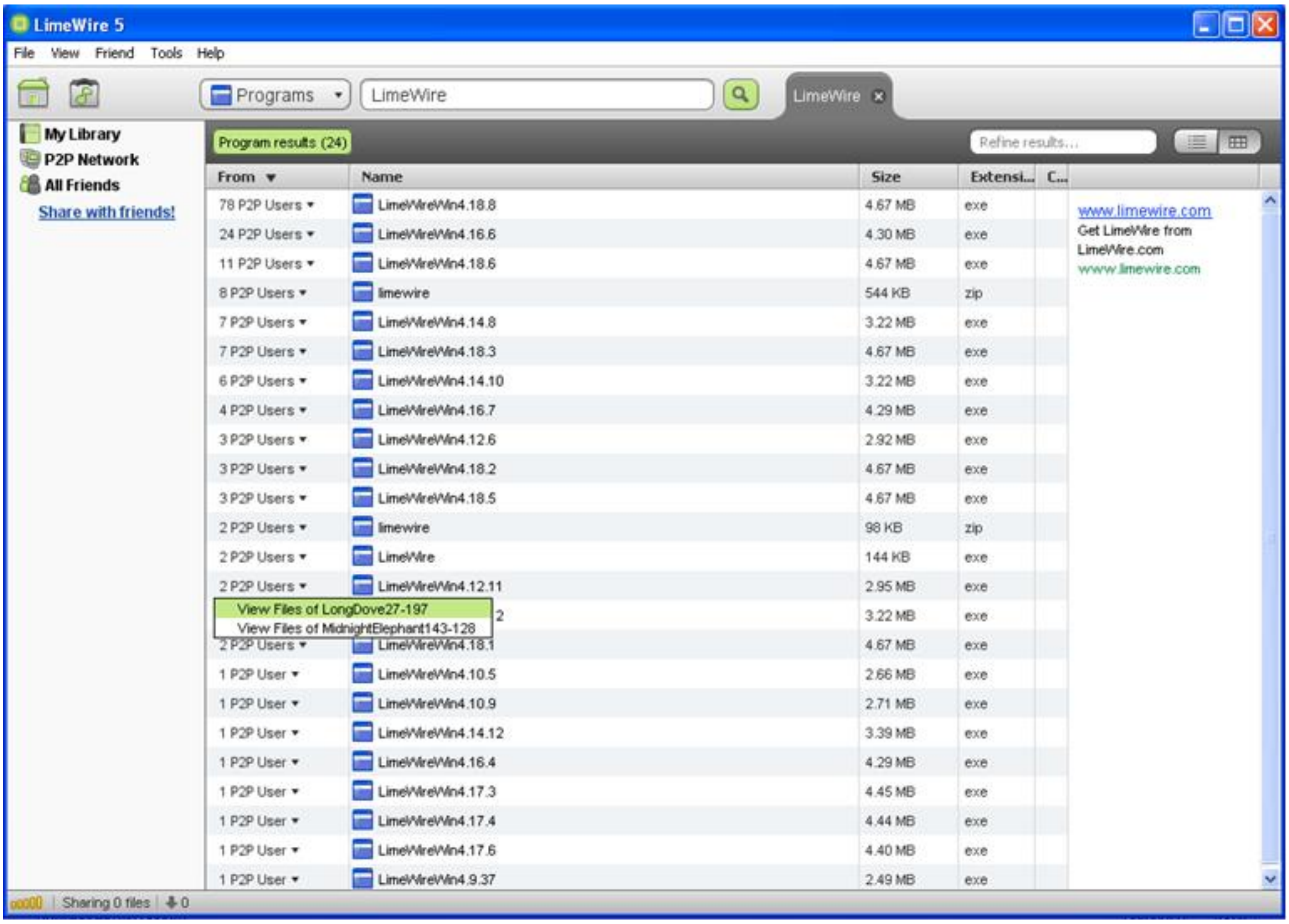
Browse files is a way to see all the files someone who appears in a search result is sharing. Click the down arrow next to '1 P2P User', '# P2P Users', 'Friend' or even 'People' to browse which files are shared.

'Friend' appears if you are using Friends and a contact has a file which matches your search. On the other hand, 'People' might appear if a friend and other people on the P2P Network are sharing the file.



LimeWireWin4.18.8.exe	4.67 MB	78	P2P Users
LimeWireWin4.16.6.exe	4.30 MB	24	P2P Users
LimeWireWin4.18.6.exe	4.67 MB	11	P2P Users
LimeWireWin4.14.8.exe	3.22 MB	7	P2P Users
LimeWireWin4.18.3.exe	4.67 MB	7	P2P Users
LimeWireWin4.14.10.exe	3.22 MB	6	P2P Users
LimeWireWin4.16.7.exe	4.29 MB	4	P2P Users
LimeWireWin4.12.6.exe	2.92 MB	3	P2P Users
LimeWireWin4.18.2.exe	4.67 MB	3	P2P Users
LimeWireWin4.18.5.exe	4.67 MB	3	P2P Users
LimeWire.exe	144 KB	2	P2P Users
LimeWireWin4.12.11.exe	2.95 MB	2	P2P Users
LimeWireWin4.14.12.exe	3.22 MB	2	P2P Users

or with the Classic View



From	Name	Size	Extensi...	C...
78 P2P Users	LimeWireWin4.18.8	4.67 MB	exe	
24 P2P Users	LimeWireWin4.16.6	4.30 MB	exe	
11 P2P Users	LimeWireWin4.18.6	4.67 MB	exe	
8 P2P Users	limewire	544 KB	zip	
7 P2P Users	LimeWireWin4.14.8	3.22 MB	exe	
7 P2P Users	LimeWireWin4.18.3	4.67 MB	exe	
6 P2P Users	LimeWireWin4.14.10	3.22 MB	exe	
4 P2P Users	LimeWireWin4.16.7	4.29 MB	exe	
3 P2P Users	LimeWireWin4.12.6	2.92 MB	exe	
3 P2P Users	LimeWireWin4.18.2	4.67 MB	exe	
3 P2P Users	LimeWireWin4.18.5	4.67 MB	exe	
2 P2P Users	limewire	98 KB	zip	
2 P2P Users	LimeWire	144 KB	exe	
2 P2P Users	LimeWireWin4.12.11	2.95 MB	exe	
2		3.22 MB	exe	
2 P2P Users	LimeWireWin4.18.1	4.67 MB	exe	
1 P2P User	LimeWireWin4.10.5	2.66 MB	exe	
1 P2P User	LimeWireWin4.10.9	2.71 MB	exe	
1 P2P User	LimeWireWin4.14.12	3.39 MB	exe	
1 P2P User	LimeWireWin4.16.4	4.29 MB	exe	
1 P2P User	LimeWireWin4.17.3	4.45 MB	exe	
1 P2P User	LimeWireWin4.17.4	4.44 MB	exe	
1 P2P User	LimeWireWin4.17.6	4.40 MB	exe	
1 P2P User	LimeWireWin4.9.37	2.49 MB	exe	

www.limewire.com
Get LimeWire from LimeWire.com
www.limewire.com

Then when you select a person to browse, the library is shown on the Sidebar under On LimeWire:

Download

Download a search result through LimeWire by clicking on the file name.

Downloads from the P2P Network are automatically shared, as specified in your Options. On the other hand, downloads from Friends are not shared automatically.

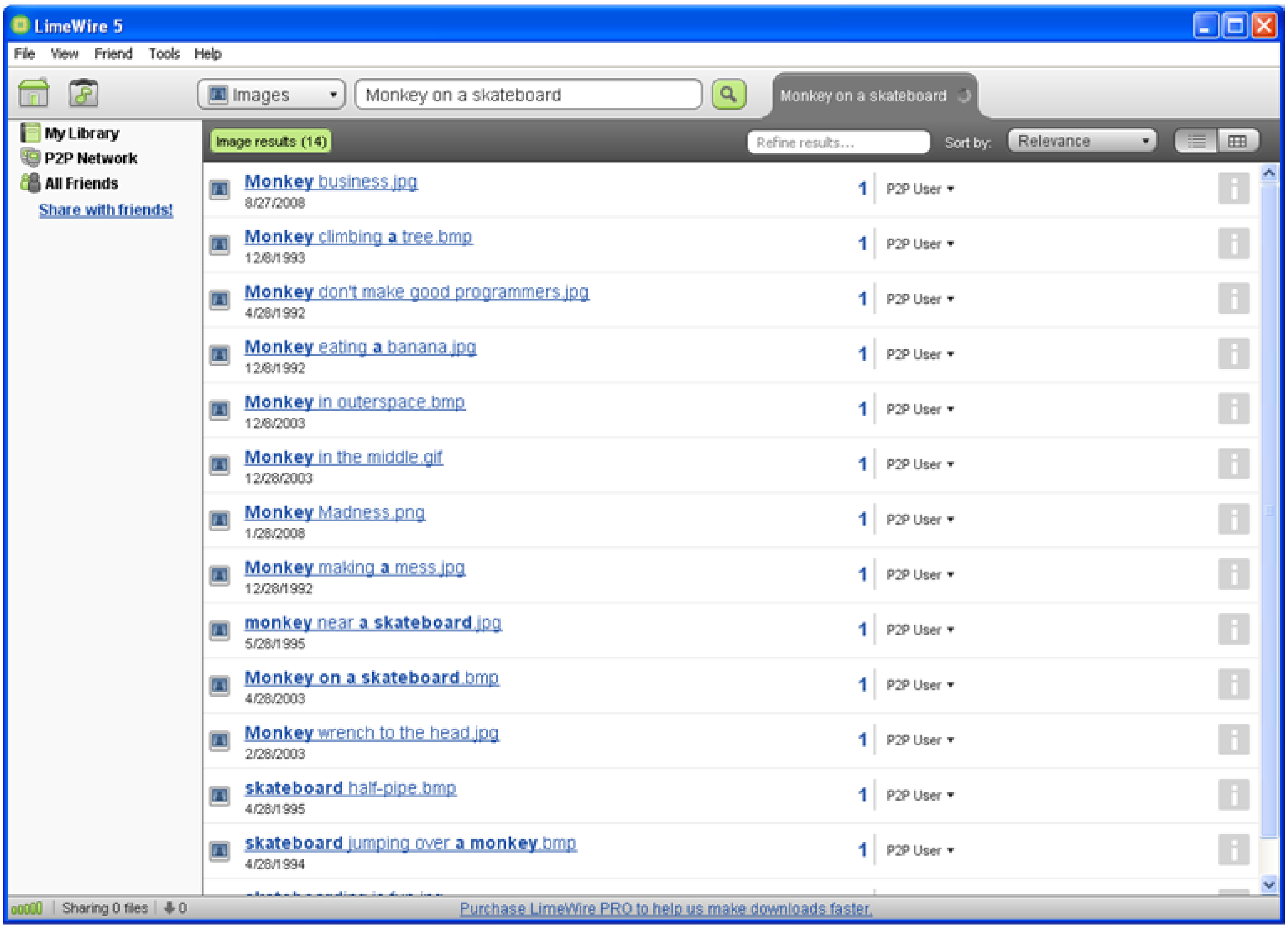
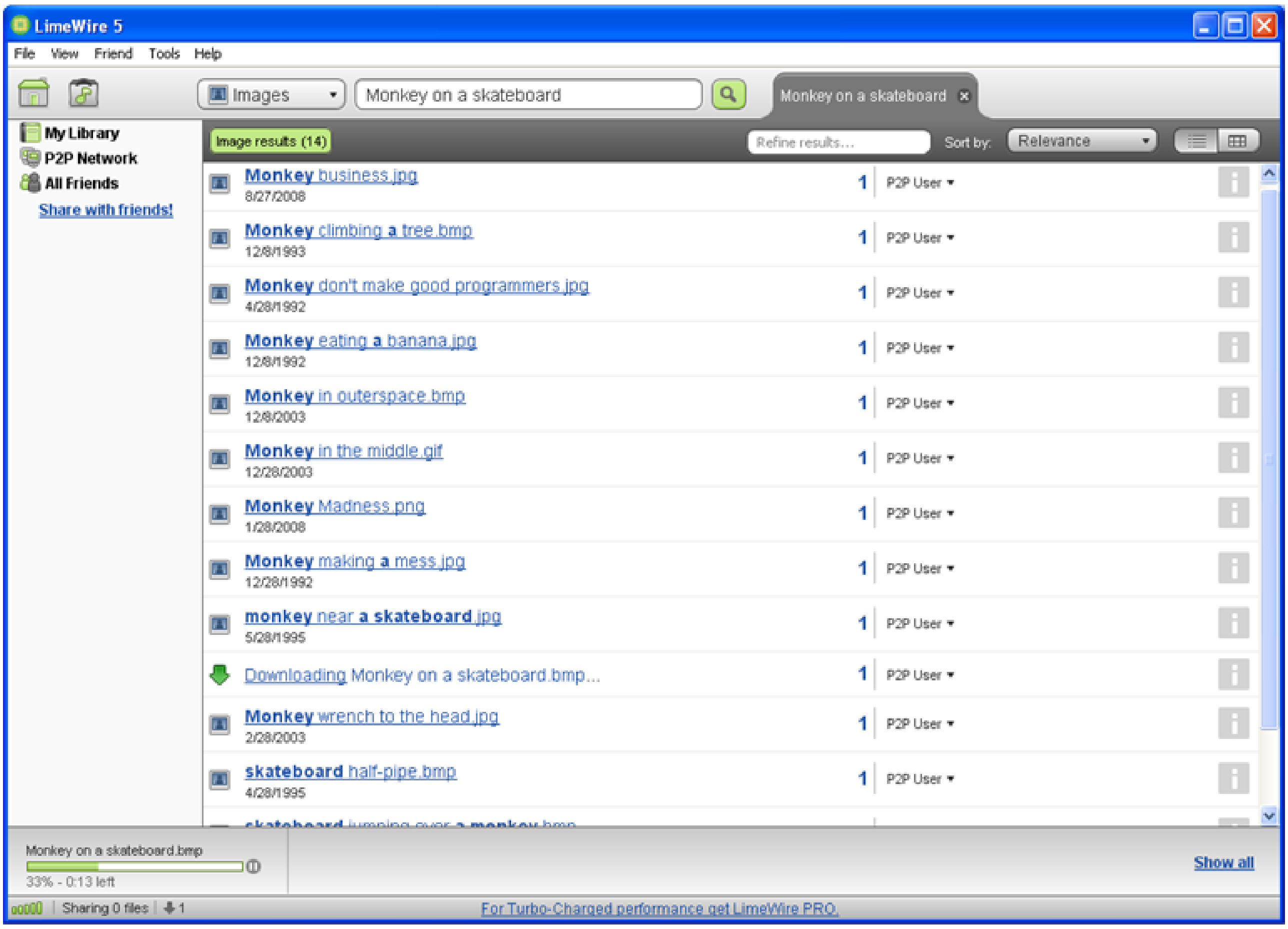


Image results (14)

Monkey business.jpg 8/27/2008	1	P2P User
Monkey climbing a tree.bmp 12/8/1993	1	P2P User
Monkey don't make good programmers.jpg 4/28/1992	1	P2P User
Monkey eating a banana.jpg 12/8/1992	1	P2P User
Monkey in outerspace.bmp 12/8/2003	1	P2P User
Monkey in the middle.gif 12/28/2003	1	P2P User
Monkey Madness.png 1/28/2008	1	P2P User
Monkey making a mess.jpg 12/28/1992	1	P2P User
monkey near a skateboard.jpg 5/28/1995	1	P2P User
Monkey on a skateboard.bmp 4/28/2003	1	P2P User
Monkey wrench to the head.jpg 2/28/2003	1	P2P User
skateboard half-pipe.bmp 4/28/1995	1	P2P User
skateboard jumping over a monkey.bmp 4/28/1994	1	P2P User

When you click a search result to download, the search results shows an arrow and adds "Downloading" to the search result. At the bottom of the screen is the status of your last few downloads.



LimeWire 5

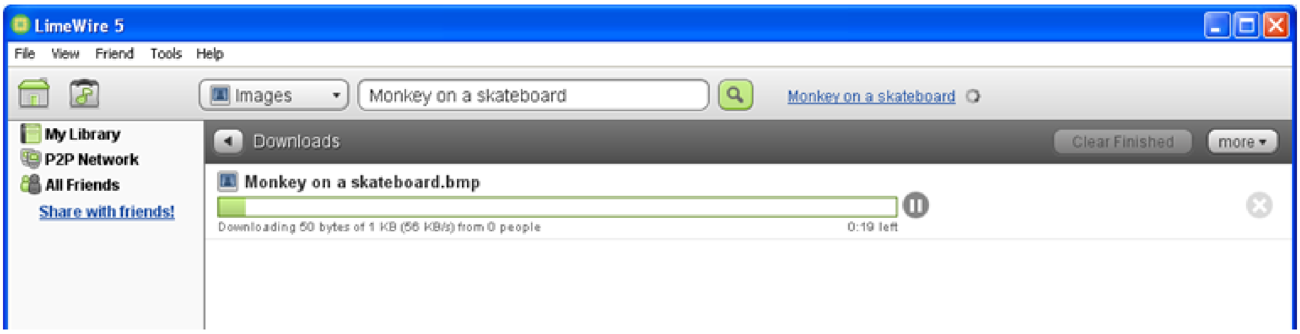
Monkey business.jpg 8/27/2008	1	P2P User
Monkey climbing a tree.bmp 12/8/1993	1	P2P User
Monkey don't make good programmers.jpg 4/28/1992	1	P2P User
Monkey eating a banana.jpg 12/8/1992	1	P2P User
Monkey in outerspace.bmp 12/8/2003	1	P2P User
Monkey in the middle.gif 12/28/2003	1	P2P User
Monkey Madness.png 1/28/2008	1	P2P User
Monkey making a mess.jpg 12/28/1992	1	P2P User
monkey near a skateboard.jpg 5/28/1995	1	P2P User
Downloading Monkey on a skateboard.bmp...	1	P2P User
Monkey wrench to the head.jpg 2/28/2003	1	P2P User
skateboard half-pipe.bmp 4/28/1995	1	P2P User
skateboard jumping over a monkey.bmp		

Monkey on a skateboard.bmp
33% - 0:13 left

When the file finishes downloading, the down arrow becomes a book icon to show it's in My Library. If you double-click the book icon or single-click the underlined 'My Library', LimeWire takes you to My Library and selects the file.

Monkey on a skateboard.bmp is in My Library.

Additionally, you can click Show all from the search results to see all your downloads along with more detailed information:

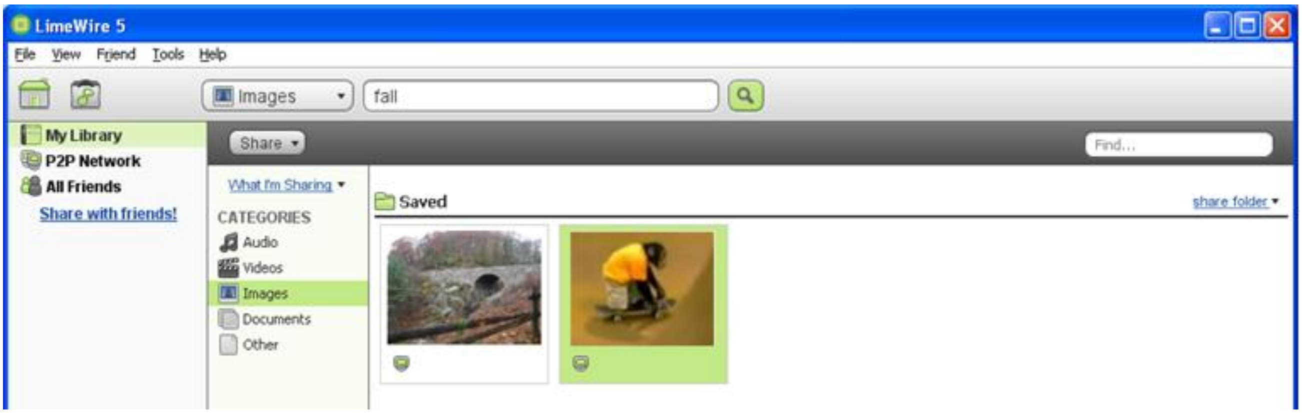


LimeWire 5

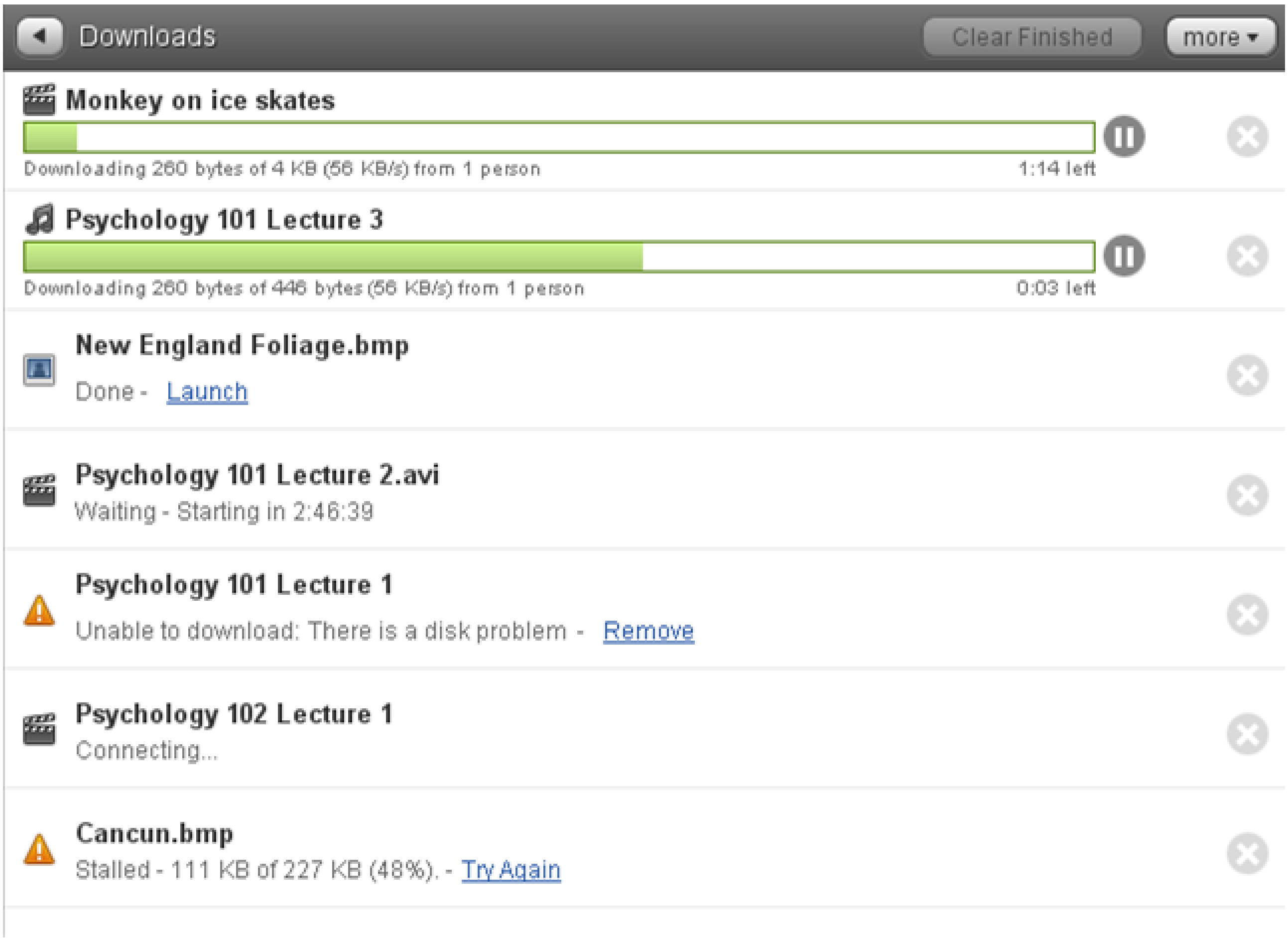
Monkey on a skateboard.bmp

Downloading 50 bytes of 1 KB (56 KB/s) from 0 people 0:19 left

Here's a thumbnail view of the monkey image in My Library:



Here's a list of Downloads with different progress:



Monkey on ice skates
Downloading 260 bytes of 4 KB (56 KB/s) from 1 person 1:14 left

Psychology 101 Lecture 3
Downloading 260 bytes of 446 bytes (56 KB/s) from 1 person 0:03 left

New England Foliage.bmp
Done - Launch

Psychology 101 Lecture 2.avi
Waiting - Starting in 2:46:39

Psychology 101 Lecture 1
Unable to download: There is a disk problem - Remove

Psychology 102 Lecture 1
Connecting...

Cancun.bmp
Stalled - 111 KB of 227 KB (48%). - Try Again

- Monkey on ice skates - Downloading
- Psychology 101 Lecture 3 - Downloading
- New England Foliage.bmp - Done. You can launch the file to check it out.
- Psychology 101 Lecture 2.avi - Waiting. LimeWire will attempt to download the file after a time period. You might receive this message if the computer who is sharing the file has a limit

on how many people can download at once so you have to wait your turn. Also, you might have reached a limit of how many downloads you can start at once.

- Psychology 101 Lecture 1 - Unable to download. Remove it and try searching again. The file you are trying to download might have a problem.
- Psychology 102 Lecture 1 - Connecting. Your computer is attempting to connect to the computer that has this file. If your computer can't connect, the download becomes Stalled.
- Cancun.bmp - Stalled. You should click Try again so your computer will again attempt to connect to a computer with the file. Between starting and finishing the download, the computer sharing the file might have shut down. You can either cancel the download (clicking on the x), try again or wait.

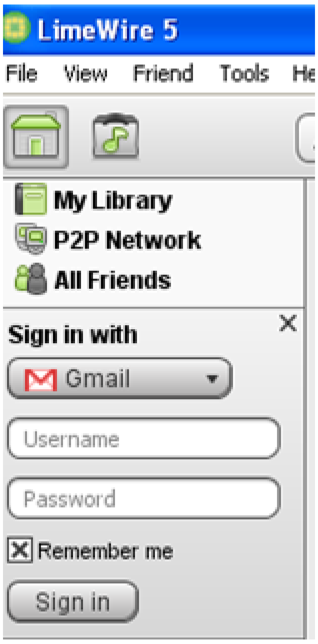
The Friends feature is a way for you to use an account to get a list of contacts who you can share files from My Library and, or chat.

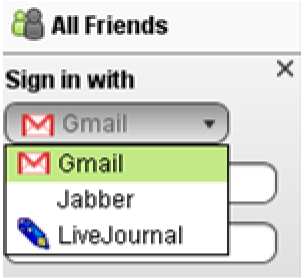
The accounts use an open standard (XMPP) which maintains lists of contacts per account.

Note: Signing in with an account and password through LimeWire doesn't give you, nor anyone else access to your email or your account information. Signing in with the email account only lets you see your contacts who you can then either share files with, or download files your friends are sharing with you.

You can add a friend to your contact two ways:

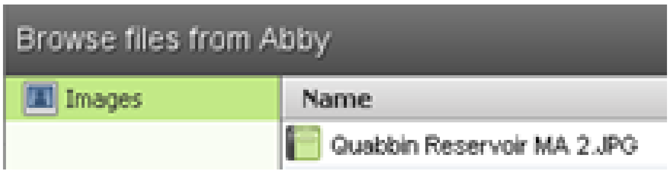
1. send and receive an email from a friend with your email account
2. add the friend's account through LimeWire. Then your friend must accept you as a friend through his account or through LimeWire. Similarly, you would need to accept a friend through LimeWire or your email account if he added you as a friend.

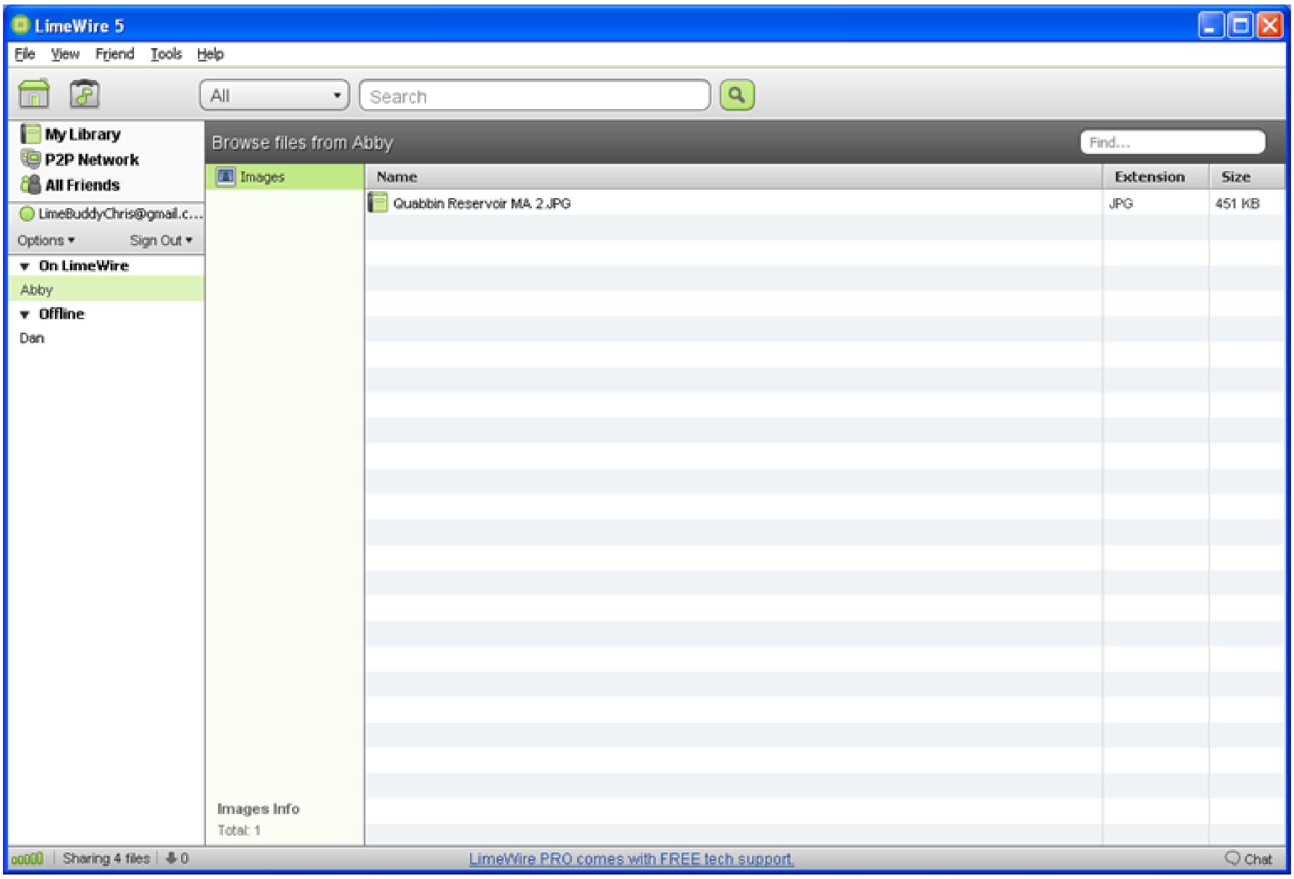




Browse Files from a friend

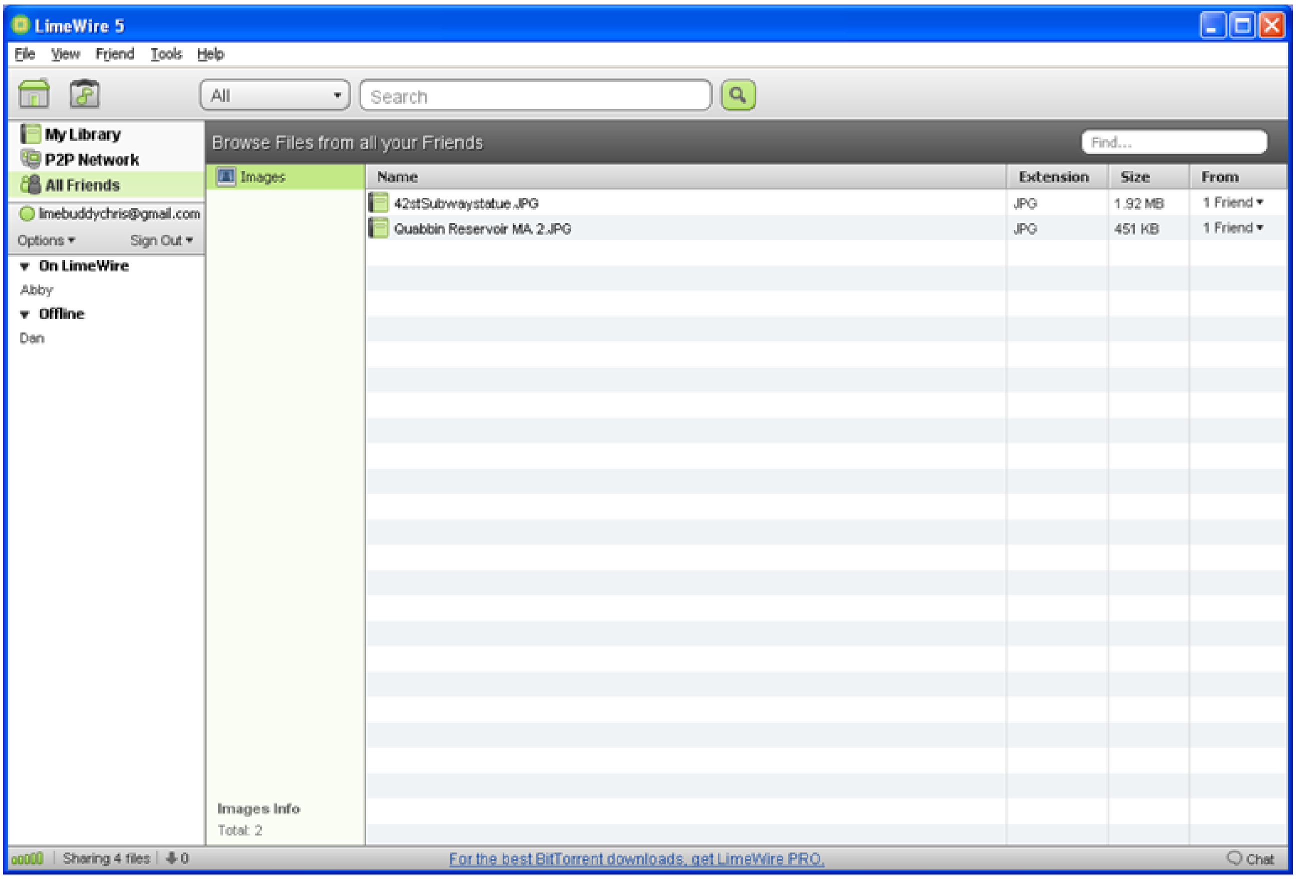
Here Abby shared an image, 'Quabbin Reservoir MA 2.JPG' which you downloaded as shown by the book icon:





Name	Extension	Size
Quabbin Reservoir MA 2.JPG	JPG	451 KB

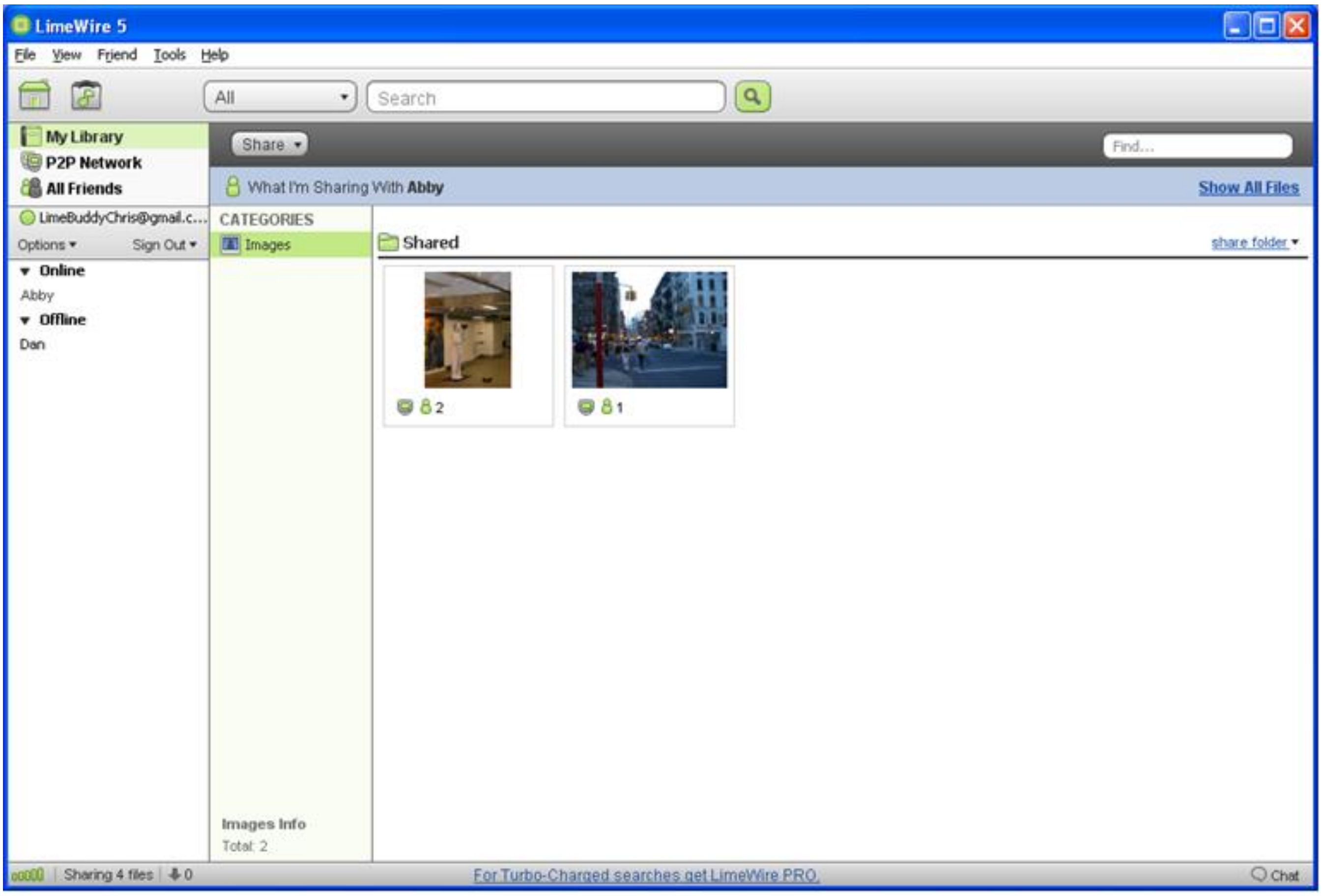
You can get a list of all the files your friends are currently sharing with you through All Friends:



Name	Extension	Size	From
42stSubwaystatue.JPG	JPG	1.92 MB	1 Friend ▾
Quabbin Reservoir MA 2.JPG	JPG	451 KB	1 Friend ▾

What I'm Sharing With

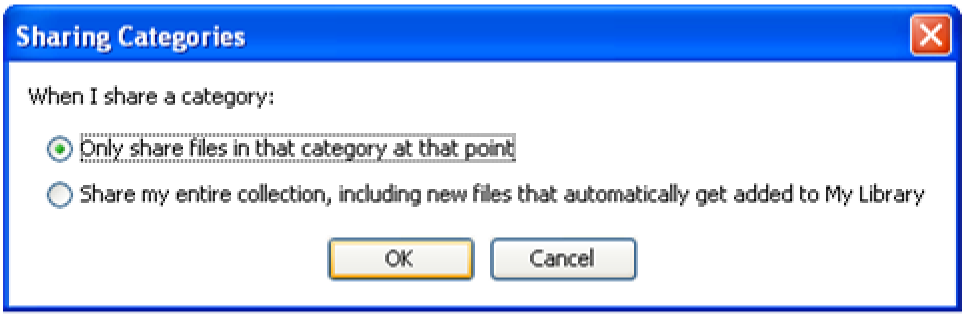
Here you can see you decided to share a picture of a man posing as a statue and a night scene at the Feast of San Gennaro with Abby.



Sharing Categories

You can share all the files in a category, either current snapshot of files, or the current snapshot plus future files. Through Options, you can select how to share all the files in your audio, images, video or documents categories.

Note: Changing your Sharing Categories setting makes all previous category shares with friends a snapshot share.



Sharing Categories

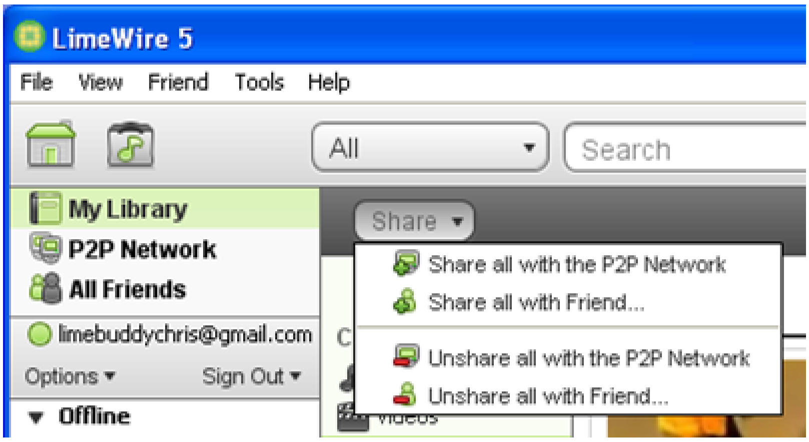
When I share a category:

● Only share files in that category at that point

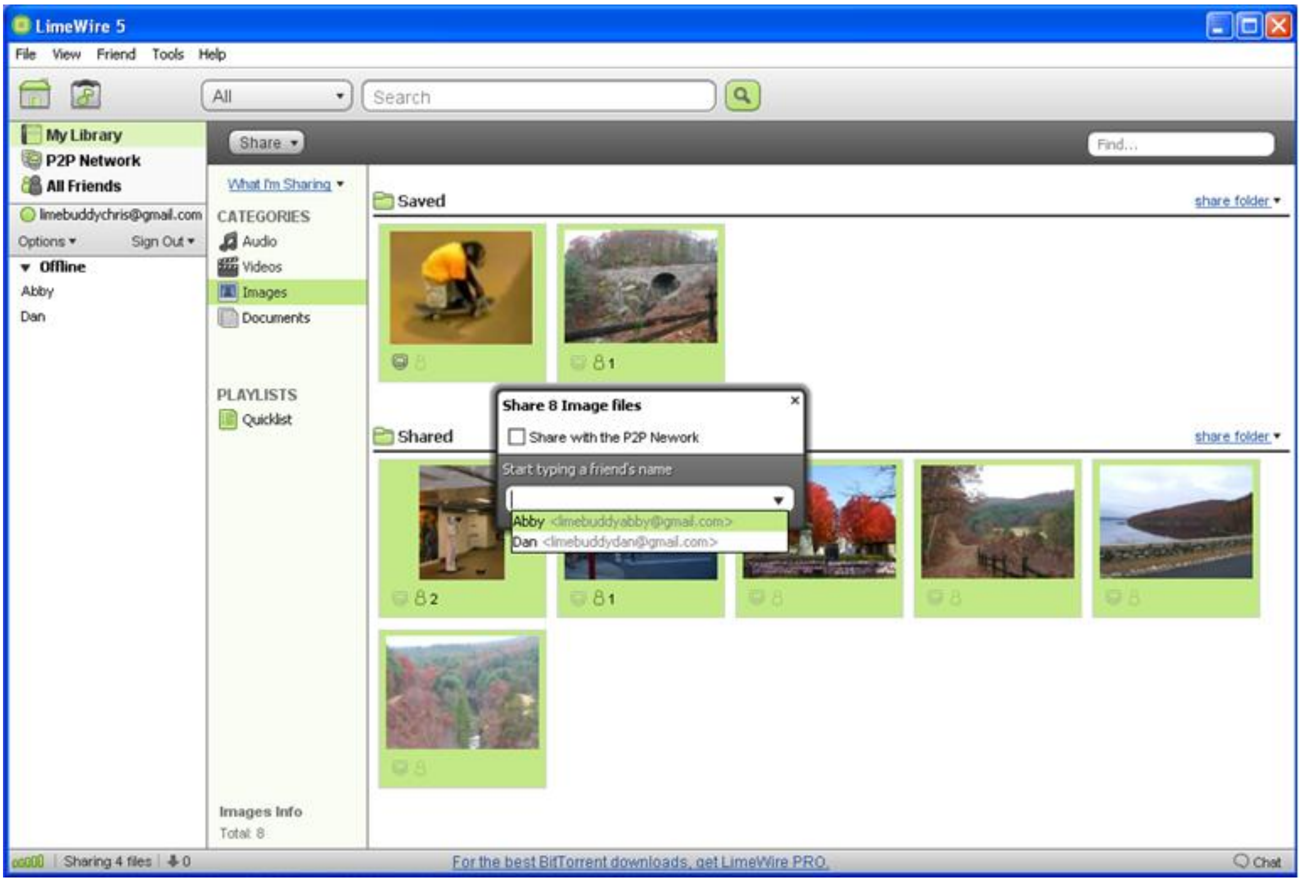
○ Share my entire collection, including new files that automatically get added to My Library

Snapshot

From My Library, select a file category (either Audio, Videos, Images or Documents), then click 'Share' and select 'Share all with Friend...'.



Then all the files in your image category are selected and the Share Widget appears to add friends:

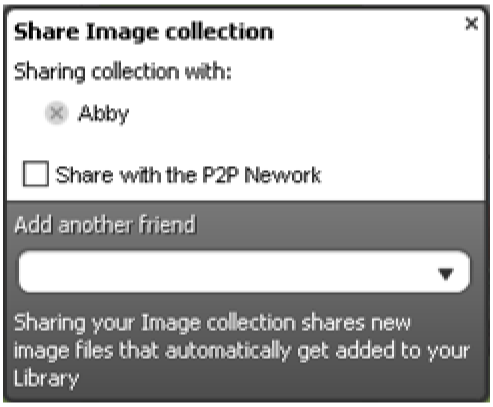


Snapshot plus future files

Additionally, you can share the current and future files you add to My Library in your audio, image or video category with your friends.

For example, you decide to share your image category with Abby, along with future downloads. After you find and download another image of the Quabbin, whether from a friend of the P2P Network, that file is automatically shared with Abby.

To share all files in a category including new files, you need to make a change in the Tools > Options. Then from My Library, highlight a file category, then click 'Share' and select 'Share all with a Friend...' to get the collection share widget:



Share Image collection

Sharing collection with:

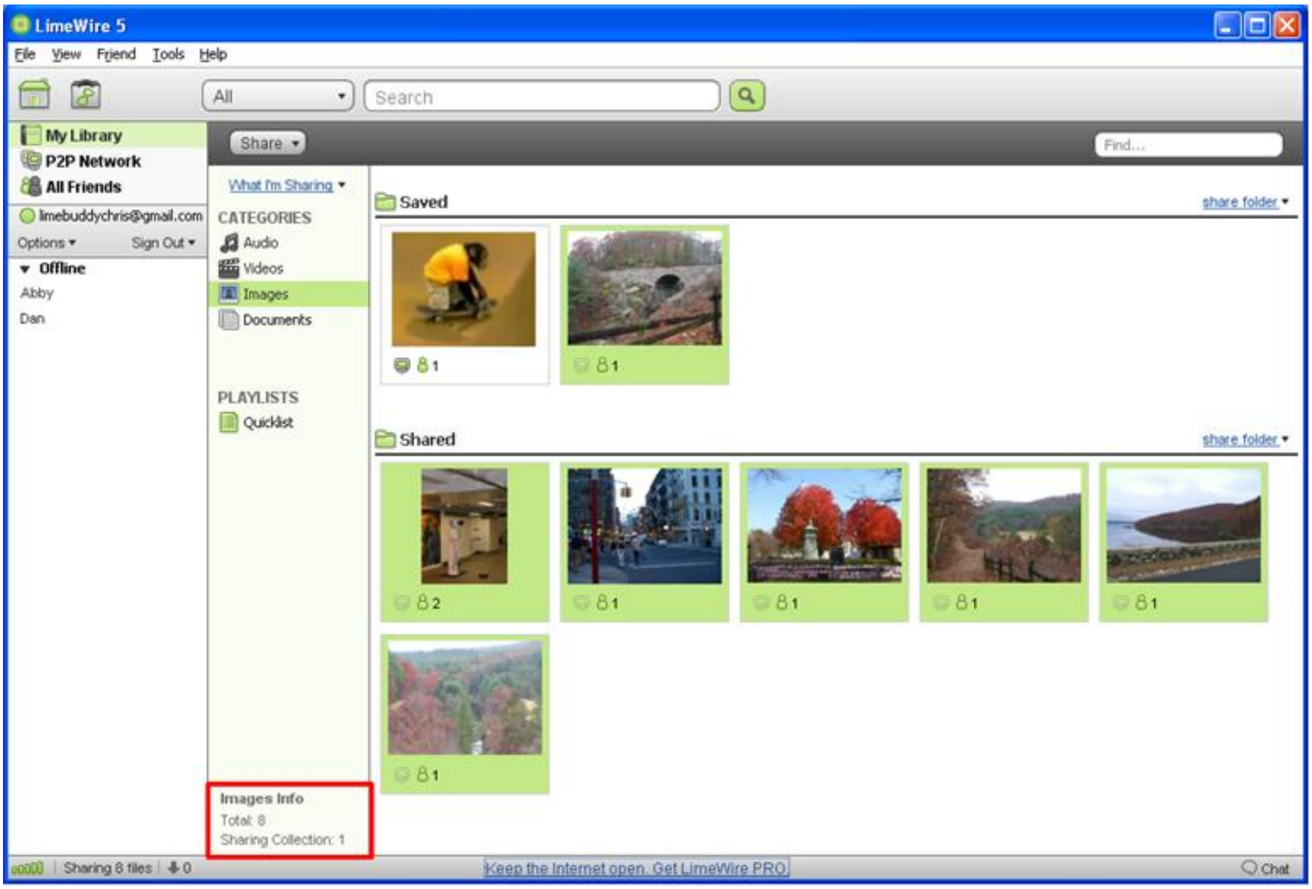
Abby

□ Share with the P2P Nework

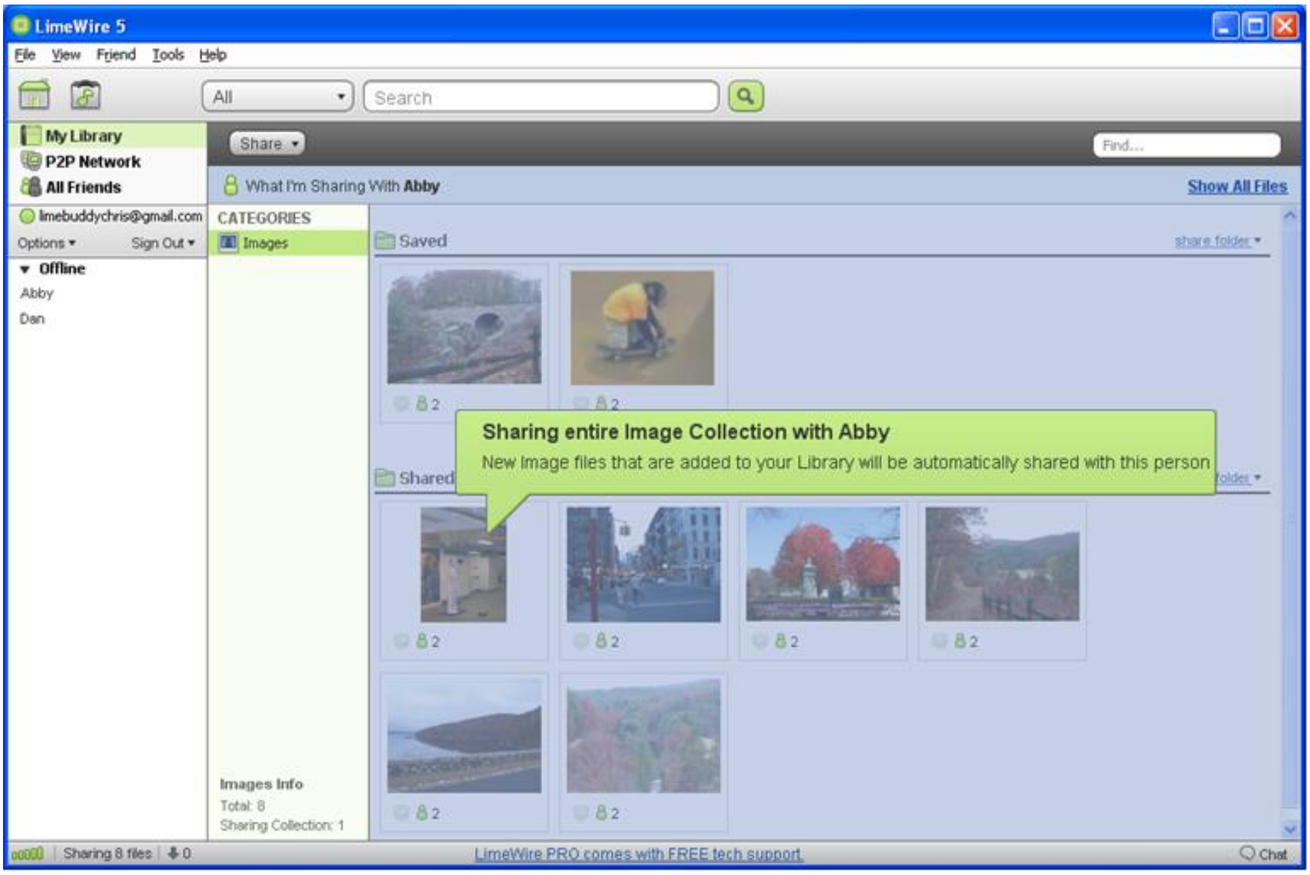
Add another friend

Sharing your Image collection shares new image files that automatically get added to your Library

To show you are sharing future files, My Library states 'Sharing Collection: 1':



Also, if you see 'What I'm Sharing' with a friend through My Library, you get a notification you are sharing future files:



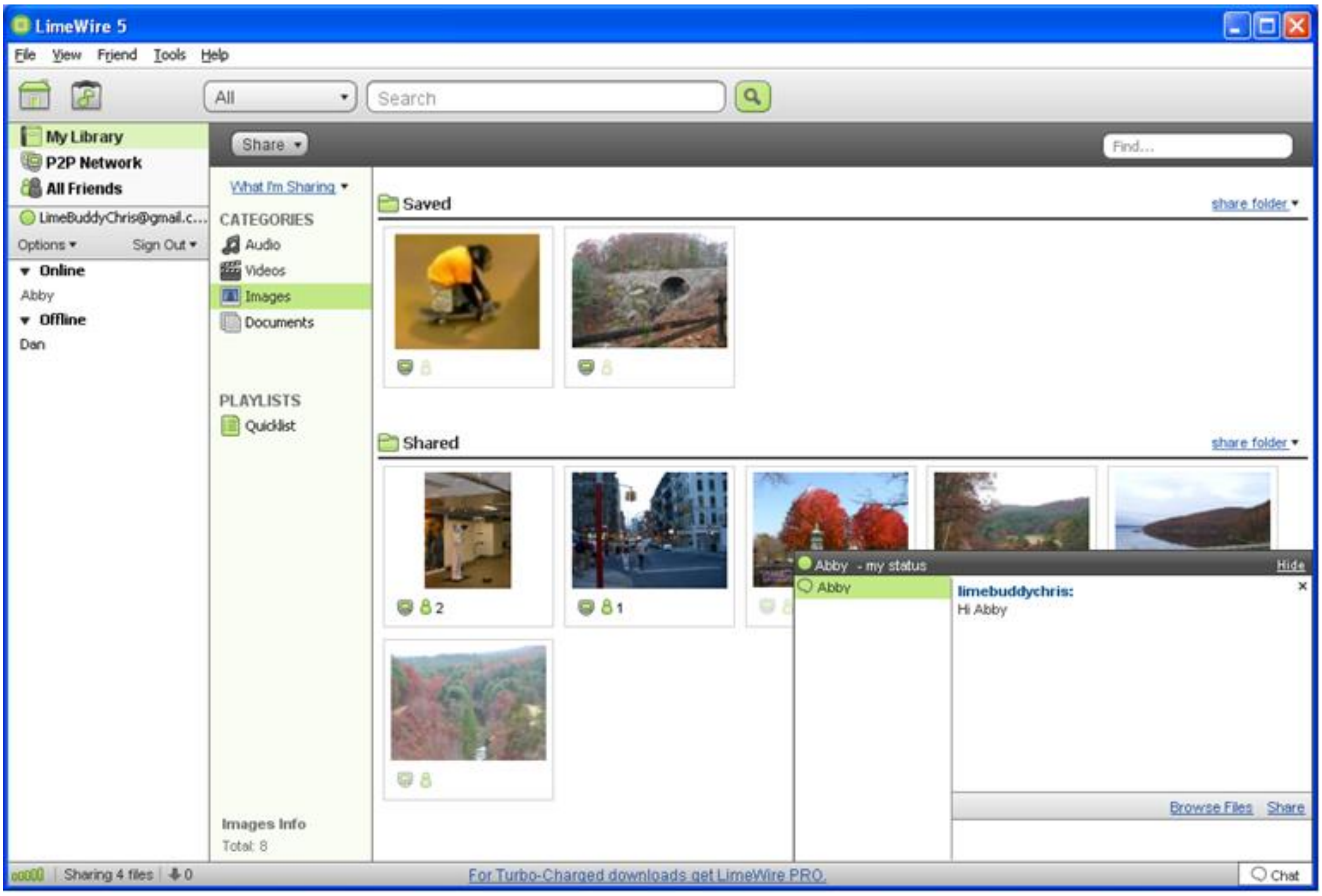
Sharing entire Image Collection with Abby

New image files that are added to your Library will be automatically shared with this person

Chat

You can chat with friends whether they are 'On LimeWire' or 'Online'. A friend could be signed into their account, for example checking their email, without being 'On LimeWire'. You can use LimeWire to chat with your friend even if he isn't 'On LimeWire'.

Highlight a friend from the Sidebar, right click (control click) and select 'Chat':



limebuddychris:
Hi Abby

Supported accounts

LimeWire supports the following accounts:

Google's Gmail(tm)* webmail service
Hot-Chilli
Jabber.ru (r),
JabberES
Jabberim
LiveJournal (r)
MacJabber.de

Domain names

For the active list of Jabber serices, see http://www.jabber.org/web/Services

Enter the following in the Domain name depending on your account:

- binaryfreedom.info
- darkdna.net
- im.apinc.org
- im.flosoft.biz

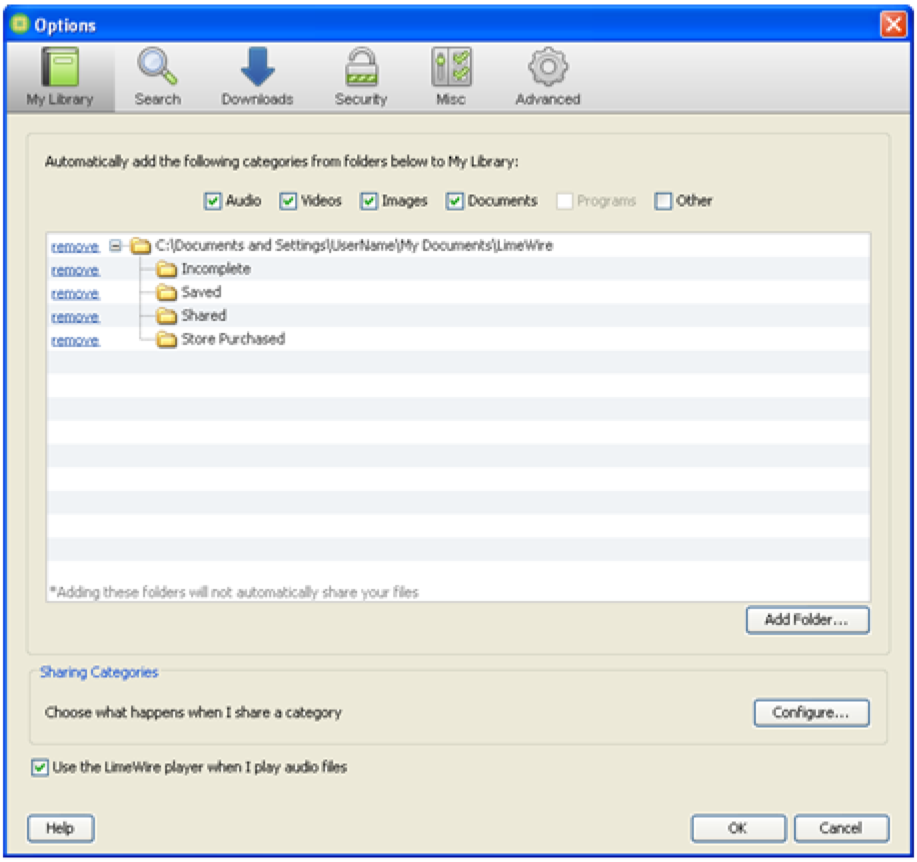
- im.thiessen.it
- jabber.ccc.de
- jabber.hot-chilli.net
- jabber.org
- jabber.rootbash.com
- jabber.se
- jabberes.org
- jabster.pl
- macjabber.de
- programmer-art.org
- swissjabber.ch

My Library

My Library is the central location to view or share files with LimeWire. These are files you either told LimeWire to watch, or downloaded from the P2P Network or the LimeWire Store. Files and folders you add to My Library aren't automatically shared with the P2P Network unless you previously shared them.

You can add files or folders to My Library if you select File > 'Add File to Library...' or 'Add Folder to Library...' in LimeWire.

Click on Tools > Options (Preferences > Options), My Library to see which files and folders you want LimeWire to manage:



Automatically add the following categories from folders below to My Library:

☑ Audio ☑ Videos ☑ Images ☑ Documents □ Programs □ Other

remove C:\Documents and Settings\UserName\My Documents\LimeWire
remove Incomplete
remove Saved
remove Shared
remove Store Purchased

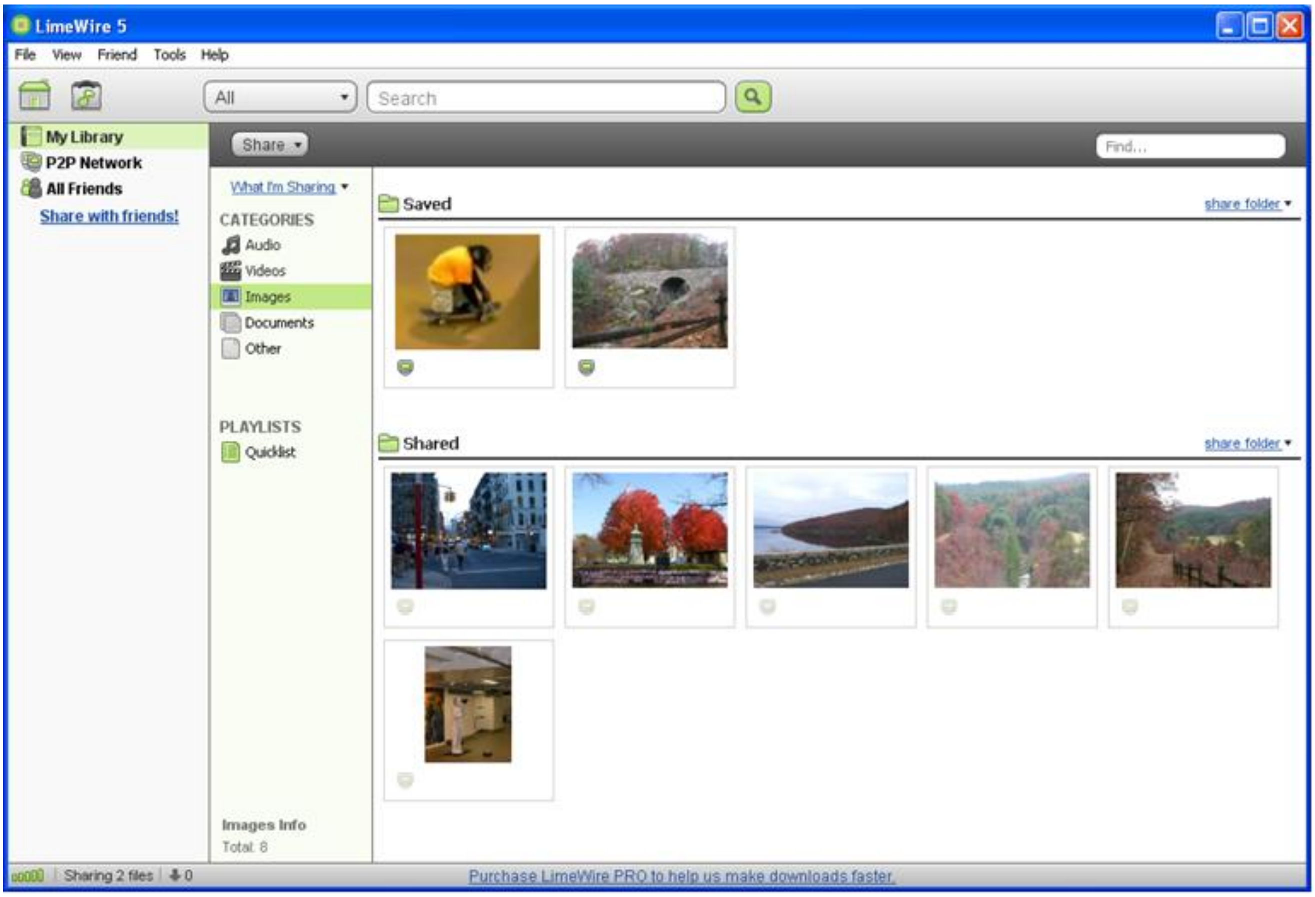
*Adding these folders will not automatically share your files

Sharing Categories

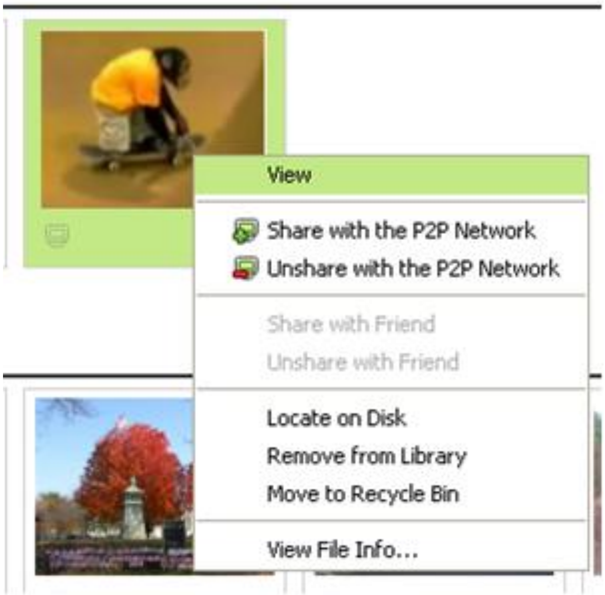
Choose what happens when I share a category

☑ Use the LimeWire player when I play audio files

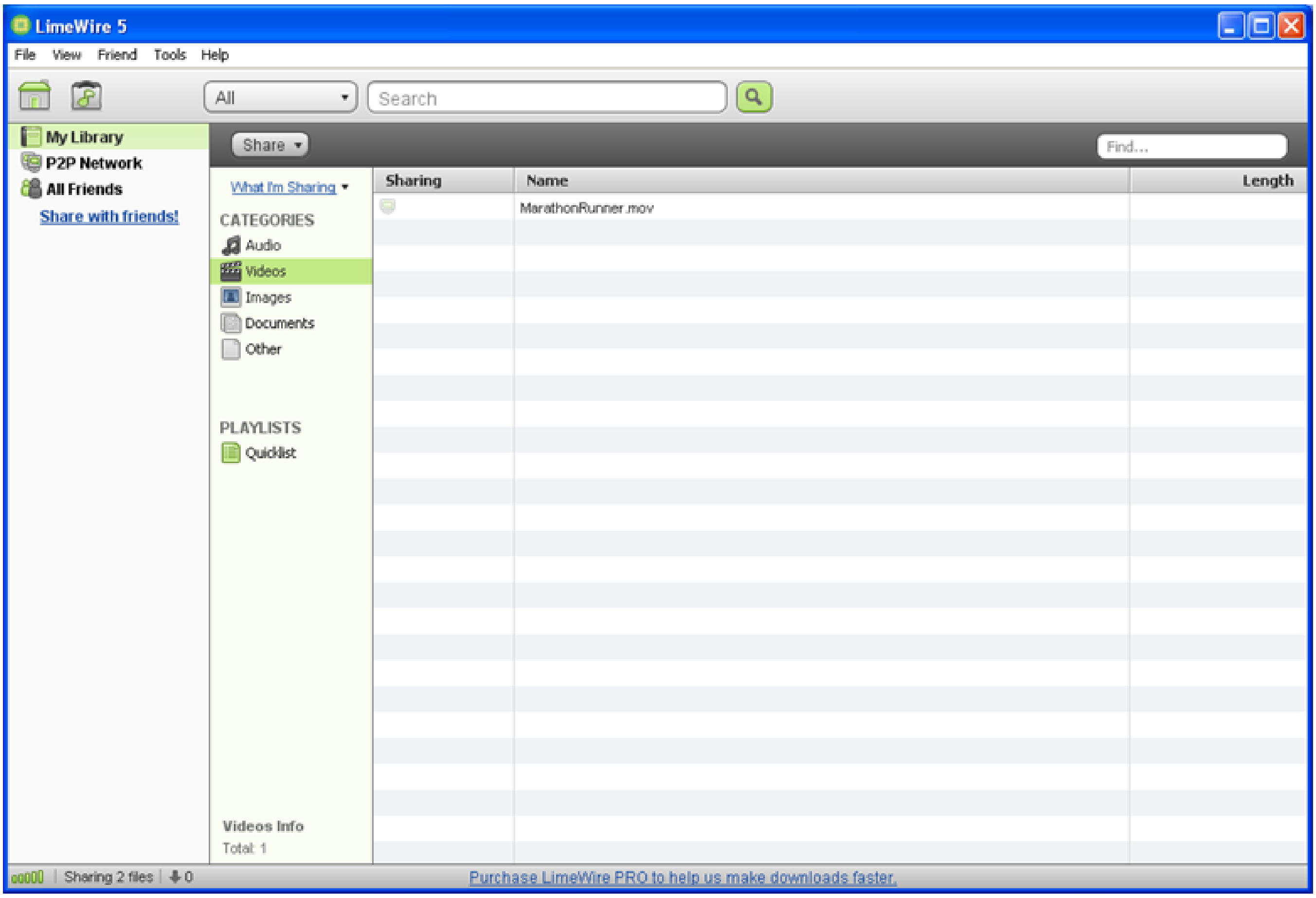
Here are files in the Images category of My Library:



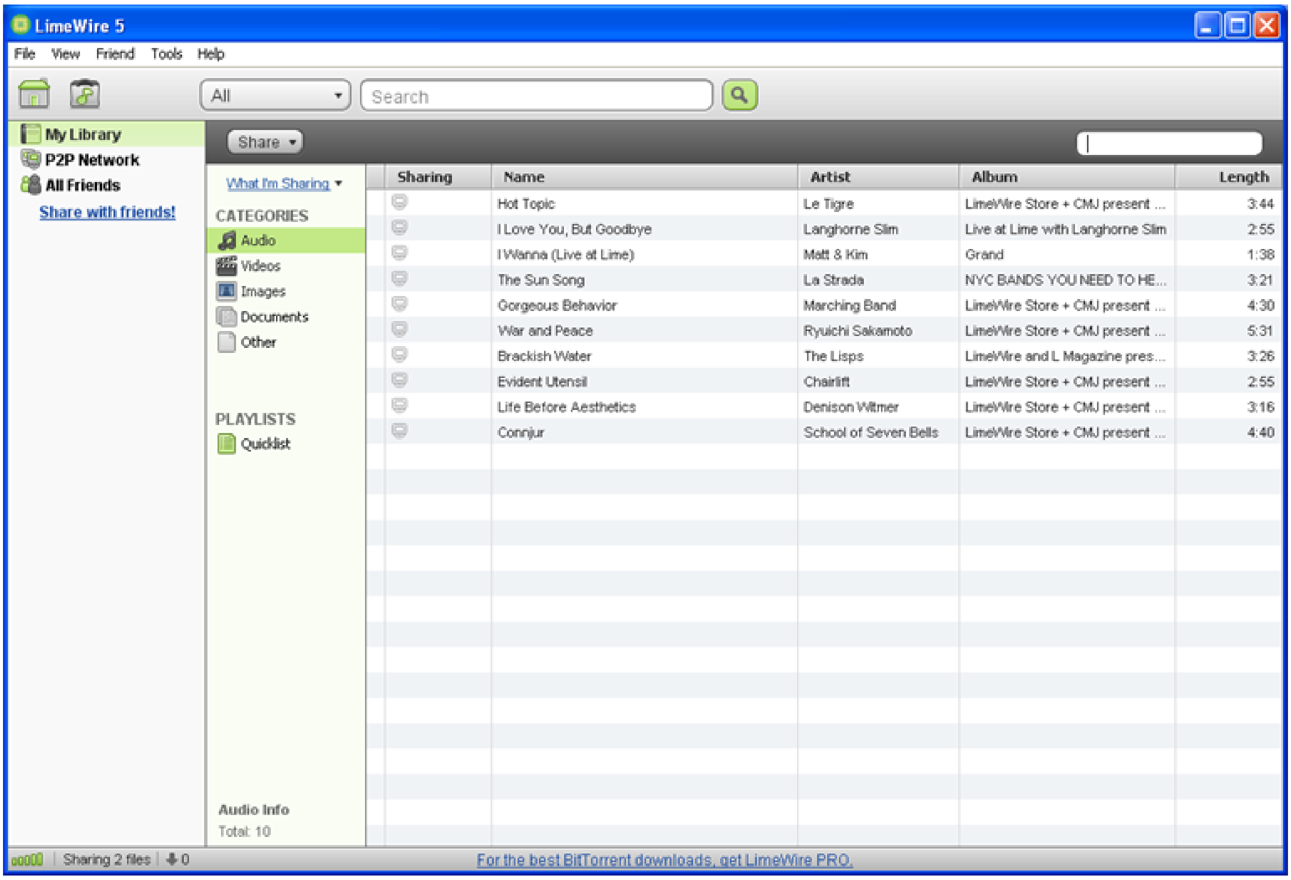
If you right-click (Control-click) you can get more options:



Here's the Videos category of My Library:



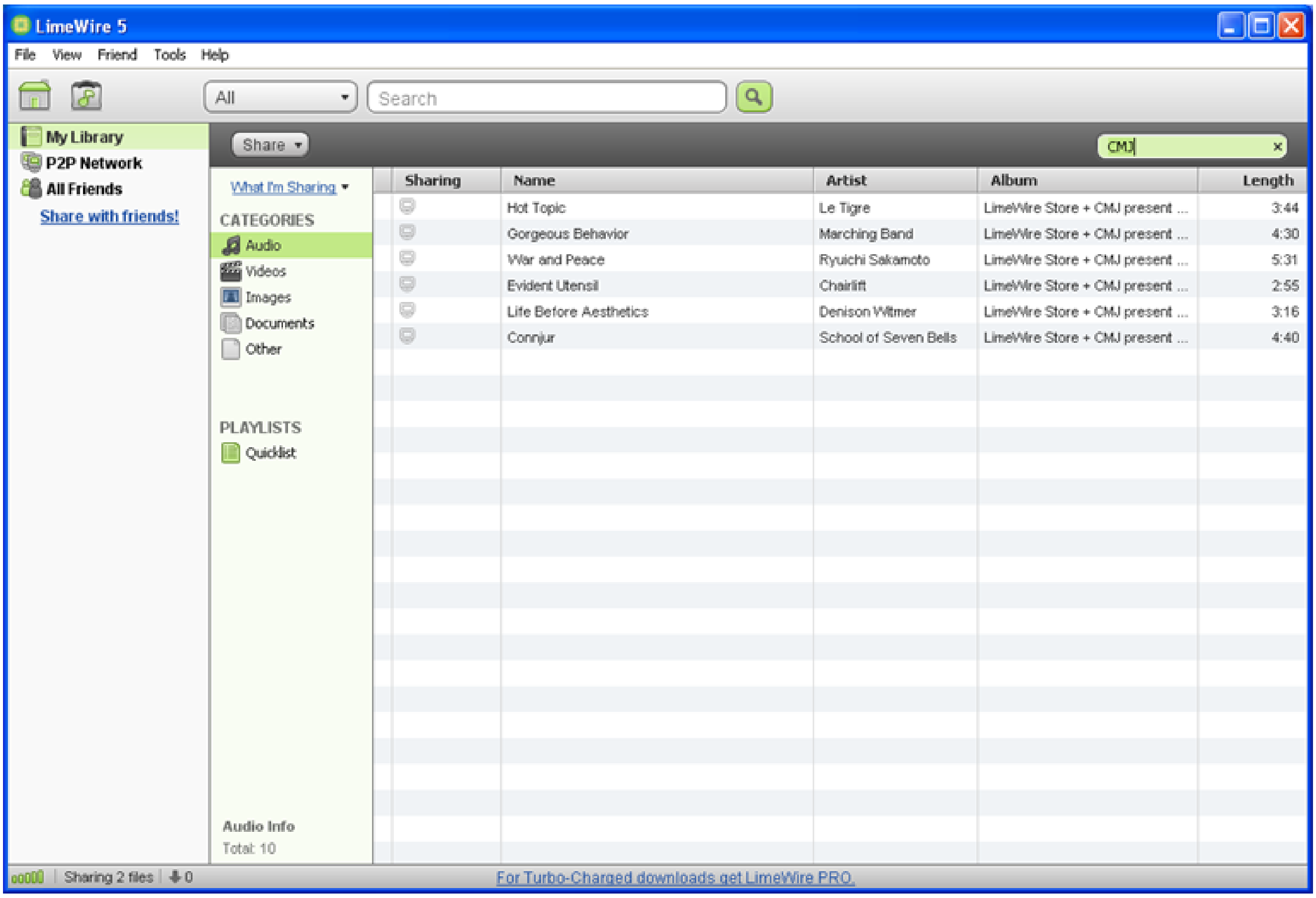
Here are audio files in My Library:



Sharing	Name	Artist	Album	Length
	Hot Topic	Le Tigre	LimeWire Store + CMJ present ...	3:44
	I Love You, But Goodbye	Langhorne Slim	Live at Lime with Langhorne Slim	2:55
	I Wanna (Live at Lime)	Matt & Kim	Grand	1:38
	The Sun Song	La Strada	NYC BANDS YOU NEED TO HE...	3:21
	Gorgeous Behavior	Marching Band	LimeWire Store + CMJ present ...	4:30
	War and Peace	Ryuichi Sakamoto	LimeWire Store + CMJ present ...	5:31
	Brackish Water	The Lisps	LimeWire and L Magazine pres...	3:26
	Evident Utensil	Chairlift	LimeWire Store + CMJ present ...	2:55
	Life Before Aesthetics	Denison Witmer	LimeWire Store + CMJ present ...	3:16
	Connjur	School of Seven Bells	LimeWire Store + CMJ present ...	4:40

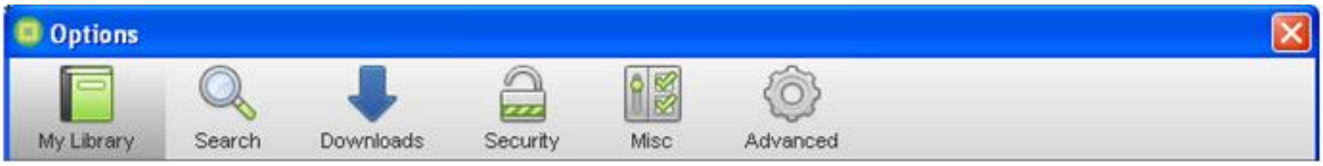
You can narrow down files shown in My Library to display only files in My Library which match the filter. The filter searches information known about the files, including information listed in 'View More Info...'.

For example, filtering for 'CMJ' shows:



Sharing	Name	Artist	Album	Length
	Hot Topic	Le Tigre	LimeWire Store + CMJ present ...	3:44
	Gorgeous Behavior	Marching Band	LimeWire Store + CMJ present ...	4:30
	War and Peace	Ryuichi Sakamoto	LimeWire Store + CMJ present ...	5:31
	Evident Utensil	Chairlift	LimeWire Store + CMJ present ...	2:55
	Life Before Aesthetics	Denison Witmer	LimeWire Store + CMJ present ...	3:16
	Connjur	School of Seven Bells	LimeWire Store + CMJ present ...	4:40

Options



My Library

Use My Library to set which folders you want LimeWire to look for files to manage.

Note: Files in My Library aren't shared automatically.

Once LimeWire adds a file to My Library, you have a central location to find files on your computer. Here you can share files with the Person to Person (P2P) Network your Friends, or both.

Click Add Folder to add folders to scan.

Additionally, you can control which file categories LimeWire adds to My Library.

File category

LimeWire groups files into categories based on the files' extensions. The categories are:

- audio (may only have sound)
- documents (may have words, numbers, images and sometimes sounds and videos)
- images (may have pictures)
- programs (may have computer instructions; for example LimeWire is a program)
- other (Since there are thousands of file extensions used with computers, it's impossible for LimeWire to group every file extension into a type. This category includes extensions LimeWire isn't sure where to put.)
- video (may have sound, pictures and video)

For example, 'sailboat.JPG' is the name of an image file. The file extension, 'JPG', is a common extension for files with pictures so LimeWire puts all files with the extension 'JPG' (and 'jpg') into the image file category.

You can click Manage in the Tools > Options > Advanced > Files option to see the file categories for each file extension.

File extension

The file extension is the letters and, or numbers after the dot in a file name. For example, the file extension for the file name 'sailboat.JPG' is 'JPG'.

File extensions help you figure out what category the file is (audio, document, image, program or videos).

Sharing Categories

You can share a category of files in My Library (Audio, Images or Videos) in two ways:

- Snapshot
- Snapshot plus future files in that category

A snapshot are all the files you currently have in that category. This is a quick way to share all files of a particular category in all folders in My Library.

On the other hand, a snapshot also includes any files you may add to My Library in the future. For example, when share your image collection with a friend, then all images which LimeWire lists in My Library are shared with him. Then if you download an image of a 'Monkey on a skateboard', then the monkey file is automatically shared with that friend. Also, if you add an image of a cute cat to My Library, then it too is shared with your friend who you shared the image collection.

LimeWire player

You can either use the LimeWire player when you launch audio files from LimeWire, or use another player on your computer.

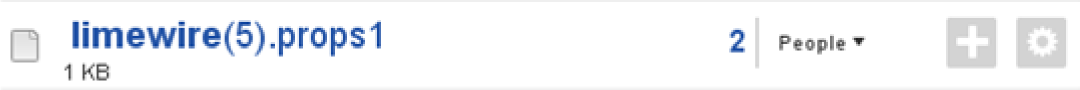
Search

Search bar

You can set which file category to search. For example, if you only want to search for images, you can set that here.

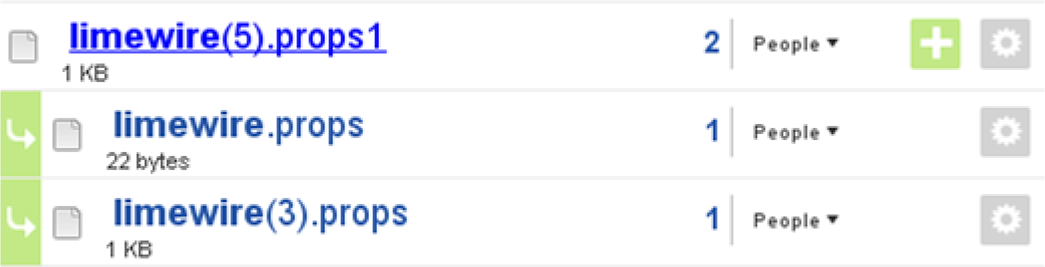
Also, you can Group similar search results together. Based on the available data, LimeWire groups search results that appear to be similar. For example, if the network has two files, Simon_Short_Story.txt and Simon.txt (both have similar content, like they are the same size and the same file extension), then when you search for "Simon Short Story", both results are grouped.

For example, the search result for 'LimeWire' returned:



limewire(5).props1
1 KB
2 People

When you click on the plus sign, you see two additional files which are similar.



limewire(5).props1
1 KB
2 People

limewire.props
22 bytes
1 People

limewire(3).props
1 KB
1 People

Downloads

Saving

Before LimeWire starts downloading a file, it checks if there is a file already with the same name. Checking this option tells LimeWire to add a number to avoid replacing the existing file with the new file.

For example, instead of replacing 'sailboat.JPG', LimeWire saves the download file as 'sailboat(1).JPG'.

Share files downloaded from the P2P Network with the P2P Network

This option gives other people the chance to download files you downloaded from the P2P Network. When you search using LimeWire you are actually searching the Gnutella network of computers. These computers create a person to person (P2P) connection of computers to allow you to share files.

Another download option is having LimeWire update your iTunes Library.

Also, LimeWire keeps a list of your recent downloads in File > Recent Downloads.

Security

Warning Messages

Unsafe Categories

In order to protect users from unknowingly downloading potentially harmful programs, LimeWire doesn't let you search for, or share programs by default. Known programs, like 'LimeWire' can be safe to download, however many times virus hide inside programs. Therefore, we recommend your don't download programs.

Additionally, to protect your personal information, LimeWire doesn't share Documents by default with the P2P Network. However, you can share documents with Friends. (See Manage Extensions for a list of document file extensions.)

Filtering

Don't show adult content in search results

Select this option to prevent common adult search results from appearing.

Additionally, you can add terms to Filter Keywords... to further restrict search results. For example, if you added 'ime' to the Filter Keywords... and then searched for 'limewire', you wouldn't see any search results with the letters 'ime'.

The Filter File Extensions... prevents showing results with file extensions which could include viruses or cause harm to your computer.

Misc

You can set which language you'd like to see LimeWire's text use.

Notifications

A notification includes a dialog box that appears in the lower right corner of your monitor when you receive a chat message from a friend.

Friends and Chat

Like Google's Gmail(tm)* webmail service LimeWire uses the XMPP open standard for the Friends feature.

The Friends feature lets you send text messages to your friends, or to share files directly with friends. Your email account and messages are not accessible through the Friends feature and the password is encrypted to protect your privacy.

* Gmail is a trademark of Google Inc. Google Inc is not a sponsor or partner of Lime Wire LLC.

Advanced

Files

File Extensions

Here you can see how LimeWire groups file extensions into categories. For example, LimeWire puts all files with the file extension 'txt' into the Documents category.

Also, you can control what file extensions LimeWire recognizes for loading into My Library. If, for example, you decide to exclude MS Word documents from loading into your library, then remove the check.

Setting file extensions is a great way to control what files you share. For example, if you have sensitive information in MS Excel files, you might want to restrict sharing 'xls' and 'xlsx' extensions.

Download Folders

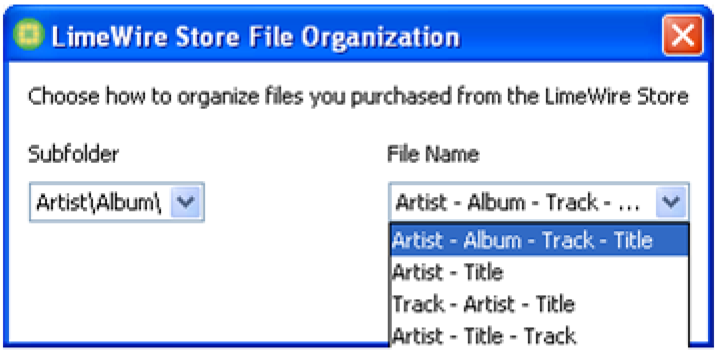
You can set where downloaded files are stored on your computer for Audio, Documents, Images, Programs, Other, or Video.

LimeWire Store

Configure file naming

You can decide how files purchased from the LimeWire Store are saved onto your computer. LimeWire could create a folder structure with the name of the artist and, or the album, and various file name possibilities (artist/album/title/track number, etc.).

For example, if you set:



LimeWire Store File Organization

Choose how to organize files you purchased from the LimeWire Store

Subfolder: Artist\Album\

File Name: Artist - Album - Track - ...

Then when you use LimeWire to download "Connjur" by the artist "School of Seven Bells" through the LimeWire Store (from the album "LimeWire Store + CMJ present CMJ08: 28 Years, 28 Tracks"), the file is saved:

... \Store Purchased\School of Seven Bells\LimeWire Store + CMJ present CMJ08_ 28 Years, 28 Tracks\School of Seven Bells - LimeWire Store + CMJ present CMJ08_ 28 Years, 28 Tracks - 01 - Connjur.mp3

iTunes

Transfers

Downloads

Uploads

An upload is a file on your computer another person is downloading.

The upload bandwidth is how much data you want to allow someone to download from you. Like adjusting how wide a window is open to control how much air goes out, the greater you increase the upload bandwidth, you give others more opportunity to download data. Older and, or slow Internet connection computers might want to decrease the upload bandwidth to improve computer performance.

Connection Speed

Setting your network connection speed is critical to allow fast searches and downloads from the P2P Network.

A Broadband connection typically means you have a fast Internet connection. On the other hand, a Dial-up connection is typically a slower connection where your modem makes a call through the telephone lines into an Internet service provider (ISP).

System

File Associations

You can tell your computer to use LimeWire to open .magnet or .torrent files when using the Windows operating system.

Startup and Shutdown

Here you can tell LimeWire to run when your computer starts. Also, you can set if you want to minimize LimeWire to the System Tray when you hit X (the 'Close' button in the upper right of the program), or to exit.

Bugs

Bug reports list areas in the code where a problem traveled and helps software developers fix mistakes.

Tell me about Beta updates

Here you set if you want LimeWire to notify you about Beta updates. Beta versions of LimeWire are work-in-progress releases of the software with the latest features and bug fixes. The goal of a beta release is for a small sample of users to find bugs, or to report what they like or don't like. LimeWire uses the beta feedback to improve the next wide release.

Super Really Advanced

These settings are quite technical and difficult to explain to a broad audience without some confusion. Therefore, since we expect only people already familiar with these options to make change here, we won't document.

Firewall

Proxy

Network Interface

Performance

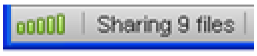
BitTorrent

Filtering

Spam

Share

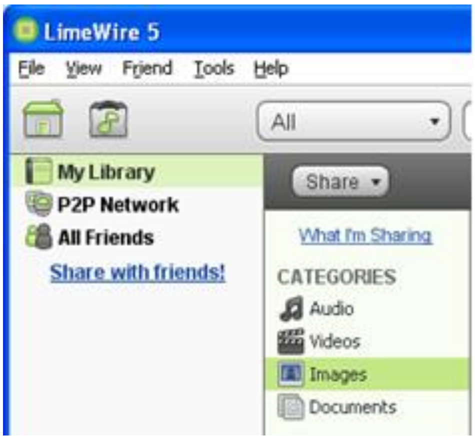
Sharing files is what makes the P2P Network. The more shares, the bigger the network. The bottom left corner of LimeWire lists the number of files you are sharing:



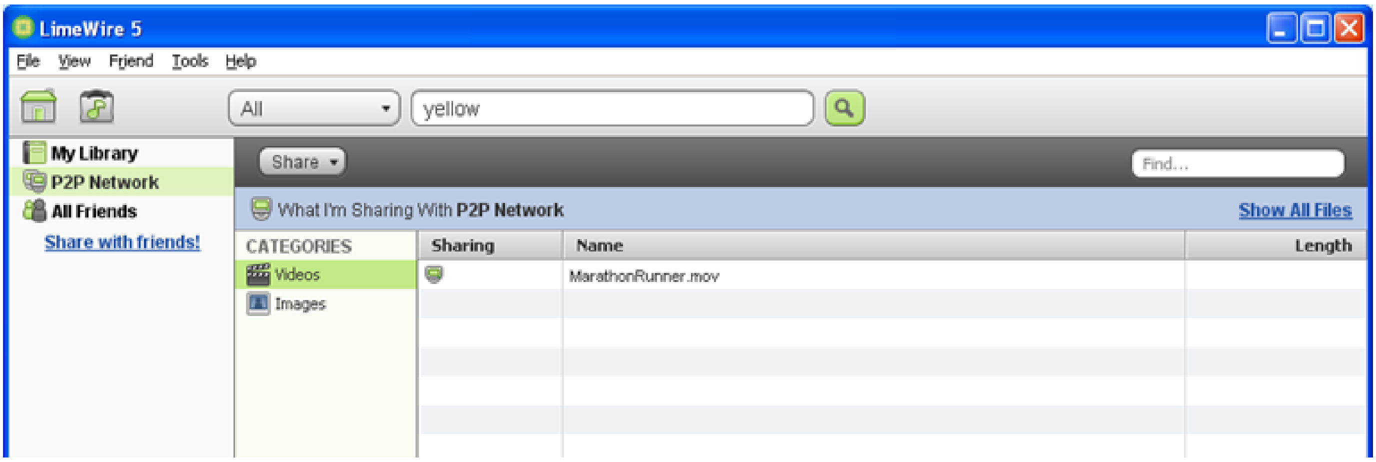
My Library is the central location to manage files and folders. You can add folders to My Library using Tools > Options, My Library.

Note: Once you add files or folders to My Library, the files aren't automatically shared. You can use the Share Widget to select which files to share. Additionally, you can use the Share Widget to stop sharing a file.

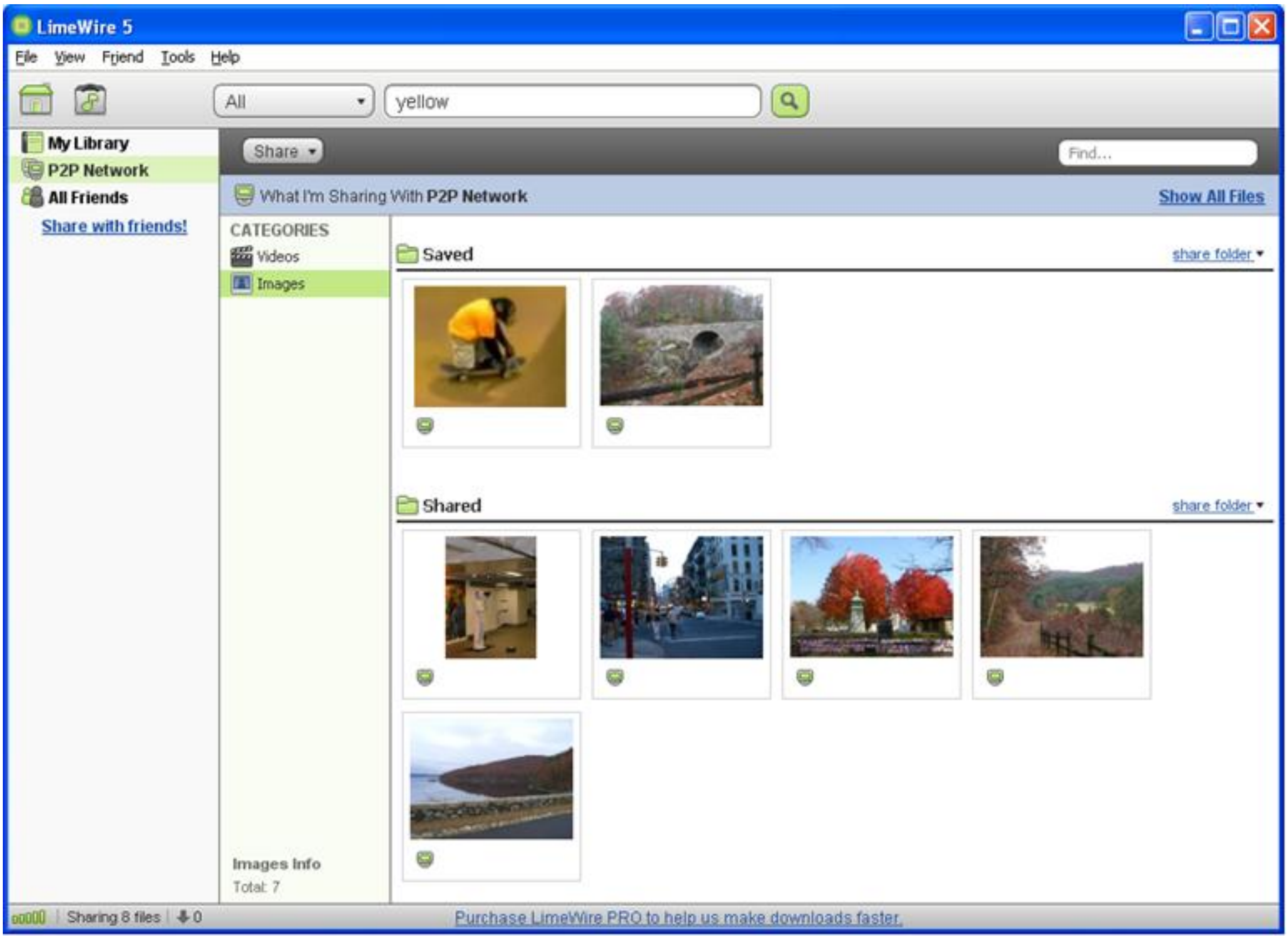
Click on My Library and then 'What I'm Sharing'.



Here is a list of the videos category of what you are sharing with the P2P Network:



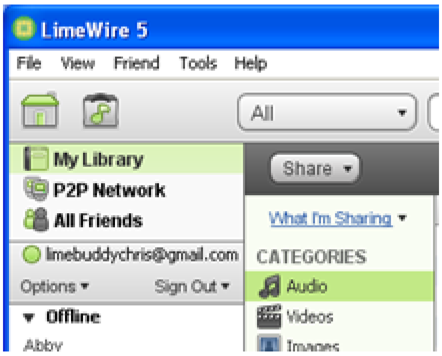
Here is a thumbnail view of the images category of what you are sharing with the P2P Network:



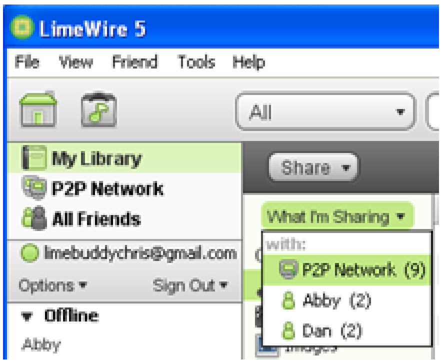
Friends

If you are signed into Friends, you additionally see the friends icon (👤) and your list of friends.

Click on My Library and then 'What I'm Sharing'.



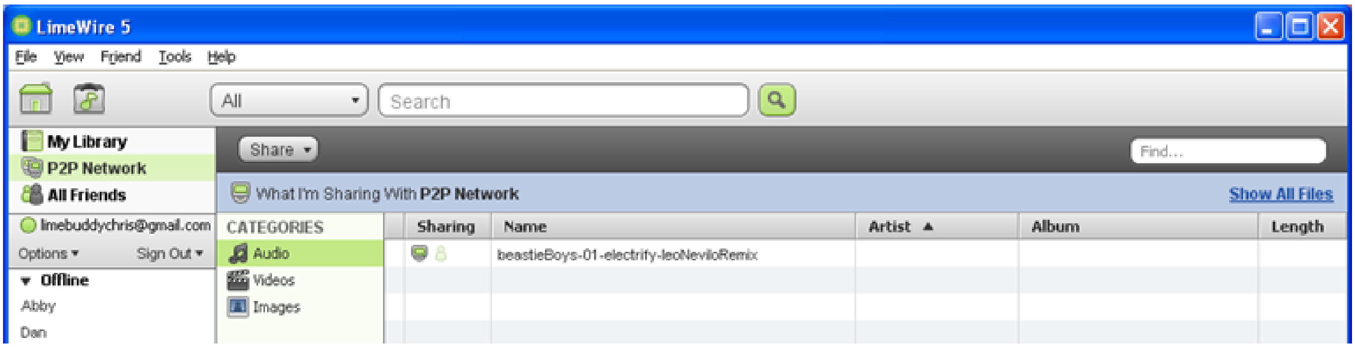
Then select either 'P2P Network' or a friend to see which files you are sharing:



A file is shared if the share icon is enabled. The share icon can either be:

- disabled; the file is not shared with the P2P Network
- enabled; the file is shared with the P2P Network
- disabled; the file is not shared with any friends
- 1 enabled; the file is shared with one friend

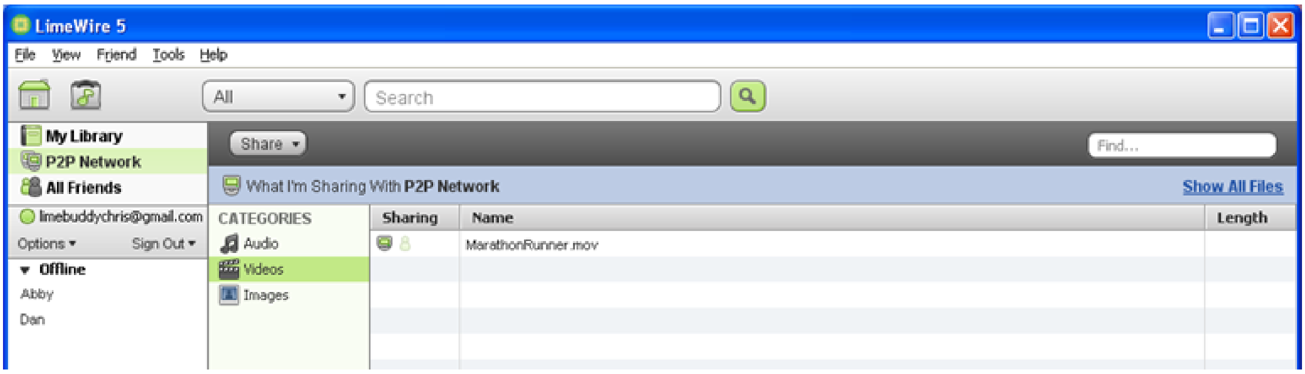
You could for example, share a file with the P2P Network and not a friend. Here you are sharing a Creative Commons audio file with the P2P Network but not with any friends:



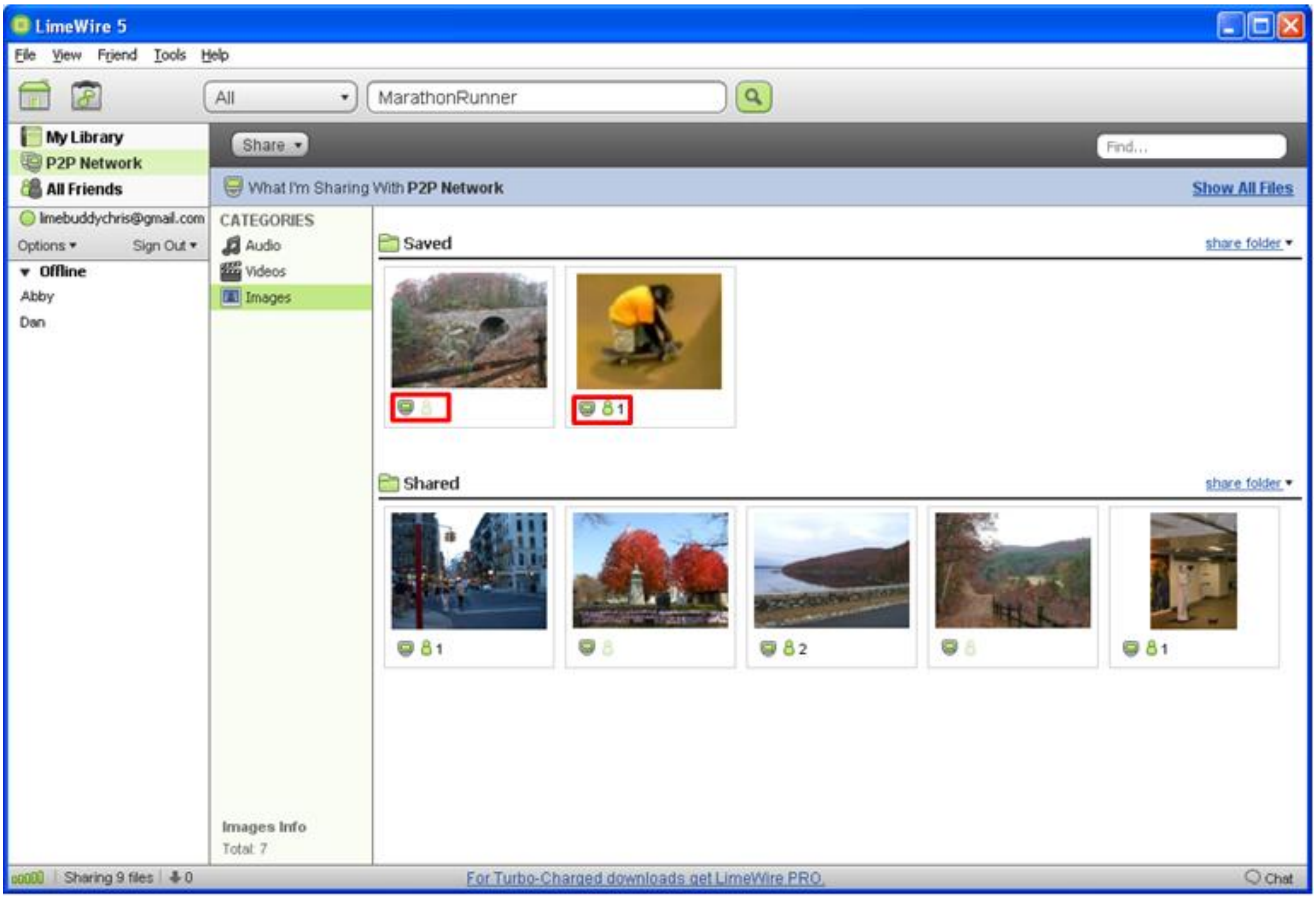
What I'm Sharing With P2P Network

Sharing	Name	Artist ▲	Album	Length
	beastieBoys-01-electrify-leoNeviloRemix			

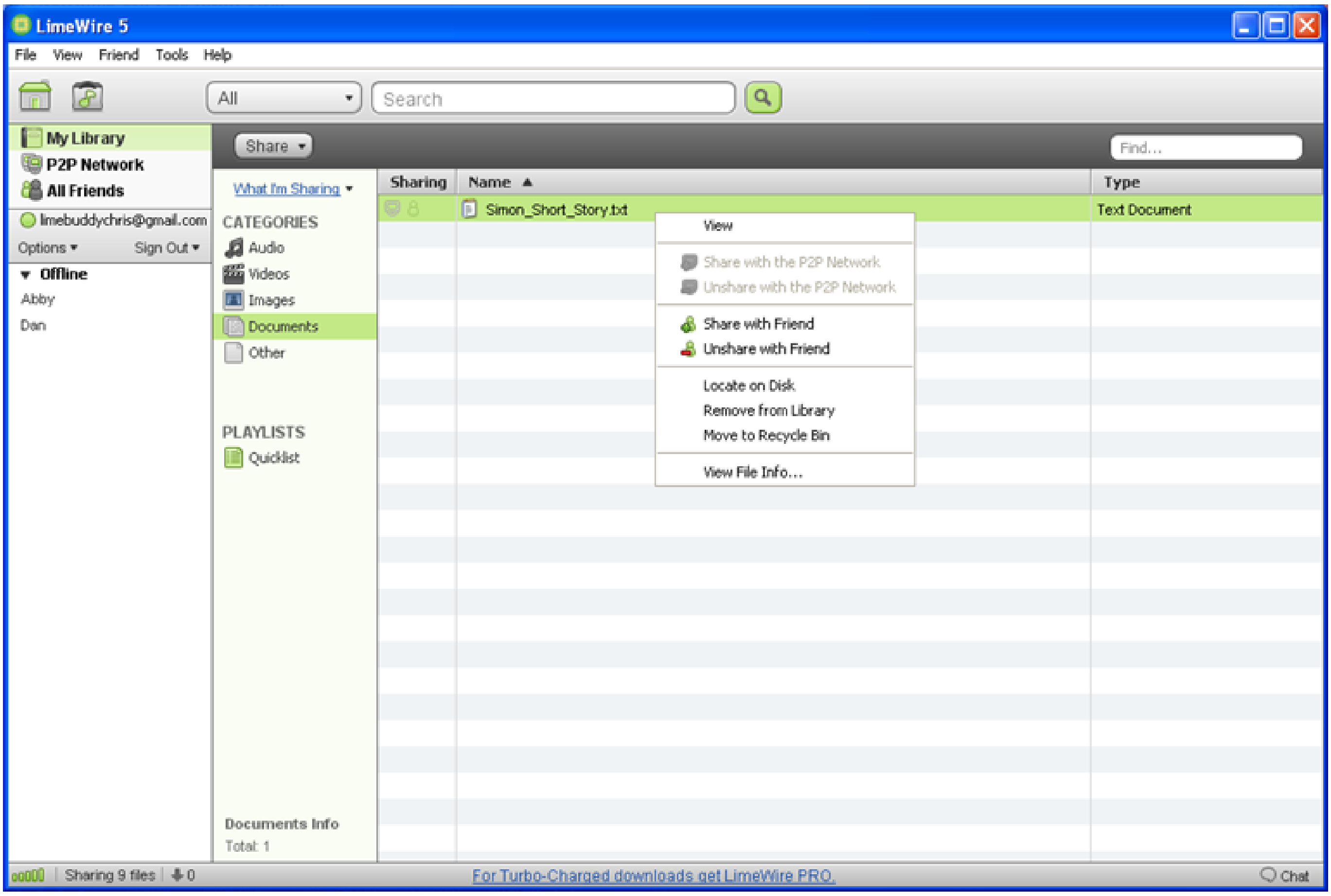
Here you are sharing a video of you running your first marathon:



Here you are sharing images. In the first case you are sharing with only the P2P Network and in the second case you are sharing with both the P2P Network and a friend.

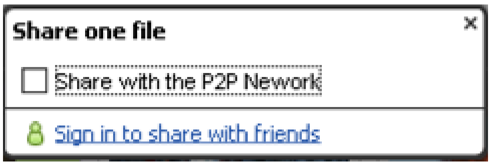


Documents are not shared by default:



Share Widget

The Share Widget lets you control if a file is shared with the P2P Network and, or with friends.

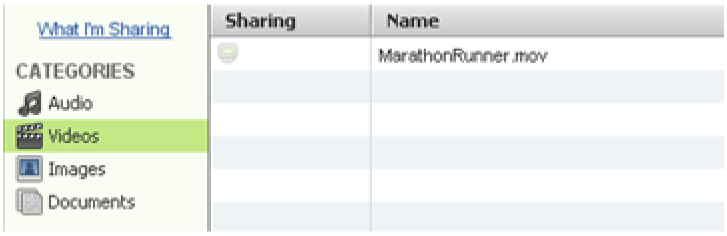


The P2P Network is a group of person to person users who create the Gnutella Network. When you are searching the network, you are searching for files hosted by users like you on the P2P Network.

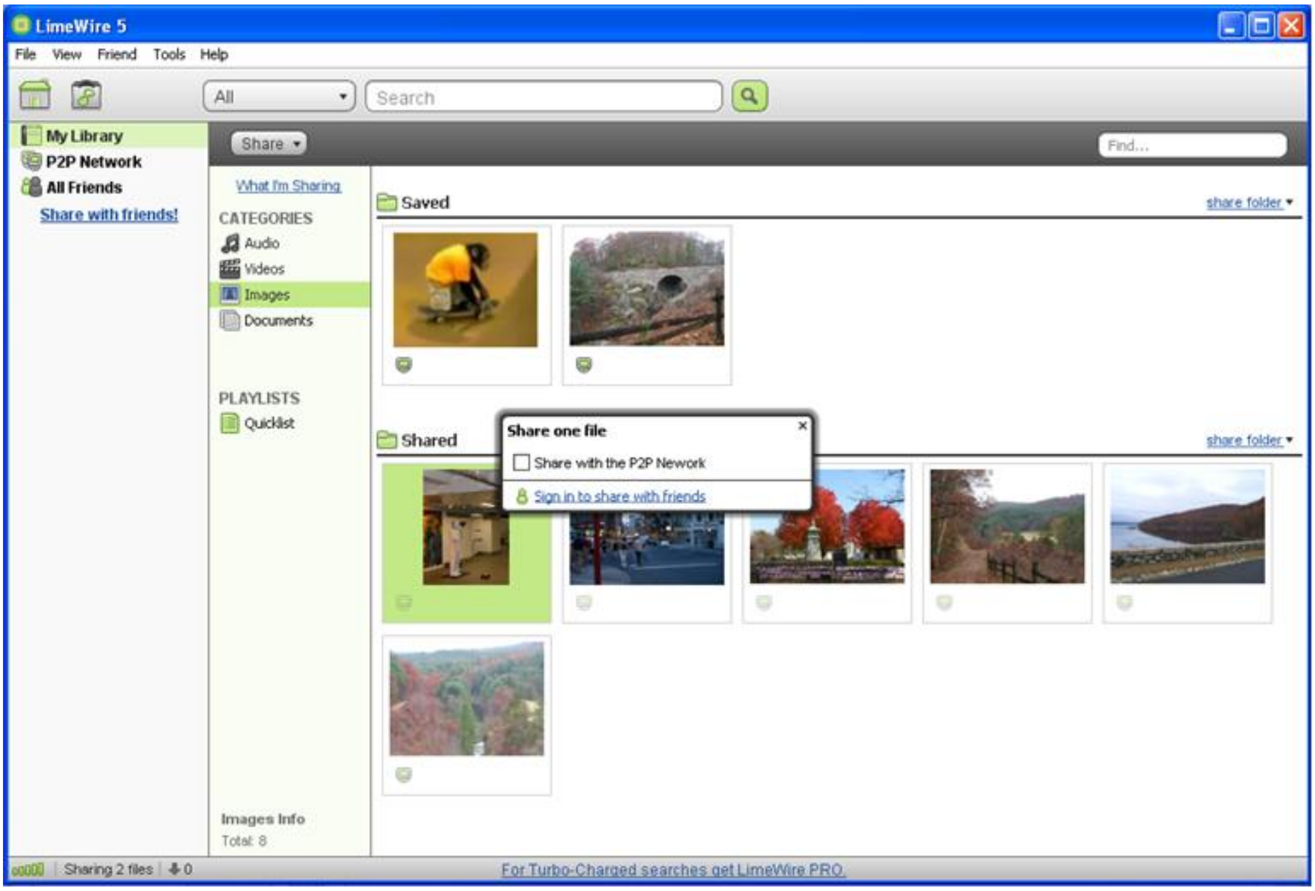
You can access the Share Widget through the file's share icon which can either be:

- disabled; the file is not shared
- enabled; the file is shared

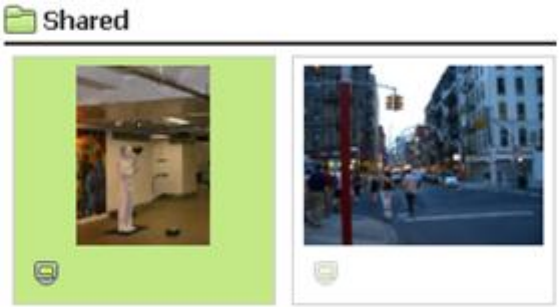
Here is the share icon as seen in the videos category of My Library:



Click the share icon to show the Share Widget:



Once you share a file, the share icon is enabled as shown for the subway statue file.



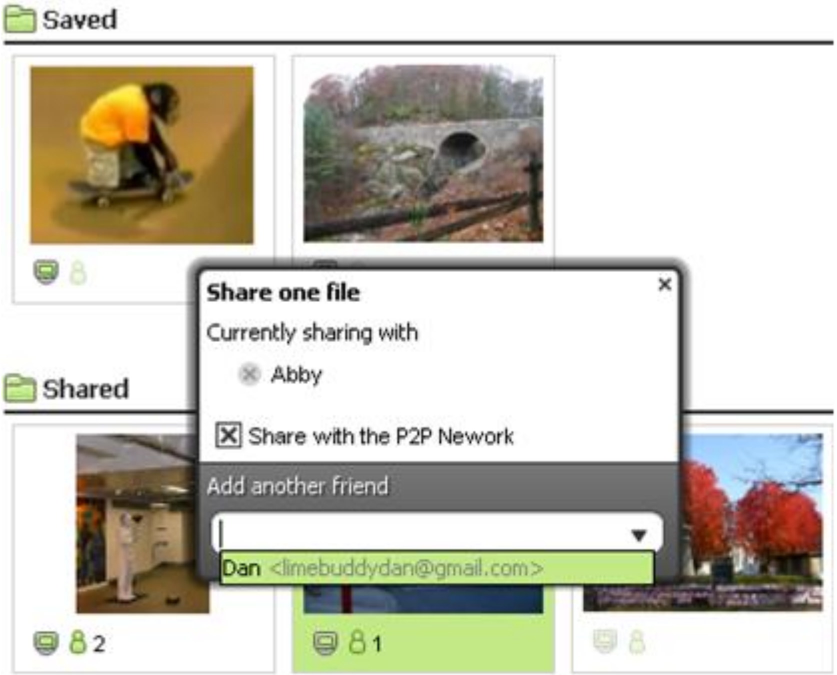
Friends

When using the Friends feature, the Friend share icon appears near the file and means:

- 👤 - not shared with any friends
- 👤1 - shared with one friend
- 👤2 - shared with multiple friends

Note: the number lists the number of friends you are sharing with so it can grow beyond two.

When you click on either the P2P Network or Friends share icons, you get the Share Widget to manage sharing with both the P2P Network and, or friends. Here, you are sharing an image with the P2P Network and Abby, and haven't yet shared it with Dan:



Forensic examination of LimeWire 5.1.3

Default installation path (WindowsXP)

LimeWire is by default installed at "C:\Program Files\LimeWire". In this folder, you find the program "core files".

The files containing the settings is found at "C:\Documents and Settings\ <USER>\Application Data\LimeWire". (It's among these data you find what you want :-))

In this folder you - among other files - find the following files of interest:

- limewire.props
- downloads.dat
- version.props
- library5.dat
- fileurns.cache

limewire.props

The "limewire.props" file contains the "properties" of the system. There is a lot of good information in this file, e.g.

- RECENT_DOWNLOADS=
  Shows the recent downloaded files and their paths
- HARD_MAX_UPLOADS=
  This entry is ONLY present, if the user has changed the number of "upload slots". If the entry is "0", then sharing is disabled
- UPLOAD_SPEED=
  This entry is ONLY present, if the user has changed the uploadspeed
- DIRECTORY_FOR_SAVING_FILES=
  Contains the path to the folder used for saving downloaded files. This file will often contain the files that automatically are shared
- CLIENT_ID=
  Contains a unique SHA1 value to identify the user
- TOTAL_UPTIME=
  Total uptime of the client in seconds

- LAST_SHUTDOWN_TIME=
  UNIX time/date stamp

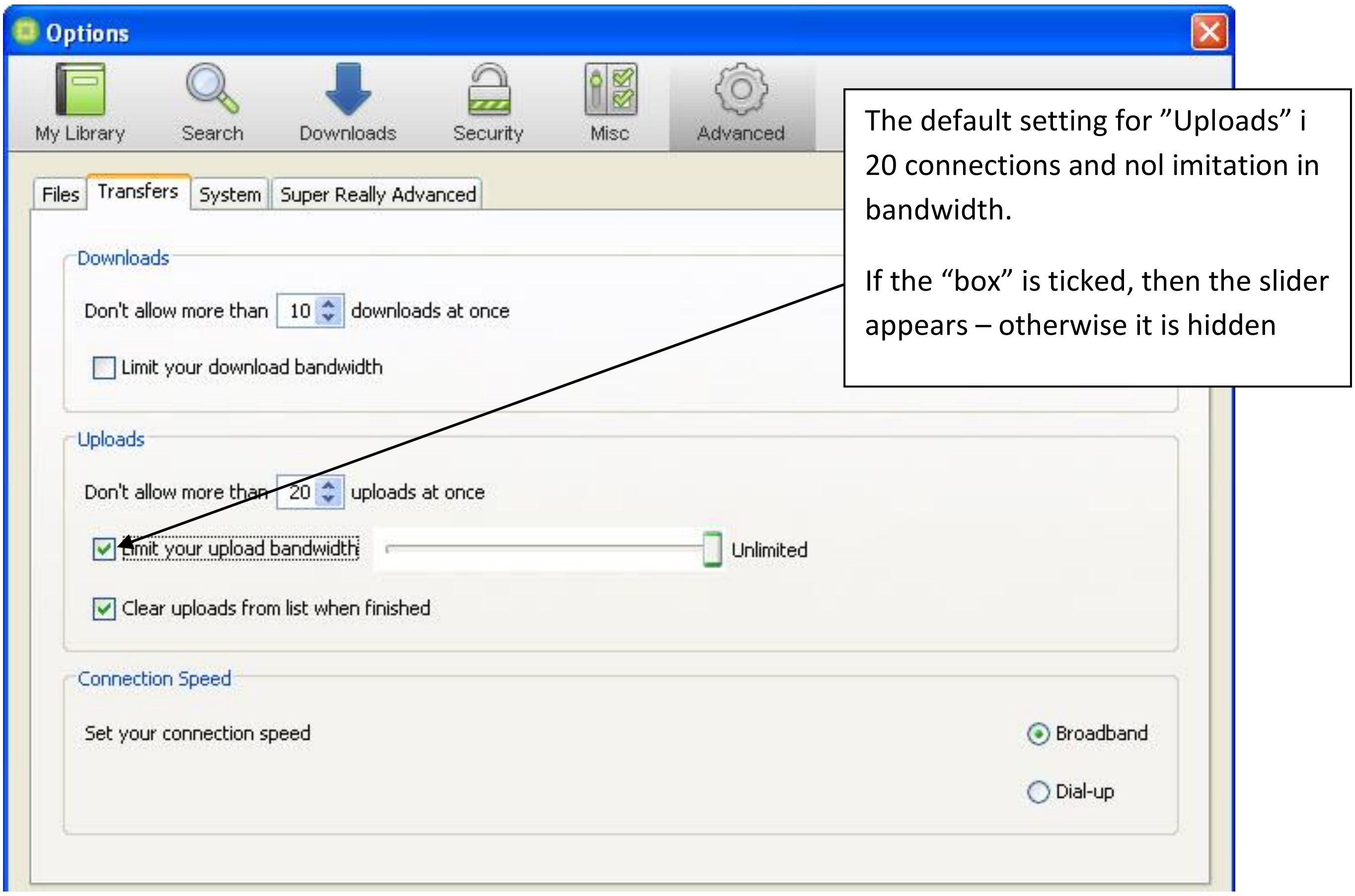
- TOTAL_CONNECTION_TIME=
  Total connectiontime to the network in miliseconds

- LAST_UPDATE_TIMESTAMP=
  UNIX time/date stamp

- LAST_SHUTDOWN_TIME=
  UNIX time/date stamp

“limewire.props” is constantly overwritten, and it’s possible to search for information in unallocated clusters for old versions of the file. If you search unallocated clusters for information it’s a “must” to search for “HARD_MAX_UPLOADS=” as this is crucial information regarding proving past sharing of files.

The limitation of upload speed/simultaneous uploads is found in the <Tools>-><Options>-><Advanced>-><Transfers> tab



Downloads

Don't allow more than 10 downloads at once

□ Limit your download bandwidth

Uploads

Don't allow more than 20 uploads at once

☑ Limit your upload bandwidth Unlimited

☑ Clear uploads from list when finished

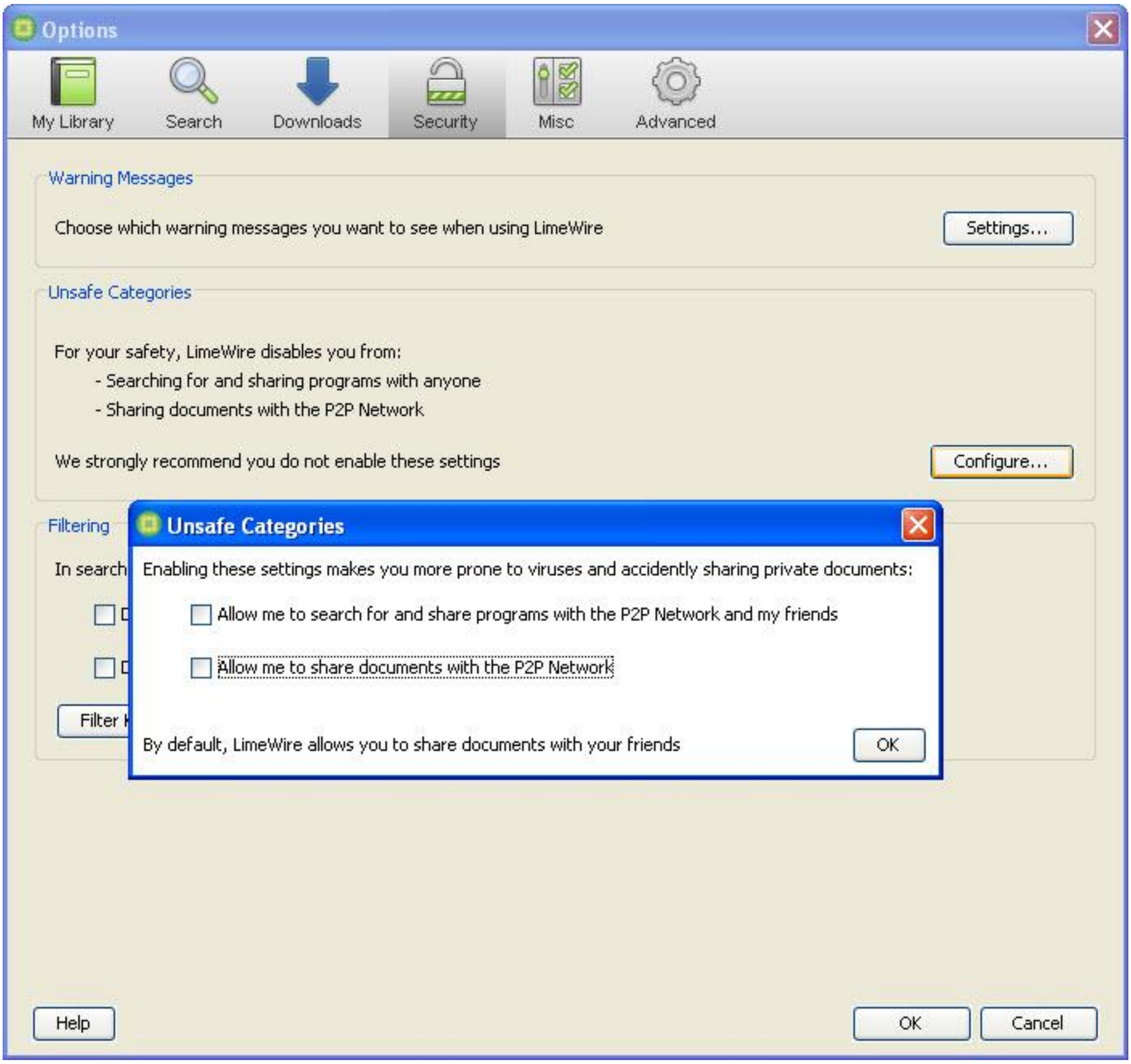
Connection Speed

Set your connection speed ● Broadband ○ Dial-up

The default setting for ”Uploads” i 20 connections and nol imitation in bandwidth.

If the “box” is ticked, then the slider appears – otherwise it is hidden

By default LimeWire only allows search and sharing of music-, video- and image files. To allow search for other filetypes – click <Tools>-><Options>-><Security> - Unsafe Categories



Warning Messages

Choose which warning messages you want to see when using LimeWire

Unsafe Categories

For your safety, LimeWire disables you from:

- Searching for and sharing programs with anyone
- Sharing documents with the P2P Network

We strongly recommend you do not enable these settings

Unsafe Categories

Enabling these settings makes you more prone to viruses and accidently sharing private documents:

□ Allow me to search for and share programs with the P2P Network and my friends

□ Allow me to share documents with the P2P Network

By default, LimeWire allows you to share documents with your friends

If these settings are applied the "limewire.props" file is added the lines

DOCUMENT_SHARING_ENABLED=true

PROGRAMS_ALLOWED=true

downloads.dat

Downloads.dat contains information on the current downloads. The file is rewritten constantly, so there is a good possibility to find information in unallocated clusters, pagefile.sys etc.

To se what currently is being downloaded – look in the “Temp-folder” – the temporary files shows there with name. An example is seen below:

T-5395563-Madonna - Hey Mr. DJ.mp3.

The “T-5395563-“ is added in fornt of the filename here – “T” for temporary – and the number sequence is the filesize in bytes.

The adding of the “prefix” does not indicate, that the temporary file has been played/viewed

Version. Props

Version.props contains information on what version of LimeWire is installed

5.1.3=true

Version 5.1.3 is installed

Library5.dat

As shared files in Limewire v.5.x not are shared on “folder basis”, but on file level, the information on which files are shared has to be stored somewhere – and in this case the information is stored in the file “library5.dat” In the previous version the shared files where mentioned in “library.dat”.

The content of the file looks like this:

```
¬í··sr··java.util.HashMap··ÚÁÃ·`Ñ···F·

loadFactorI·
                thresholdxp?@······w·········t··USER_EXTENSIONSsr··java.util.HashSetºD???¸·4···xpw·····
?@······xt··MANAGED_DIRECTORIESsq·~··w·····?@······sr··java.io.File·-¤E·

äÿ···L··patht··Ljava/lang/String;xpt·:C:\Documents and Settings\USER\My
Documents\LimeWire\Savedw··\xsq·~··t·+C:\Documents and Settings\USER\My
Documentsw··\xsq·~··t·DC:\Documents and Settings\USER\My Documents\LimeWire\Store
Purchasedw··\xsq·~··t·&C:\Documents and Settings\USER\Desktopw··\xxt·
```

```
EXCLUDE_FILESsq·~··w·····?@······xt··USER_REMOVEDsq·~··w····@?@······t··mnyt··xlst··xlsxt··docmt··
qdft··dott··dotmt··xlsmt··qdbt··xlsbt··dotxt··qsdt··xlamt··xltxt··bakt··qelt··qtxt··qift··datt··xltmt··flvt··
mbft··docxt··csvt··qphxt·

DO_NOT_MANAGEsq·~··w·····?@······xt·

SHARE_DATAsq·~··?@······w·········sq·~··t·VC:\Documents and Settings\USER\My
Documents\LimeWire\Saved\Madonna - Like A
Prayer.mp3w··\xsr·=com.limegroup.gnutella.library.LibraryFileData$FileProperties

¥Ð^Cgª®···Z··gnutellaL··friendst··Ljava/util/Set;xp·psq·~··t·XC:\Documents and Settings\USER\My
Documents\LimeWire\Saved\Metallica - Enter Sandman.mp3w··\xsq·~·4·pxx
```

As seen, there is a lot of “not human readable data” in the file. To interpret the data, you have to look at in HEX mode. The data then looks like this:

```
AC ED 00 05 73 72 00 11 6A 61 76 61 2E 75 74 69 6C 2E 48 61 73 68 4D 61 70 05 07 DA C1 C3 16
60 D1 03 00 02 46 00 0A 6C 6F 61 64 46 61 63 74 6F 72 49 00 09 74 68 72 65 73 68 6F 6C 64 78 70
3F 40 00 00 00 00 00 0C 77 08 00 00 00 10 00 00 00 06 74 00 0F 55 5345 52 5F 45 58 54 45 4E 53
49 4F 4E 53 73 72 00 11 6A 61 76 61 2E 75 74 69 6C 2E 48 61 73 68 53 65 74 BA 44 85 95 96 B8 B7
34 03 00 00 78 70 77 0C 00 00 00 10 3F 40 00 00 00 00 00 00 78 74 00 13 4D 41 4E 41 47 45 44 5F
44 49 52 45 43 54 4F 52 49 45 53 73 71 00 7E 00 03 77 0C 00 00 00 10 3F 40 00 00 00 00 00 04 73
72 00 0C 6A 61 76 61 2E 69 6F 2E 46 69 6C 65 04 2D A4 45 0E 0D E4 FF 03 00 01 4C 00 04 70 61 74
68 74 00 12 4C 6A 61 76 61 2F 6C 61 6E 67 2F 53 74 72 69 6E 67 3B 78 70 74 00 3A 43 3A 5C 44 6F
63 75 6D65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 4D 79 20 44 6F 63
75 6D 65 6E 74 73 5C 4C 69 6D 65 57 69 7265 5C 53 61 76 65 64 77 02 00 5C 78 73 71 00 7E 00 07
74 00 2B 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45
52 5C 4D 79 20 44 6F 63 75 6D 65 6E 74 73 77 02 00 5C 78 73 71 00 7E 00 07 74 00 44 43 3A 5C 44
6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 4D 79 20 44 6F
63 75 6D 65 6E 74 73 5C 4C 69 6D 65 57 69 72 65 5C 53 74 6F 72 65 20 50 75 72 63 68 61 73 65 64
77 02 00 5C 78 73 71 00 7E 00 07 74 00 26 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53
65 74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74 6F 70 77 02 00 5C 78 78 74 00 0D 45 58 43
4C 55 44 45 5F 46 49 4C 45 53 73 71 00 7E 00 03 77 0C 00 00 00 10 3F 40 00 00 00 00 00 00 78 74
00 0C 55 53 45 52 5F 52 45 4D 4F 56 45 44 73 71 00 7E 00 03 77 0C 00 00 00 40 3F 40 00 00 00 00
00 19 74 00 03 6D 6E 79 74 00 03 78 6C 73 74 00 04 78 6C 73 78 74 00 04 64 6F 63 6D 74 00 03 71
64 66 74 00 03 64 6F 74 74 00 04 64 6F 74 6D 74 00 04 78 6C 73 6D 74 00 03 71 64 62 74 00 04 78
6C 73 62 74 00 04 64 6F 74 78 74 00 03 71 73 64 74 00 04 78 6C 61 6D 74 00 04 78 6C 74 78 74 00
03 62 61 6B 74 00 03 71 65 6C 74 00 03 71 74 78 74 00 03 71 69 66 74 00 03 64 61 74 74 00 04 78
6C 74 6D 74 00 03 66 6C 76 74 00 03 6D 62 66 74 00 04 64 6F 63 78 74 00 03 63 73 76 74 00 03 71
```

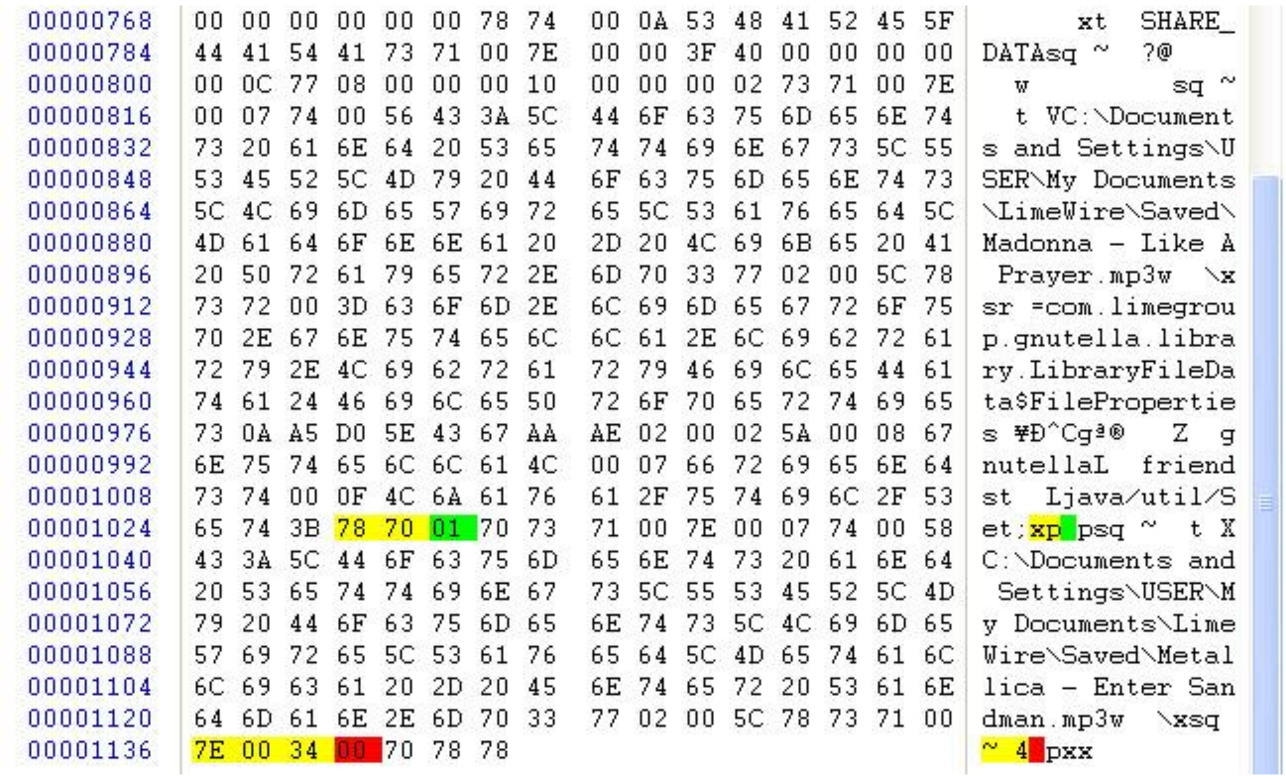
```
70 68 78 74 00 0D 44 4F 5F 4E 4F 54 5F 4D 41 4E 41 47 45 73 71 00 7E 00 03 77 0C 00 00 00 10 3F
40 00 00 00 00 00 00 78 74 00 0A 53 48 41 52 45 5F 44 41 54 41 73 71 00 7E 00 00 3F 40 00 00 00
00 00 0C 77 08 00 00 00 10 00 00 00 02 73 71 00 7E 00 07 74 00 56 43 3A 5C 44 6F 63 75 6D 65 6E
74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 4D 79 20 44 6F 63 75 6D65 6E 74
73 5C 4C 69 6D 65 57 69 72 65 5C 53 61 76 65 64 5C 4D 61 64 6F 6E 6E 61 20 2D 20 4C 69 6B 65
20 41 20 50 72 61 79 65 72 2E 6D 70 33 77 02 00 5C 78 73 72 00 3D 63 6F 6D 2E 6C 69 6D 65 67
72 6F 75 70 2E 67 6E 75 74 65 6C 6C 61 2E 6C 69 62 72 61 72 79 2E 4C 69 62 72 61 72 79 46 69 6C
65 44 61 74 61 24 46 69 6C 65 50 72 6F 70 65 72 74 69 65 73 0A A5 D0 5E 43 67 AA AE 02 00 02
5A 00 08 67 6E 75 74 65 6C 6C 61 4C 00 07 66 72 69 65 6E 64 73 74 00 0F 4C 6A 61 76 61 2F 75 74
69 6C 2F 53 65 74 3B 78 70 01 70 73 71 00 7E 00 07 74 00 58 43 3A 5C 44 6F 63 75 6D 65 6E 74 73
20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 4D 79 20 44 6F 63 75 6D 65 6E 74 73 5C
4C 69 6D 65 57 69 72 65 5C 53 61 76 65 64 5C 4D 65 74 61 6C 6C 69 63 61 20 2D 20 45 6E 74 65
72 20 53 61 6E 64 6D 61 6E 2E 6D 70 33 77 02 00 5C 78 73 71 00 7E 00 34 00 70 78 78
```

As seen, there is a lot of tata to interpret. In this “library5.dat” file, there is information on 2 files – but only 1 of them are shared – how can you determine which files are shared.

The information on sharing is stored in one byte attached to the fileentry.

When comparing 2 “library5.dat” files – one where files are shared, and one where the files have been unshared, it shows, that the “sharing byte” is at the end of each entry

When looking at the picture below, you can see, that one file is hared (green byte) and one file is unshared (red byte)



```
00000768  00 00 00 00 00 00 78 74  00 0A 53 48 41 52 45 5F        xt  SHARE_
00000784  44 41 54 41 73 71 00 7E  00 00 3F 40 00 00 00 00  DATAsq ~  ?@
00000800  00 0C 77 08 00 00 00 10  00 00 00 02 73 71 00 7E    w         sq ~
00000816  00 07 74 00 56 43 3A 5C  44 6F 63 75 6D 65 6E 74    t VC:\Document
00000832  73 20 61 6E 64 20 53 65  74 74 69 6E 67 73 5C 55  s and Settings\U
00000848  53 45 52 5C 4D 79 20 44  6F 63 75 6D 65 6E 74 73  SER\My Documents
00000864  5C 4C 69 6D 65 57 69 72  65 5C 53 61 76 65 64 5C  \LimeWire\Saved\
00000880  4D 61 64 6F 6E 6E 61 20  2D 20 4C 69 6B 65 20 41  Madonna - Like A
00000896  20 50 72 61 79 65 72 2E  6D 70 33 77 02 00 5C 78   Prayer.mp3w  \x
00000912  73 72 00 3D 63 6F 6D 2E  6C 69 6D 65 67 72 6F 75  sr =com.limegrou
00000928  70 2E 67 6E 75 74 65 6C  6C 61 2E 6C 69 62 72 61  p.gnutella.libra
00000944  72 79 2E 4C 69 62 72 61  72 79 46 69 6C 65 44 61  ry.LibraryFileDa
00000960  74 61 24 46 69 6C 65 50  72 6F 70 65 72 74 69 65  ta$FilePropertie
00000976  73 0A A5 D0 5E 43 67 AA  AE 02 00 02 5A 00 08 67  s ¥Ð^Cgª®   Z  g
00000992  6E 75 74 65 6C 6C 61 4C  00 07 66 72 69 65 6E 64  nutellaL  friend
00001008  73 74 00 0F 4C 6A 61 76  61 2F 75 74 69 6C 2F 53  st  Ljava/util/S
00001024  65 74 3B 78 70 01 70 73  71 00 7E 00 07 74 00 58  et;xp psq ~  t X
00001040  43 3A 5C 44 6F 63 75 6D  65 6E 74 73 20 61 6E 64  C:\Documents and
00001056  20 53 65 74 74 69 6E 67  73 5C 55 53 45 52 5C 4D   Settings\USER\M
00001072  79 20 44 6F 63 75 6D 65  6E 74 73 5C 4C 69 6D 65  y Documents\Lime
00001088  57 69 72 65 5C 53 61 76  65 64 5C 4D 65 74 61 6C  Wire\Saved\Metal
00001104  6C 69 63 61 20 2D 20 45  6E 74 65 72 20 53 61 6E  lica - Enter San
00001120  64 6D 61 6E 2E 6D 70 33  77 02 00 5C 78 73 71 00  dman.mp3w  \xsq
00001136  7E 00 34 00 70 78 78                              ~ 4 pxx
```

As seen, the “header” for the sharing byte is not the same, and other variations can occur. The GREP search (EnCase style GREP) below will extract the sharing state of the files within the “library5.dat” file

(\x78\x70[\x00\x01])|(\x7E\x00.[\x00\x01])

The search hits will by the last byte show, whether the file is shared or not

00 : Unshared

01: Shared

To extract filename, path and share-byte use one of the following GREP-searches:

If the first GREP shows that all files are shared use this new GREP-search:

\x73\x71\x00\x7E\x00\x07\x74\x00.{0,255}(\x78\x70\x01)|(\x7E\x00.\x01)

NOTE: If the total string length of path and filename exceeds 255 characters no hits will be returned. It is however possible to bookmark these files individually

If the first GREP shows that some files are unshared, you have to run the GREP above and the following:

\x73\x71\x00\x7E\x00\x07\x74\x00.{0,255}(\x78\x70\x00)|(\x7E\x00.\x00)

NOTE: If the total string length of path and filename exceeds 255 characters no hits will be returned. It is however possible to bookmark these files individually

By running the 2 GREP's separately, you can create 2 tables with these data for later comparison with the entries in "fileurns.cache"

When files are deleted from the "library", their entry in "library5.dat" is deleted. It is however possible to search for deleted "library5.dat" files, by searching for the "footer" of the file. The following GREP-search, will find the footer (including the share setting of the last file entry)

((\x78\x70[\x00\x01])|(\x7E\x00[\x30\x34][\x00\x01]))\x70\x78\x78

From hits on this search, you have to go backwards and save as much of the deleted file as possible

HINT (EnCase): Export the found entries into a binary file, add the file to the case and use the GREP-search that extracts the filename, paths and share-bit

As this file doesn't contain any hash values, you need to compare the findings with entries from "fileurns.cache"

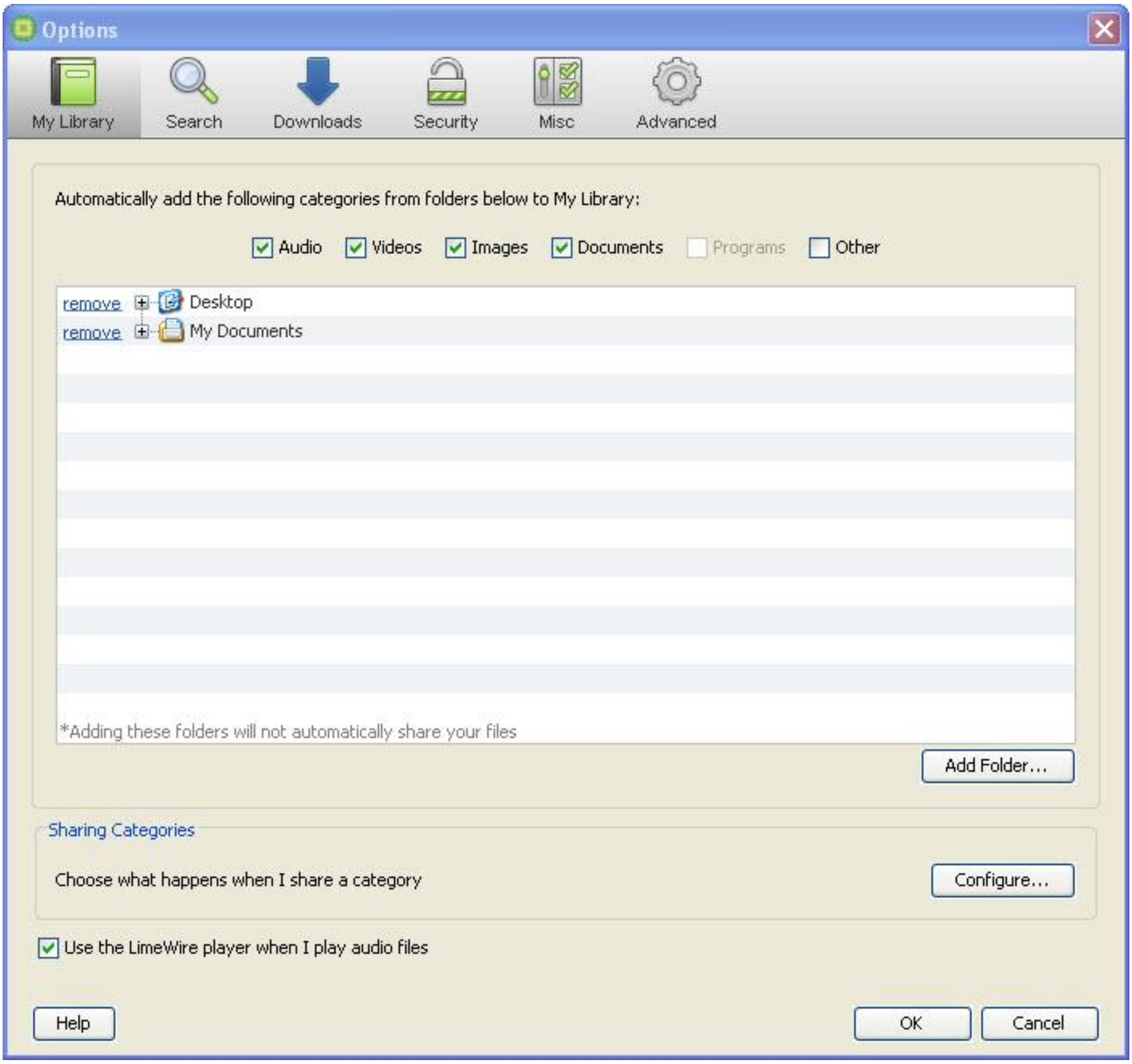
Fileurns.cache

Fileurns.cache contains information on the files that are in the LimeWire "library".

Each entry consists of Filename, storage path, LastModified date, SHA1_base32 hashvalue and TigerTree_base32 hashvalue of the file

When a file is deleted, the entry is also deleted in "fileurns.cache"

The files in "fileurns.cache" does not have to have been downloaded by LimeWire – they only have to be in one of the folders, that are mentioned in the library. By default the "Documents" and the "Desktop" (both with subfolders) are in the library (only certain filetypes – see picture below)



Options

Automatically add the following categories from folders below to My Library:

☑ Audio ☑ Videos ☑ Images ☑ Documents □ Programs □ Other

remove ⊞ Desktop
remove ⊞ My Documents

*Adding these folders will not automatically share your files

Sharing Categories

Choose what happens when I share a category

☑ Use the LimeWire player when I play audio files

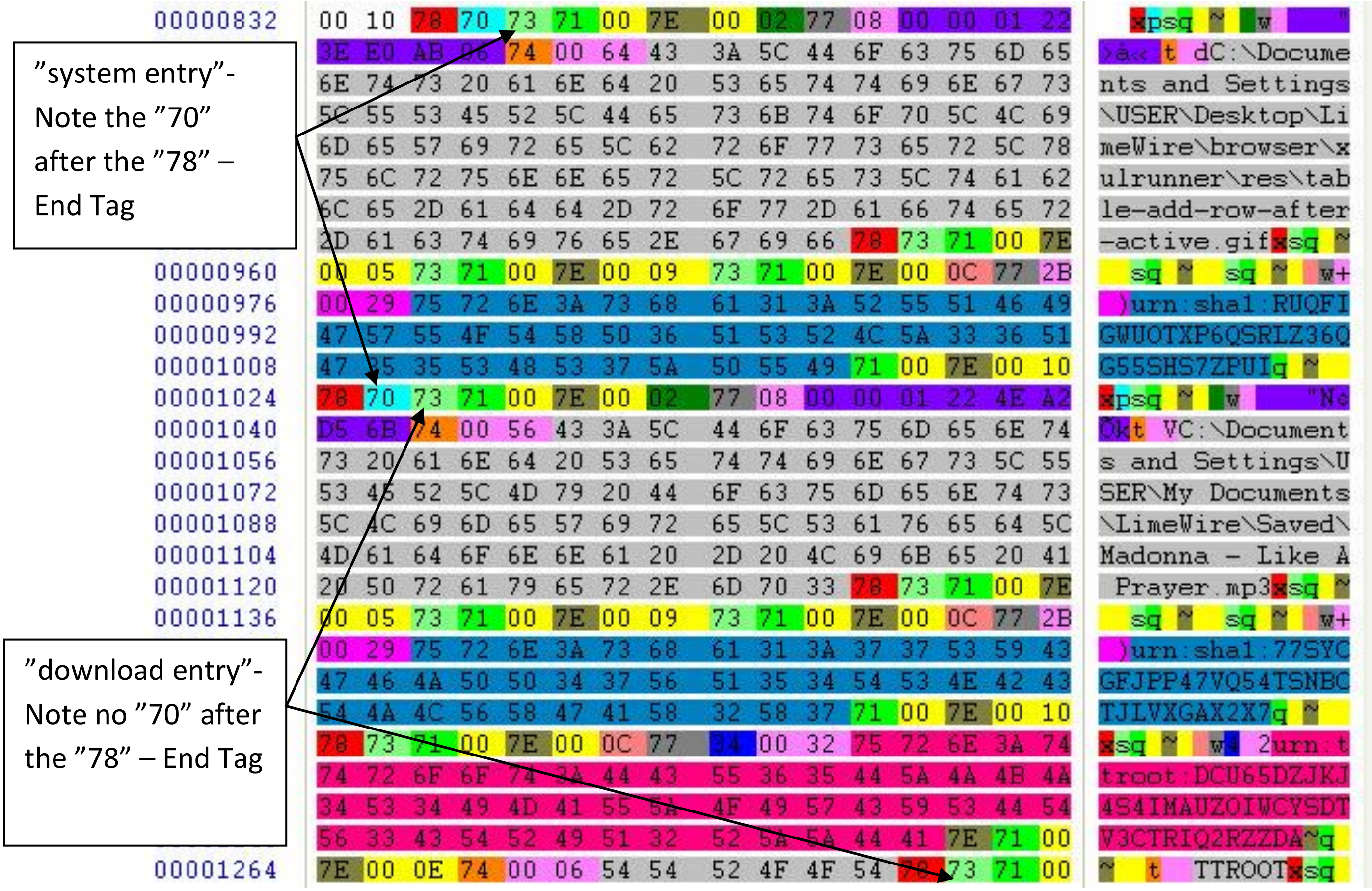
This setting means, that if you download a file from eg. Internet Explorer, ad place it on the desktop, the file will be mentioned in "fileurns.cache" – but you have to set the files as shared manually.

This means that the bare presence of a fileentry in "fileurns.cache" is not an evidence of sharing – but it's an evidence of possession of the file.

When searching unallocated clusters for deleted "fileurns.cache" files", it's possible to find the SHA1 or TTH hashvalues of the deleted files, and hereby prove the earlier possession of certain files (If you have a database of illegal files, it's possible to compare the hashvalues from the database and the hashvalues from the case and hereby prove earlier possession of these files)

How does an entry in “fileurns.cache” look like?

If you open the “fileurns.cache” in a HEX-editor, an entry could look like the picture below. In this picture, there are 2 entries. An entry starts with 73 (71 00)



```
00000832   00 10 78 70 73 71 00 7E  00 02 77 08 00 00 01 22    xpsq ~  w     "
           3E E0 AB 06 74 00 64 43  3A 5C 44 6F 63 75 6D 65   >à« t dC:\Docume
           6E 74 73 20 61 6E 64 20  53 65 74 74 69 6E 67 73   nts and Settings
           5C 55 53 45 52 5C 44 65  73 6B 74 6F 70 5C 4C 69   \USER\Desktop\Li
           6D 65 57 69 72 65 5C 62  72 6F 77 73 65 72 5C 78   meWire\browser\x
           75 6C 72 75 6E 6E 65 72  5C 72 65 73 5C 74 61 62   ulrunner\res\tab
           6C 65 2D 61 64 64 2D 72  6F 77 2D 61 66 74 65 72   le-add-row-after
           2D 61 63 74 69 76 65 2E  67 69 66 78 73 71 00 7E   -active.gifxsq ~
00000960   00 05 73 71 00 7E 00 09  73 71 00 7E 00 0C 77 2B     sq ~  sq ~  w+
00000976   00 29 75 72 6E 3A 73 68  61 31 3A 52 55 51 46 49    )urn:sha1:RUQFI
00000992   47 57 55 4F 54 58 50 36  51 53 52 4C 5A 33 36 51   GWUOTXP6QSRLZ36Q
00001008   47 35 35 53 48 53 37 5A  50 55 49 71 00 7E 00 10   G55SHS7ZPUIq ~
00001024   78 70 73 71 00 7E 00 02  77 08 00 00 01 22 4E A2   xpsq ~  w    "N¢
00001040   D5 6B 74 00 56 43 3A 5C  44 6F 63 75 6D 65 6E 74   Õkt VC:\Document
00001056   73 20 61 6E 64 20 53 65  74 74 69 6E 67 73 5C 55   s and Settings\U
00001072   53 45 52 5C 4D 79 20 44  6F 63 75 6D 65 6E 74 73   SER\My Documents
00001088   5C 4C 69 6D 65 57 69 72  65 5C 53 61 76 65 64 5C   \LimeWire\Saved\
00001104   4D 61 64 6F 6E 6E 61 20  2D 20 4C 69 6B 65 20 41   Madonna - Like A
00001120   20 50 72 61 79 65 72 2E  6D 70 33 78 73 71 00 7E    Prayer.mp3xsq ~
00001136   00 05 73 71 00 7E 00 09  73 71 00 7E 00 0C 77 2B     sq ~  sq ~  w+
           00 29 75 72 6E 3A 73 68  61 31 3A 37 37 53 59 43    )urn:sha1:77SYC
           47 46 4A 50 50 34 37 56  51 35 34 54 53 4E 42 43   GFJPP47VQ54TSNBC
           54 4A 4C 56 58 47 41 58  32 58 37 71 00 7E 00 10   TJLVXGAX2X7q ~
           78 73 71 00 7E 00 0C 77  34 00 32 75 72 6E 3A 74   xsq ~  w4 2urn:t
           74 72 6F 6F 74 3A 44 43  55 36 35 44 5A 4A 4B 4A   troot:DCU65DZJKJ
           34 53 34 49 4D 41 55 5A  4F 49 57 43 59 53 44 54   4S4IMAUZOIWCYSDT
           56 33 43 54 52 49 51 32  52 5A 5A 44 41 7E 71 00   V3CTRIQ2RZZDA~q
00001264   7E 00 0E 74 00 06 54 54  52 4F 4F 54 78 73 71 00   ~  t  TTROOTxsq
```

”system entry”- Note the ”70” after the ”78” – End Tag

”download entry”- Note no ”70” after the ”78” – End Tag

TAG	Meaning	Notes
02 (77 08)	Java Timestamp	“Last Written of file” – time when file was fully downloaded
0C (77 xx)	URN	
2B	SHA1 URN	

34	TTH URN	
70	End “system entry”	Follows entries, where the system has added the data. Note: This tag is not found right after files downloaded via LimeWire
71	Currently unknown	Followed by 1 byte – meaning currently unknown
72	Java String	Followed by 2 bytes telling length of string
73	Start of entry	
74	Path	Followed by 2 bytes telling length of string
77	Text string	Followed by 2 bytes telling length of string
7E	Currently unknown	
78	End of entry	

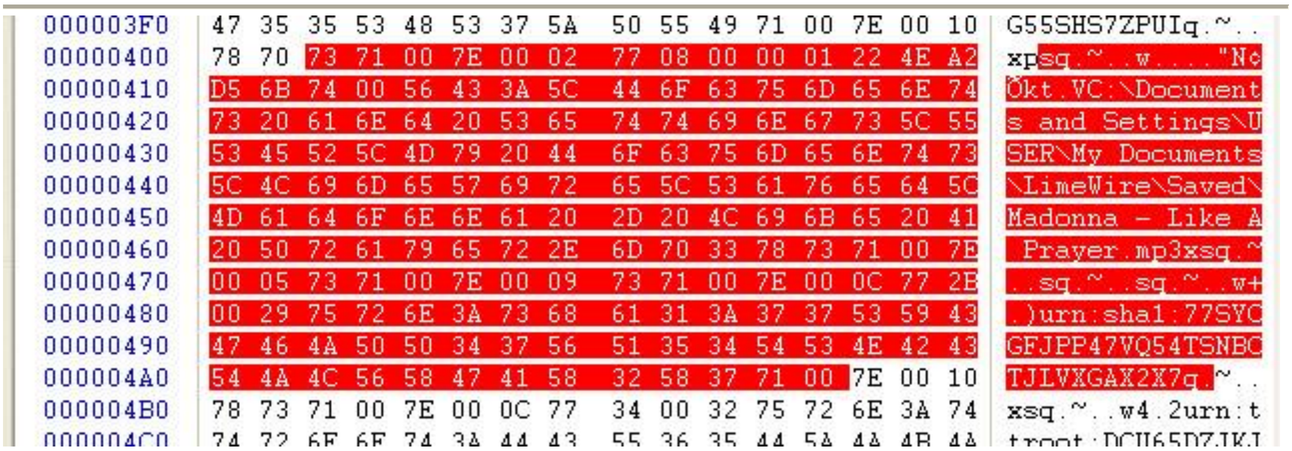
How to extract filenames, paths, dates and SHA1_base32 value from “fileurns.cache”

When using EnCase the following GREP-search can extract the desired information *)

```
\x73\x71\x00\x7E.{0,8}\x77\x08.{8,8}\x74\x00.{0,255}\x78\x73\x71.{0,30}\x2B\x00\x29urn\:sha1\:[A-Z0-9]{32,32}\x71
```

*) the GREP will return a string of max 255 carachters – see explanation later

Looking at one of the entries on the previous page, the search will find the following data:



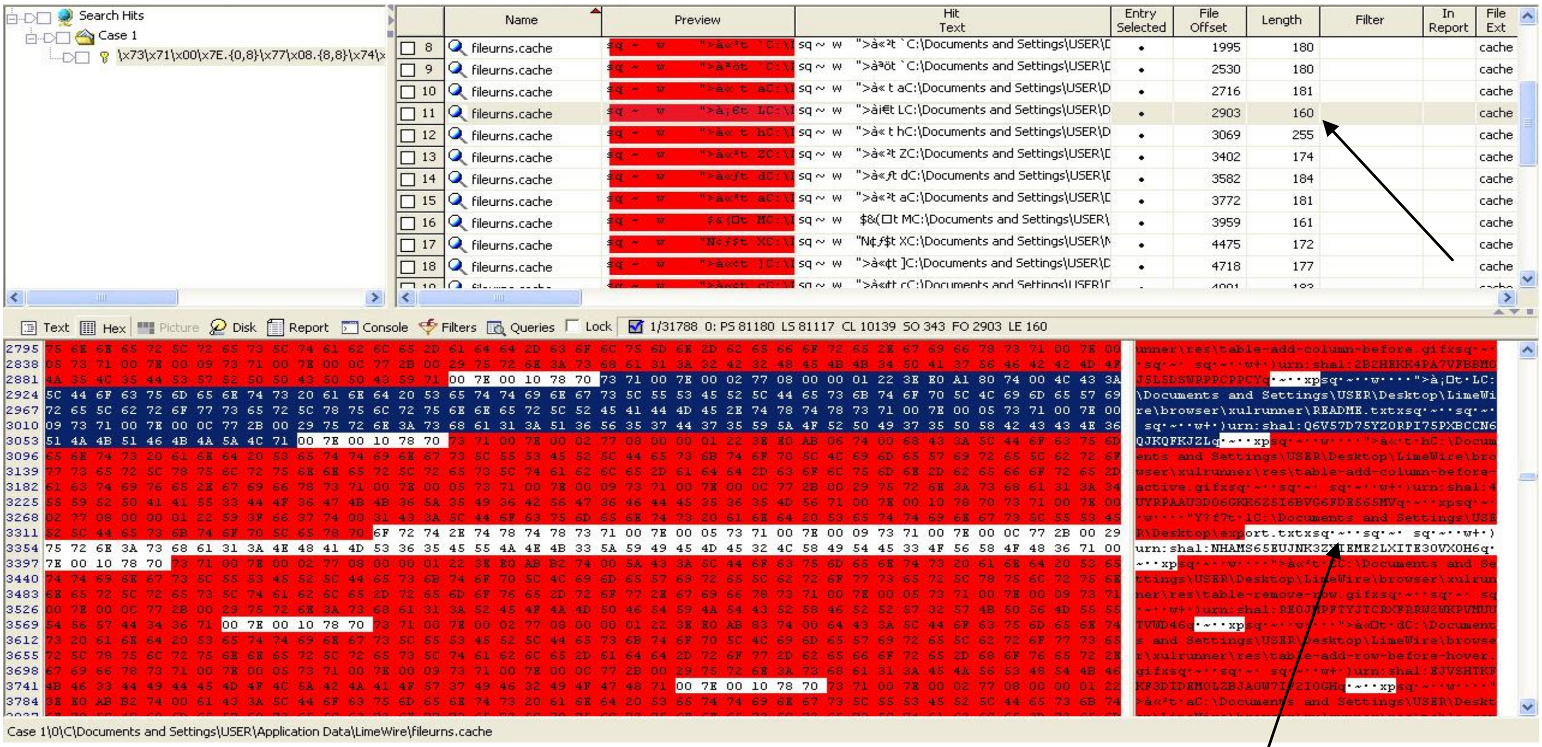
```
000003F0  47 35 35 53 48 53 37 5A  50 55 49 71 00 7E 00 10  G55SHS7ZPUIq.~..
00000400  78 70 73 71 00 7E 00 02  77 08 00 00 01 22 4E A2  xpsq.~..w...."Nc
00000410  D5 6B 74 00 56 43 3A 5C  44 6F 63 75 6D 65 6E 74  Õkt.VC:\Document
00000420  73 20 61 6E 64 20 53 65  74 74 69 6E 67 73 5C 55  s and Settings\U
00000430  53 45 52 5C 4D 79 20 44  6F 63 75 6D 65 6E 74 73  SER\My Documents
00000440  5C 4C 69 6D 65 57 69 72  65 5C 53 61 76 65 64 5C  \LimeWire\Saved\
00000450  4D 61 64 6F 6E 6E 61 20  2D 20 4C 69 6B 65 20 41  Madonna - Like A
00000460  20 50 72 61 79 65 72 2E  6D 70 33 78 73 71 00 7E   Prayer.mp3xsq.~
00000470  00 05 73 71 00 7E 00 09  73 71 00 7E 00 0C 77 2B  ..sq.~..sq.~..w+
00000480  00 29 75 72 6E 3A 73 68  61 31 3A 37 37 53 59 43  .)urn:sha1:77SYC
00000490  47 46 4A 50 50 34 37 56  51 35 34 54 53 4E 42 43  GFJPP47VQ54TSNBC
000004A0  54 4A 4C 56 58 47 41 58  32 58 37 71 00 7E 00 10  TJLVXGAX2X7q.~..
000004B0  78 73 71 00 7E 00 0C 77  34 00 32 75 72 6E 3A 74  xsq.~..w4.2urn:t
000004C0  74 72 6F 6F 74 3A 44 43  55 36 35 44 5A 4A 4B 4A  troot:DCU65DZJKJ
```

Note that the GREP not returns the TTH value

There is a flaw to this method. EnCase GREP only allows to search and return strings of maximum 255 carachters.

Look at the 2 examples below:

String below 255 carachters:



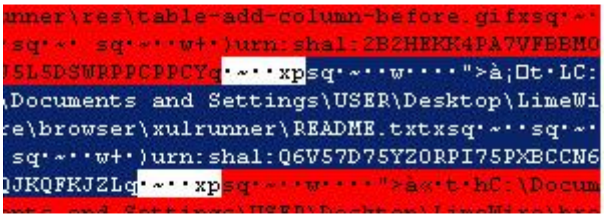
Search Hits
Case 1
\x73\x71\x00\x7E.{0,8}\x77\x08.{8,8}\x74\x

	Name	Preview	Hit Text	Entry Selected	File Offset	Length	Filter	In Report	File Ext
□ 8	fileurns.cache	sq ~ w ">à«²t `C:\I	sq ~ w ">à«²t `C:\Documents and Settings\USER\D	•	1995	180			cache
□ 9	fileurns.cache	sq ~ w ">àªöt `C:\I	sq ~ w ">àªöt `C:\Documents and Settings\USER\D	•	2530	180			cache
□ 10	fileurns.cache	sq ~ w ">à« t aC:\I	sq ~ w ">à« t aC:\Documents and Settings\USER\D	•	2716	181			cache
□ 11	fileurns.cache	sq ~ w ">à¡€t LC:\I	sq ~ w ">à¡€t LC:\Documents and Settings\USER\D	•	2903	160			cache
□ 12	fileurns.cache	sq ~ w ">à« t hC:\I	sq ~ w ">à« t hC:\Documents and Settings\USER\D	•	3069	255			cache
□ 13	fileurns.cache	sq ~ w ">à«²t ZC:\I	sq ~ w ">à«²t ZC:\Documents and Settings\USER\D	•	3402	174			cache
□ 14	fileurns.cache	sq ~ w ">à«ƒt dC:\I	sq ~ w ">à«ƒt dC:\Documents and Settings\USER\D	•	3582	184			cache
□ 15	fileurns.cache	sq ~ w ">à«²t aC:\I	sq ~ w ">à«²t aC:\Documents and Settings\USER\D	•	3772	181			cache
□ 16	fileurns.cache	sq ~ w $&(□t MC:\I	sq ~ w $&(□t MC:\Documents and Settings\USER\	•	3959	161			cache
□ 17	fileurns.cache	sq ~ w "N¢ƒ$t XC:\I	sq ~ w "N¢ƒ$t XC:\Documents and Settings\USER\M	•	4475	172			cache
□ 18	fileurns.cache	sq ~ w ">à«¢t]C:\I	sq ~ w ">à«¢t]C:\Documents and Settings\USER\D	•	4718	177			cache
□ 19	fileurns.cache	sq ~ w ">à«¢t cC:\I	sq ~ w ">à«¢t cC:\Documents and Settings\USER\D	•	4901	183			cache

☑ 1/31788 0: PS 81180 LS 81117 CL 10139 SO 343 FO 2903 LE 160

```
2795 75 6E 6E 65 72 5C 72 65 73 5C 74 61 62 6C 65 2D 61 64 64 2D 63 6F 6C 75 6D 6E 2D 62 65 66 6F 72 65 2E 67 69 66 78 73 71 00 7E 00 unner\res\table-add-column-before.gifxsq·~·
2838 05 73 71 00 7E 00 09 73 71 00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 32 42 32 48 45 4B 4B 34 50 41 37 56 46 42 42 4D 4F ·sq·~· sq·~··w+·)urn:sha1:2B2HEKK4PA7VFBBMO
2881 4A 35 4C 35 44 53 57 52 50 50 43 50 50 43 59 71 00 7E 00 10 78 70 73 71 00 7E 00 02 77 08 00 00 01 22 3E E0 A1 80 74 00 4C 43 3A J5L5DSWRPPCPPCYq·~··xpsq·~··w····">à¡□t·LC:
2924 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74 6F 70 5C 4C 69 6D 65 57 69 \Documents and Settings\USER\Desktop\LimeWi
2967 72 65 5C 62 72 6F 77 73 65 72 5C 78 75 6C 72 75 6E 6E 65 72 5C 52 45 41 44 4D 45 2E 74 78 74 78 73 71 00 7E 00 05 73 71 00 7E 00 re\browser\xulrunner\README.txtxsq·~··sq·~·
3010 09 73 71 00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 51 36 56 35 37 44 37 35 59 5A 4F 52 50 49 37 35 50 58 42 43 43 4E 36  sq·~··w+·)urn:sha1:Q6V57D75YZORPI75PXBCCN6
3053 51 4A 4B 51 46 4B 4A 5A 4C 71 00 7E 00 10 78 70 73 71 00 7E 00 02 77 08 00 00 01 22 3E E0 AB 06 74 00 68 43 3A 5C 44 6F 63 75 6D QJKQFKJZLq·~··xpsq·~··w····">à«·t·hC:\Docum
3096 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74 6F 70 5C 4C 69 6D 65 57 69 72 65 5C 62 72 6F ents and Settings\USER\Desktop\LimeWire\bro
3139 77 73 65 72 5C 78 75 6C 72 75 6E 6E 65 72 5C 72 65 73 5C 74 61 62 6C 65 2D 61 64 64 2D 63 6F 6C 75 6D 6E 2D 62 65 66 6F 72 65 2D wser\xulrunner\res\table-add-column-before-
3182 61 63 74 69 76 65 2E 67 69 66 78 73 71 00 7E 00 05 73 71 00 7E 00 09 73 71 00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 34 active.gifxsq·~··sq·~· sq·~··w+·)urn:sha1:4
3225 55 59 52 50 41 41 55 33 44 4F 36 47 4B 4B 36 5A 35 49 36 42 56 47 36 46 44 45 35 36 35 4D 56 71 00 7E 00 10 78 70 73 71 00 7E 00 UYRPAAU3DO6GKK6Z5I6BVG6FDE565MVq·~··xpsq·~·
3268 02 77 08 00 00 01 22 59 3F 66 37 74 00 31 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 ·w····"Y?f7t·1C:\Documents and Settings\USE
3311 52 5C 44 65 73 6B 74 6F 70 5C 65 78 70 6F 72 74 2E 74 78 74 78 73 71 00 7E 00 05 73 71 00 7E 00 09 73 71 00 7E 00 0C 77 2B 00 29 R\Desktop\export.txtxsq·~··sq·~· sq·~··w+·)
3354 75 72 6E 3A 73 68 61 31 3A 4E 48 41 4D 53 36 35 45 55 4A 4E 4B 33 5A 59 49 45 4D 45 32 4C 58 49 54 45 33 4F 56 58 4F 48 36 71 00 urn:sha1:NHAMS65EUJNK3ZYIEME2LXITE3OVXOH6q·
3397 7E 00 10 78 70 73 71 00 7E 00 02 77 08 00 00 01 22 3E E0 AB B2 74 00 5A 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 ~··xpsq·~··w····">à«²t·ZC:\Documents and Se
3440 74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74 6F 70 5C 4C 69 6D 65 57 69 72 65 5C 62 72 6F 77 73 65 72 5C 78 75 6C 72 75 6E ttings\USER\Desktop\LimeWire\browser\xulrun
3483 6E 65 72 5C 72 65 73 5C 74 61 62 6C 65 2D 72 65 6D 6F 76 65 2D 72 6F 77 2E 67 69 66 78 73 71 00 7E 00 05 73 71 00 7E 00 09 73 71 ner\res\table-remove-row.gifxsq·~··sq·~· sq
3526 00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 52 45 4F 4A 4D 50 46 54 59 4A 54 43 52 58 46 52 52 57 32 57 4B 50 56 4D 55 55 ·~··w+·)urn:sha1:REOJMPFTYJTCRXFRRW2WKPVMUU
3569 54 56 57 44 34 36 71 00 7E 00 10 78 70 73 71 00 7E 00 02 77 08 00 00 01 22 3E E0 AB 83 74 00 64 43 3A 5C 44 6F 63 75 6D 65 6E 74 TVWD46q·~··xpsq·~··w····">à«□t·dC:\Document
3612 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74 6F 70 5C 4C 69 6D 65 57 69 72 65 5C 62 72 6F 77 73 65 s and Settings\USER\Desktop\LimeWire\browse
3655 72 5C 78 75 6C 72 75 6E 6E 65 72 5C 72 65 73 5C 74 61 62 6C 65 2D 61 64 64 2D 72 6F 77 2D 62 65 66 6F 72 65 2D 68 6F 76 65 72 2E r\xulrunner\res\table-add-row-before-hover.
3698 67 69 66 78 73 71 00 7E 00 05 73 71 00 7E 00 09 73 71 00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 45 4A 56 53 48 54 4B 46 gifxsq·~··sq·~· sq·~··w+·)urn:sha1:EJVSHTKF
3741 4B 46 33 44 49 44 45 4D 4F 4C 5A 42 4A 41 4F 57 37 49 46 32 49 4F 47 48 71 00 7E 00 10 78 70 73 71 00 7E 00 02 77 08 00 00 01 22 KF3DIDEMOLZBJAOW7IF2IOGHq·~··xpsq·~··w····"
3784 3E E0 AB B2 74 00 61 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74 >à«²t·aC:\Documents and Settings\USER\Deskt
```

Case 1\0\C\Documents and Settings\USER\Application Data\LimeWire\fileurns.cache

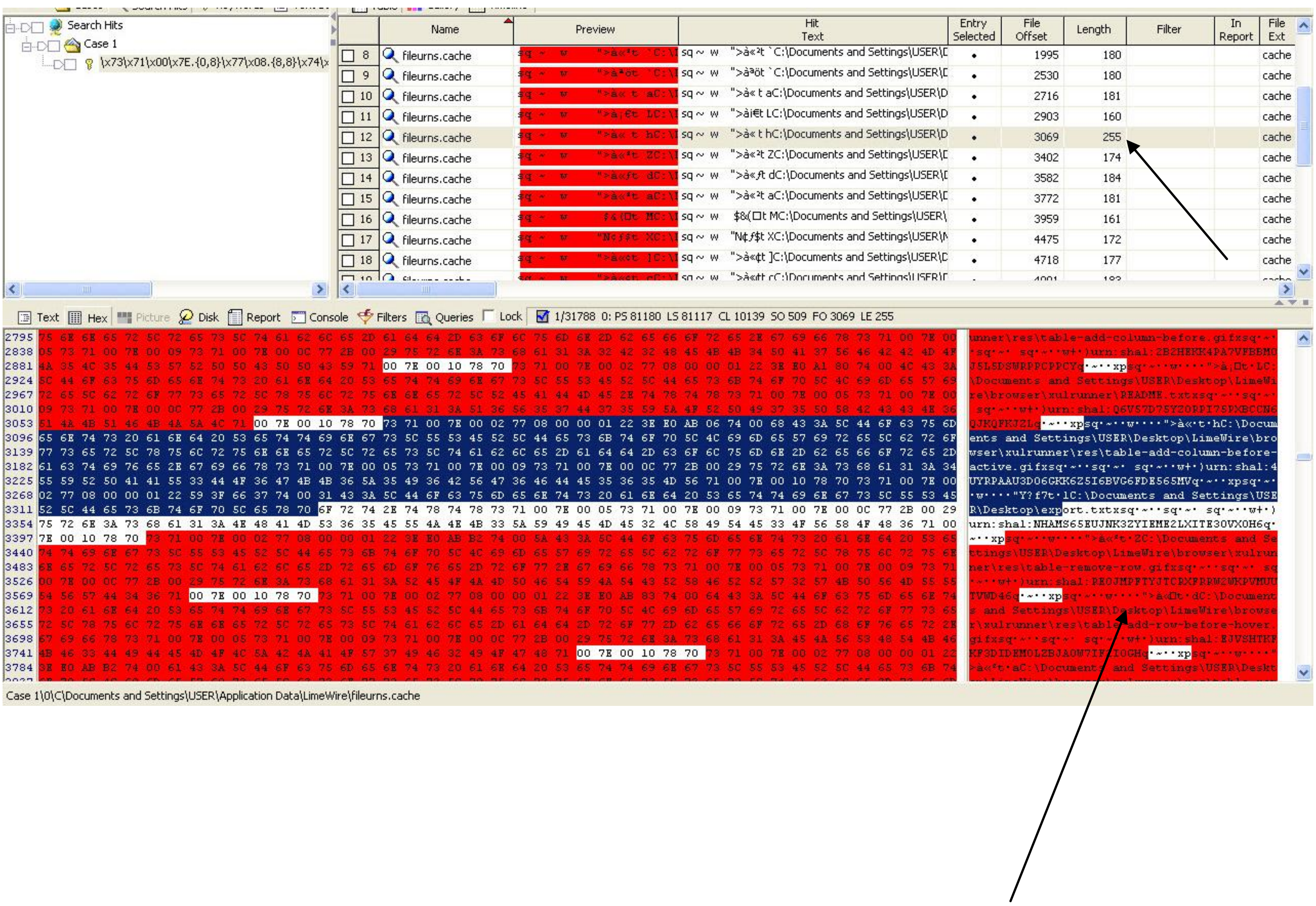


```
unner\res\table-add-column-before.gifxsq·~·
·sq·~·  sq·~··w+·)urn:shal:2B2HEKK4PA7VFBBMO
J5L5DSWRPPCPPCYq·~··xpsq·~··w····">à¡□t·LC:
\Documents and Settings\USER\Desktop\LimeWi
re\browser\xulrunner\README.txtxsq·~··sq·~·
 sq·~··w+·)urn:shal:Q6V57D75YZORPI75PXBCCN6
QJKQFKJZLq·~··xpsq·~··w····">à«·t·hC:\Docum
```

Note that the full entry is extracted

String above 255 carachters

When the strings get long, it's often due too extremely long filenames or storage paths



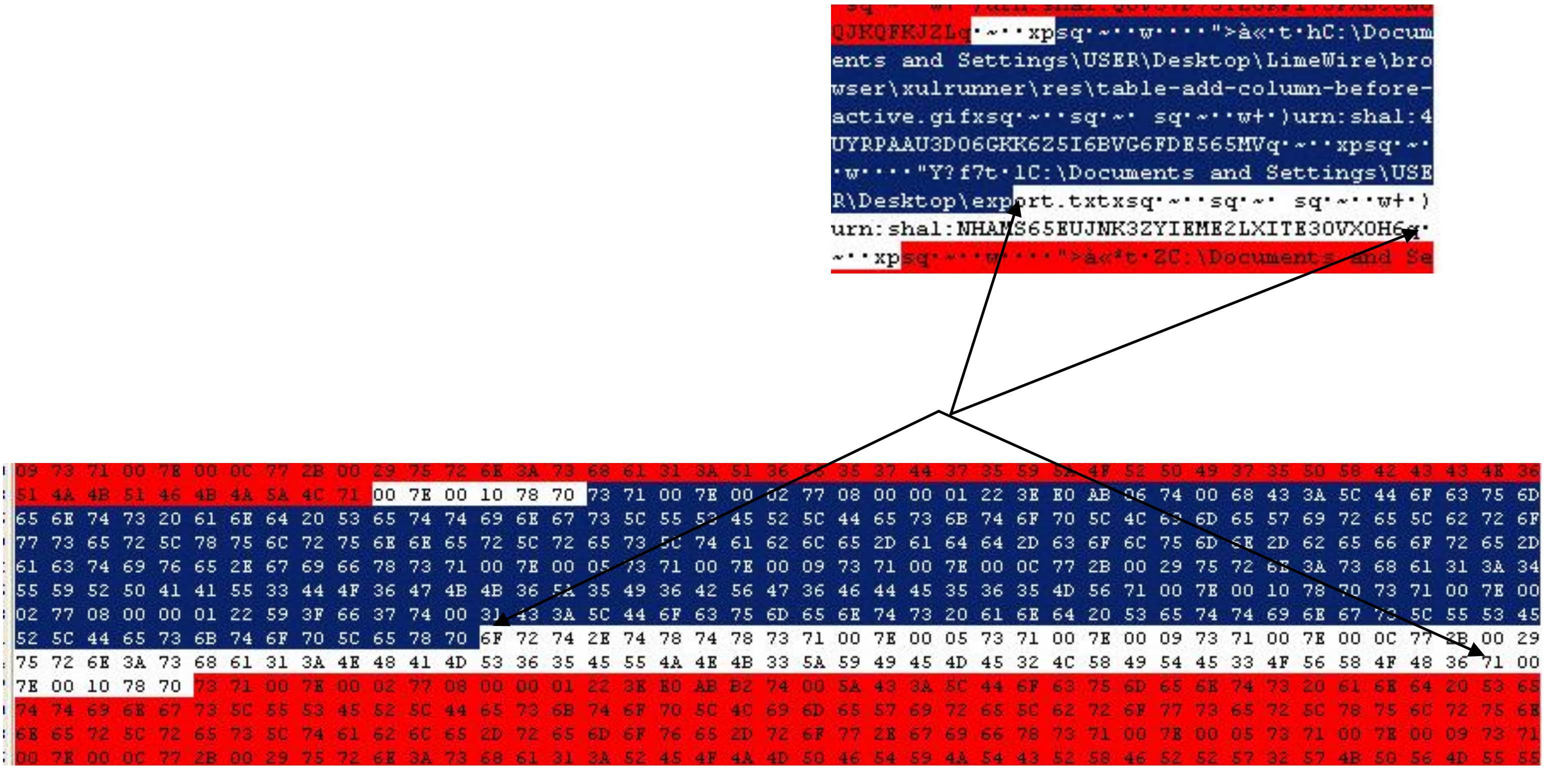
Search Hits
Case 1
\x73\x71\x00\x7E.{0,8}\x77\x08.{8,8}\x74\x

		Name	Preview	Hit Text	Entry Selected	File Offset	Length	Filter	In Report	File Ext
□	8	fileurns.cache	sq ~ w ">à«²t `C:\I	sq ~ w ">à«²t `C:\Documents and Settings\USER\D	•	1995	180			cache
□	9	fileurns.cache	sq ~ w ">àªöt `C:\I	sq ~ w ">àªöt `C:\Documents and Settings\USER\D	•	2530	180			cache
□	10	fileurns.cache	sq ~ w ">à« t aC:\I	sq ~ w ">à« t aC:\Documents and Settings\USER\D	•	2716	181			cache
□	11	fileurns.cache	sq ~ w ">à¡€t LC:\I	sq ~ w ">ài€t LC:\Documents and Settings\USER\D	•	2903	160			cache
□	12	fileurns.cache	sq ~ w ">à« t hC:\I	sq ~ w ">à« t hC:\Documents and Settings\USER\D	•	3069	255			cache
□	13	fileurns.cache	sq ~ w ">à«²t ZC:\I	sq ~ w ">à«²t ZC:\Documents and Settings\USER\D	•	3402	174			cache
□	14	fileurns.cache	sq ~ w ">à«ƒt dC:\I	sq ~ w ">à«ƒt dC:\Documents and Settings\USER\D	•	3582	184			cache
□	15	fileurns.cache	sq ~ w ">à«²t aC:\I	sq ~ w ">à«²t aC:\Documents and Settings\USER\D	•	3772	181			cache
□	16	fileurns.cache	sq ~ w $&(□t MC:\I	sq ~ w $&(□t MC:\Documents and Settings\USER\	•	3959	161			cache
□	17	fileurns.cache	sq ~ w "N¢ƒ$t XC:\I	sq ~ w "N¢ƒ$t XC:\Documents and Settings\USER\N	•	4475	172			cache
□	18	fileurns.cache	sq ~ w ">à«¢t]C:\I	sq ~ w ">à«¢t]C:\Documents and Settings\USER\D	•	4718	177			cache
□	19	fileurns.cache	sq ~ w ">à«¢t cC:\I	sq ~ w ">à«¢t cC:\Documents and Settings\USER\D	•	4901	183			cache

☑ 1/31788 0: PS 81180 LS 81117 CL 10139 SO 509 FO 3069 LE 255

```
2795 75 6E 6E 65 72 5C 72 65 73 5C 74 61 62 6C 65 2D 61 64 64 2D 63 6F 6C 75 6D 6E 2D 62 65 66 6F 72 65 2E 67 69 66 78 73 71 00 7E 00  unner\res\table-add-column-before.gifxsq·~·
2838 05 73 71 00 7E 00 09 73 71 00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 32 42 32 48 45 4B 4B 34 50 41 37 56 46 42 42 4D 4F  ·sq·~·  sq·~··w+·)urn:shal:2B2HEKK4PA7VFBBMO
2881 4A 35 4C 35 44 53 57 52 50 50 43 50 50 43 59 71 00 7E 00 10 78 70 73 71 00 7E 00 02 77 08 00 00 01 22 3E E0 A1 80 74 00 4C 43 3A  J5L5DSWRPPCPPCYq·~··xpsq·~··w····">à¡□t·LC:
2924 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74 6F 70 5C 4C 69 6D 65 57 69  \Documents and Settings\USER\Desktop\LimeWi
2967 72 65 5C 62 72 6F 77 73 65 72 5C 78 75 6C 72 75 6E 6E 65 72 5C 52 45 41 44 4D 45 2E 74 78 74 78 73 71 00 7E 00 05 73 71 00 7E 00  re\browser\xulrunner\README.txtxsq·~··sq·~·
3010 09 73 71 00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 51 36 56 35 37 44 37 35 59 5A 4F 52 50 49 37 35 50 58 42 43 43 4E 36   sq·~··w+·)urn:shal:Q6V57D75YZORPI75PXBCCN6
3053 51 4A 4B 51 46 4B 4A 5A 4C 71 00 7E 00 10 78 70 73 71 00 7E 00 02 77 08 00 00 01 22 3E E0 AB 06 74 00 68 43 3A 5C 44 6F 63 75 6D  QJKQFKJZLq·~··xpsq·~··w····">à«·t·hC:\Docum
3096 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74 6F 70 5C 4C 69 6D 65 57 69 72 65 5C 62 72 6F  ents and Settings\USER\Desktop\LimeWire\bro
3139 77 73 65 72 5C 78 75 6C 72 75 6E 6E 65 72 5C 72 65 73 5C 74 61 62 6C 65 2D 61 64 64 2D 63 6F 6C 75 6D 6E 2D 62 65 66 6F 72 65 2D  wser\xulrunner\res\table-add-column-before-
3182 61 63 74 69 76 65 2E 67 69 66 78 73 71 00 7E 00 05 73 71 00 7E 00 09 73 71 00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 34  active.gifxsq·~··sq·~·  sq·~··w+·)urn:shal:4
3225 55 59 52 50 41 41 55 33 44 4F 36 47 4B 4B 36 5A 35 49 36 42 56 47 36 46 44 45 35 36 35 4D 56 71 00 7E 00 10 78 70 73 71 00 7E 00  UYRPAAU3DO6GKK6Z5I6BVG6FDE565MVq·~··xpsq·~·
3268 02 77 08 00 00 01 22 59 3F 66 37 74 00 31 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45  ·w····"Y?f7t·1C:\Documents and Settings\USE
3311 52 5C 44 65 73 6B 74 6F 70 5C 65 78 70 6F 72 74 2E 74 78 74 78 73 71 00 7E 00 05 73 71 00 7E 00 09 73 71 00 7E 00 0C 77 2B 00 29  R\Desktop\export.txtxsq·~··sq·~·  sq·~··w+·)
3354 75 72 6E 3A 73 68 61 31 3A 4E 48 41 4D 53 36 35 45 55 4A 4E 4B 33 5A 59 49 45 4D 45 32 4C 58 49 54 45 33 4F 56 58 4F 48 36 71 00  urn:shal:NHAMS65EUJNK3ZYIEME2LXITE3OVXOH6q·
3397 7E 00 10 78 70 73 71 00 7E 00 02 77 08 00 00 01 22 3E E0 AB B2 74 00 5A 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65  ~··xpsq·~··w····">à«²t·ZC:\Documents and Se
3440 74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74 6F 70 5C 4C 69 6D 65 57 69 72 65 5C 62 72 6F 77 73 65 72 5C 78 75 6C 72 75 6E  ttings\USER\Desktop\LimeWire\browser\xulrun
3483 6E 65 72 5C 72 65 73 5C 74 61 62 6C 65 2D 72 65 6D 6F 76 65 2D 72 6F 77 2E 67 69 66 78 73 71 00 7E 00 05 73 71 00 7E 00 09 73 71  ner\res\table-remove-row.gifxsq·~··sq·~·  sq
3526 00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 52 45 4F 4A 4D 50 46 54 59 4A 54 43 52 58 46 52 52 57 32 57 4B 50 56 4D 55 55  ·~··w+·)urn:shal:REOJMPFTYJTCRXFRRW2WKPVMUU
3569 54 56 57 44 34 36 71 00 7E 00 10 78 70 73 71 00 7E 00 02 77 08 00 00 01 22 3E E0 AB 83 74 00 64 43 3A 5C 44 6F 63 75 6D 65 6E 74  TVWD46q·~··xpsq·~··w····">à«□t·dC:\Document
3612 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74 6F 70 5C 4C 69 6D 65 57 69 72 65 5C 62 72 6F 77 73 65  s and Settings\USER\Desktop\LimeWire\browse
3655 72 5C 78 75 6C 72 75 6E 6E 65 72 5C 72 65 73 5C 74 61 62 6C 65 2D 61 64 64 2D 72 6F 77 2D 62 65 66 6F 72 65 2D 68 6F 76 65 72 2E  r\xulrunner\res\table-add-row-before-hover.
3698 67 69 66 78 73 71 00 7E 00 05 73 71 00 7E 00 09 73 71 00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 45 4A 56 53 48 54 4B 46  gifxsq·~··sq·~·  sq·~··w+·)urn:shal:EJVSHTKF
3741 4B 46 33 44 49 44 45 4D 4F 4C 5A 42 4A 41 4F 57 37 49 46 32 49 4F 47 48 71 00 7E 00 10 78 70 73 71 00 7E 00 02 77 08 00 00 01 22  KF3DIDEMOLZBJAOW7IF2IOGHq·~··xpsq·~··w····"
3784 3E E0 AB B2 74 00 61 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74  >à«²t·aC:\Documents and Settings\USER\Deskt
```

Case 1\0\C\Documents and Settings\USER\Application Data\LimeWire\fileurns.cache



```
QJKQFKJZLq·~··xpsq·~··w····">à«·t·hC:\Docum
ents and Settings\USER\Desktop\LimeWire\bro
wser\xulrunner\res\table-add-column-before-
active.gifxsq·~··sq·~· sq·~··w+·)urn:shal:4
UYRPAAU3DO6GKK6Z5I6BVG6FDE565MVq·~··xpsq·~·
·w····"Y?f7t·1C:\Documents and Settings\USE
R\Desktop\export.txtxsq·~··sq·~· sq·~··w+·)
urn:shal:NHAMS65EUJNK3ZYIEME2LXITE3OVXOH6q·
~··xpsq·~··w····">à«²t·ZC:\Documents and Se
```

```
09 73 71 00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 51 36 56 35 37 44 37 35 59 5A 4F 52 50 49 37 35 50 58 42 43 43 4E 36
51 4A 4B 51 46 4B 4A 5A 4C 71 00 7E 00 10 78 70 73 71 00 7E 00 02 77 08 00 00 01 22 3E E0 AB 06 74 00 68 43 3A 5C 44 6F 63 75 6D
65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74 6F 70 5C 4C 69 6D 65 57 69 72 65 5C 62 72 6F
77 73 65 72 5C 78 75 6C 72 75 6E 6E 65 72 5C 72 65 73 5C 74 61 62 6C 65 2D 61 64 64 2D 63 6F 6C 75 6D 6E 2D 62 65 66 6F 72 65 2D
61 63 74 69 76 65 2E 67 69 66 78 73 71 00 7E 00 05 73 71 00 7E 00 09 73 71 00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 34
55 59 52 50 41 41 55 33 44 4F 36 47 4B 4B 36 5A 35 49 36 42 56 47 36 46 44 45 35 36 35 4D 56 71 00 7E 00 10 78 70 73 71 00 7E 00
02 77 08 00 00 01 22 59 3F 66 37 74 00 31 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 55 53 45
52 5C 44 65 73 6B 74 6F 70 5C 65 78 70 6F 72 74 2E 74 78 74 78 73 71 00 7E 00 05 73 71 00 7E 00 09 73 71 00 7E 00 0C 77 2B 00 29
75 72 6E 3A 73 68 61 31 3A 4E 48 41 4D 53 36 35 45 55 4A 4E 4B 33 5A 59 49 45 4D 45 32 4C 58 49 54 45 33 4F 56 58 4F 48 36 71 00
7E 00 10 78 70 73 71 00 7E 00 02 77 08 00 00 01 22 3E E0 AB B2 74 00 5A 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65
74 74 69 6E 67 73 5C 55 53 45 52 5C 44 65 73 6B 74 6F 70 5C 4C 69 6D 65 57 69 72 65 5C 62 72 6F 77 73 65 72 5C 78 75 6C 72 75 6E
6E 65 72 5C 72 65 73 5C 74 61 62 6C 65 2D 72 65 6D 6F 76 65 2D 72 6F 77 2E 67 69 66 78 73 71 00 7E 00 05 73 71 00 7E 00 09 73 71
00 7E 00 0C 77 2B 00 29 75 72 6E 3A 73 68 61 31 3A 52 45 4F 4A 4D 50 46 54 59 4A 54 43 52 58 46 52 52 57 32 57 4B 50 56 4D 55 55
```

When you go through your search hits note the length of these (sort them on length to see which ones exceed 255 characters) and manually bookmark these entries in their full length.

Comparing data from “library5.dat” and “fileurns.cache”

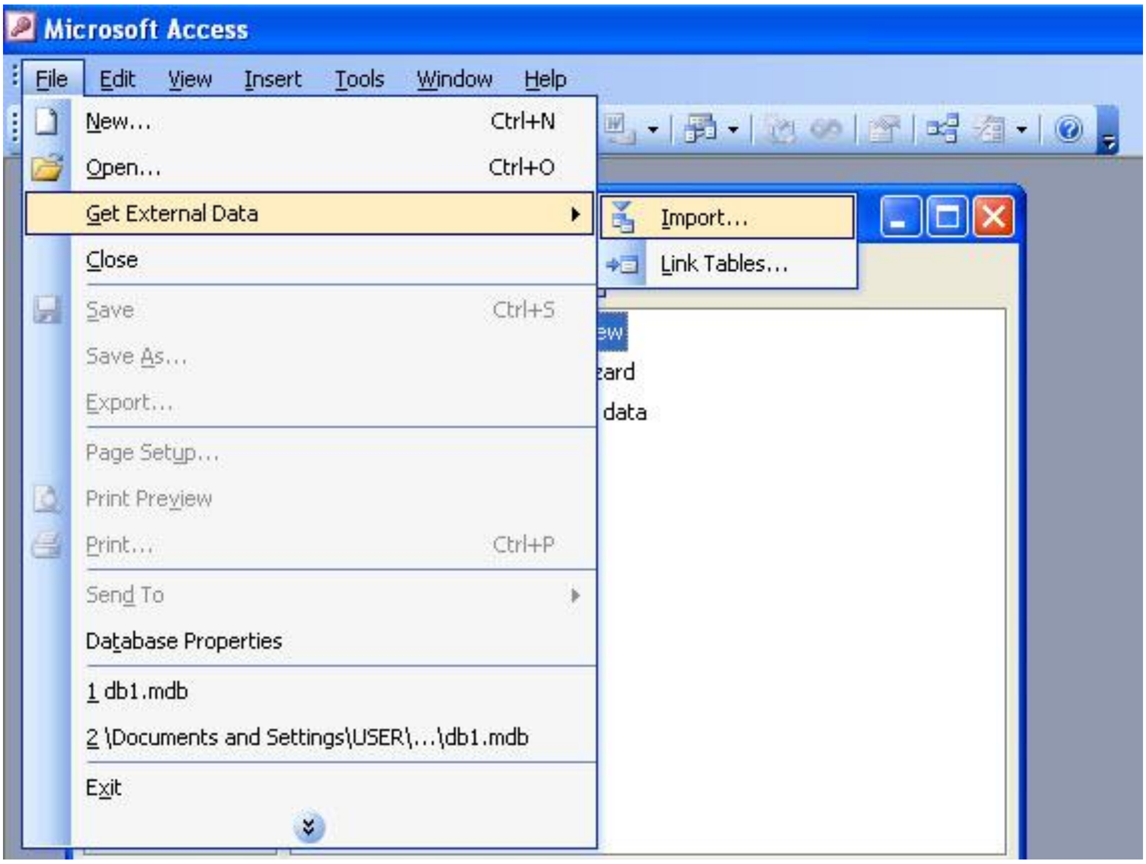
By using the above mentioned GREP searches, you should now have text documents containing the search hits.

To compare these data, you can use Microsoft Access. Before comparison you need to “clean up the data, and remove the “tag code”

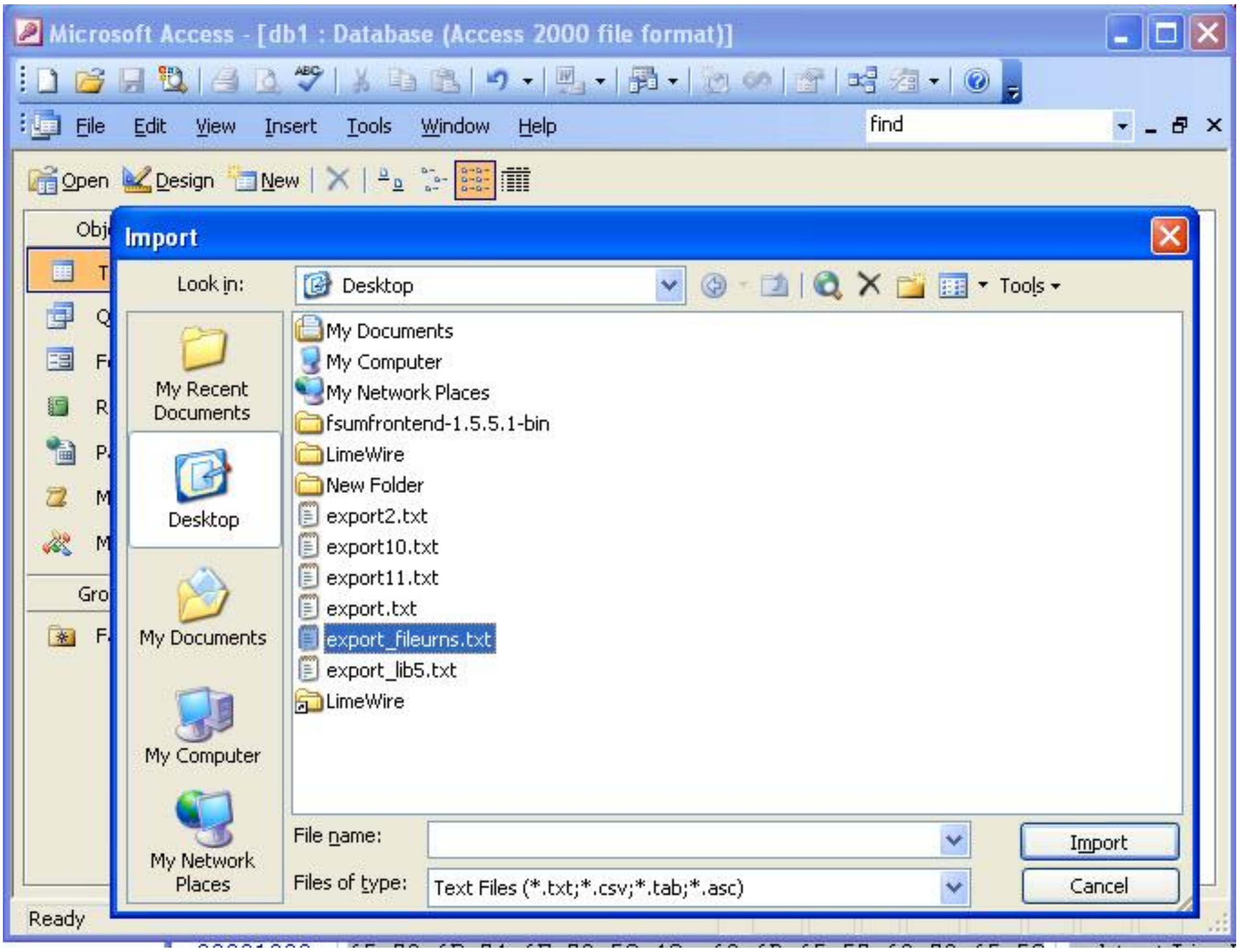
This procedure is a little tricky, but as soon a direct parser is made for the files – this is a way to get around the problem. To get the described procedures to work, you need to follow the naming of the fields and tables (unless you already is an Acces Ace ☺)

Open Access and create an empty database

Select <File> -> <Get External data> -> <Import>

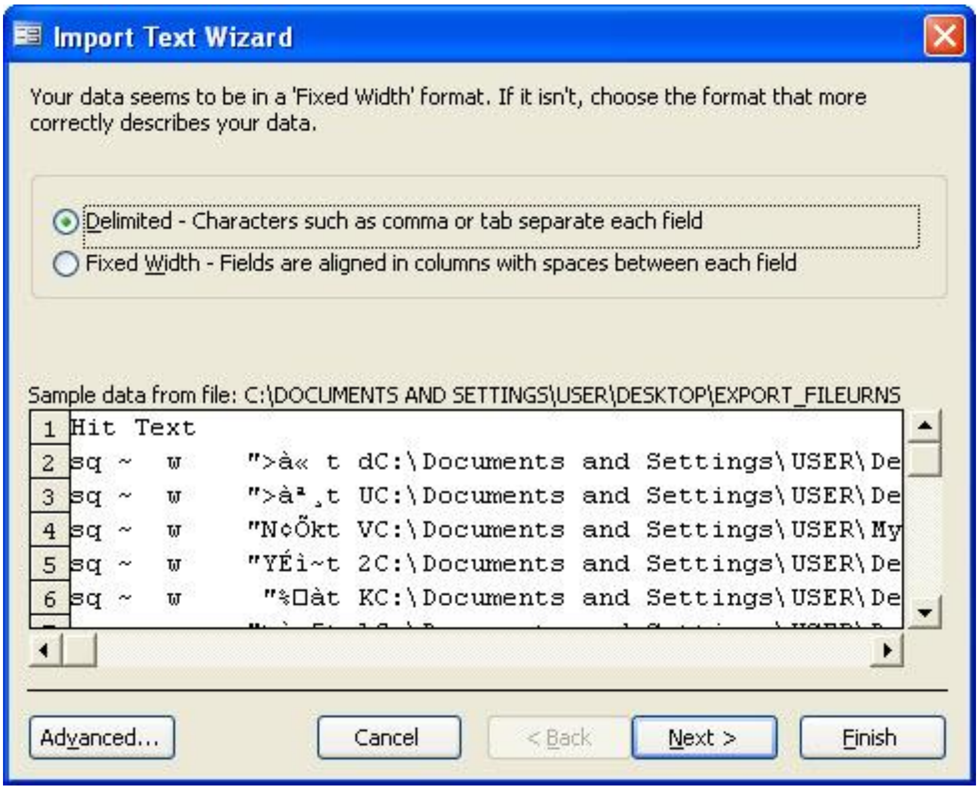


Browse to the exported data from “fileurns.cache”



Click <Import>

You will now get the opportunity to import the data into the database.



Import Text Wizard

Your data seems to be in a 'Fixed Width' format. If it isn't, choose the format that more correctly describes your data.

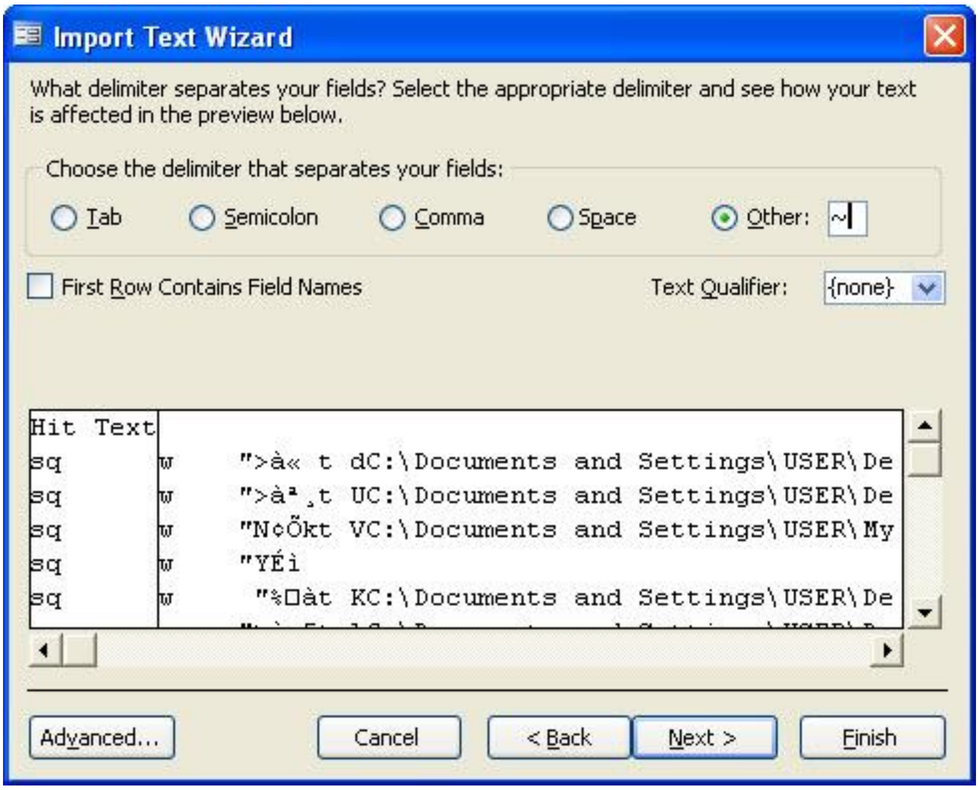
● Delimited - Characters such as comma or tab separate each field

○ Fixed Width - Fields are aligned in columns with spaces between each field

Sample data from file: C:\DOCUMENTS AND SETTINGS\USER\DESKTOP\EXPORT_FILEURNS

```
1 Hit Text
2 sq ~   w    ">à« t dC:\Documents and Settings\USER\De
3 sq ~   w    ">àª¸t UC:\Documents and Settings\USER\De
4 sq ~   w    "N¢Õkt VC:\Documents and Settings\USER\My
5 sq ~   w    "YÉi~t 2C:\Documents and Settings\USER\De
6 sq ~   w     "%□àt KC:\Documents and Settings\USER\De
```

Select <Delimited> import – click <Next>



Import Text Wizard

What delimiter separates your fields? Select the appropriate delimiter and see how your text is affected in the preview below.

Choose the delimiter that separates your fields:

○ Tab ○ Semicolon ○ Comma ○ Space ● Other: ~

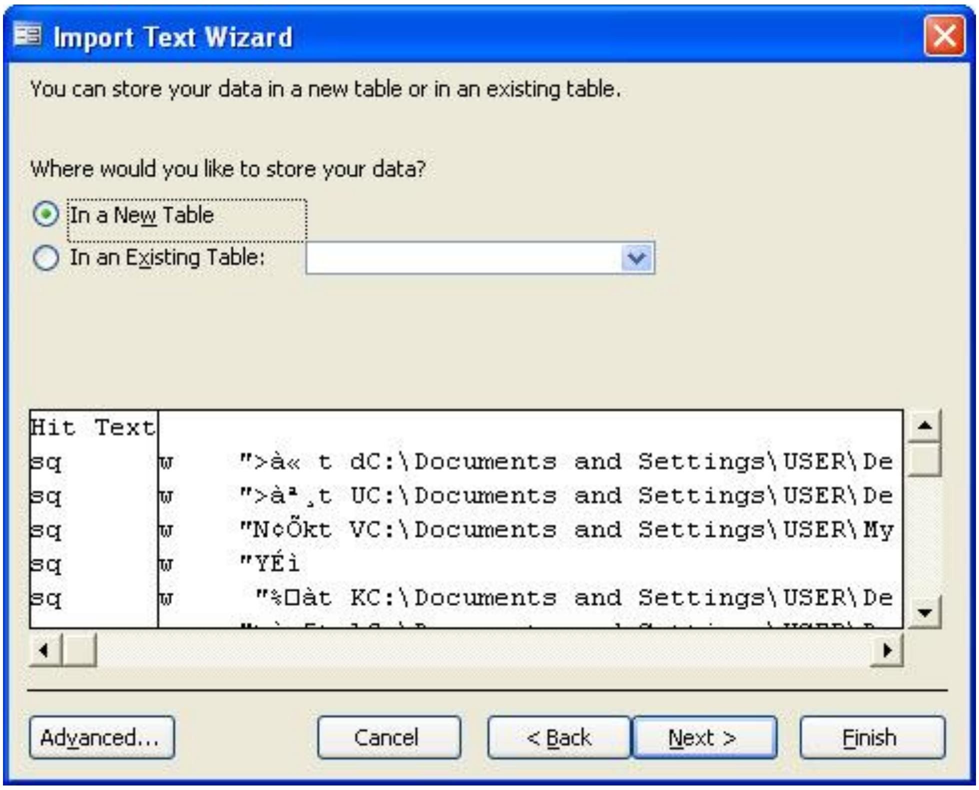
□ First Row Contains Field Names

Text Qualifier: {none}

```
Hit Text
sq        w    ">à« t dC:\Documents and Settings\USER\De
sq        w    ">àª¸t UC:\Documents and Settings\USER\De
sq        w    "N¢Õkt VC:\Documents and Settings\USER\My
sq        w    "YÉi
sq        w     "%□àt KC:\Documents and Settings\USER\De
```

Choose the “~ “ (tilde) as your separator

Click <Next>



You can store your data in a new table or in an existing table.

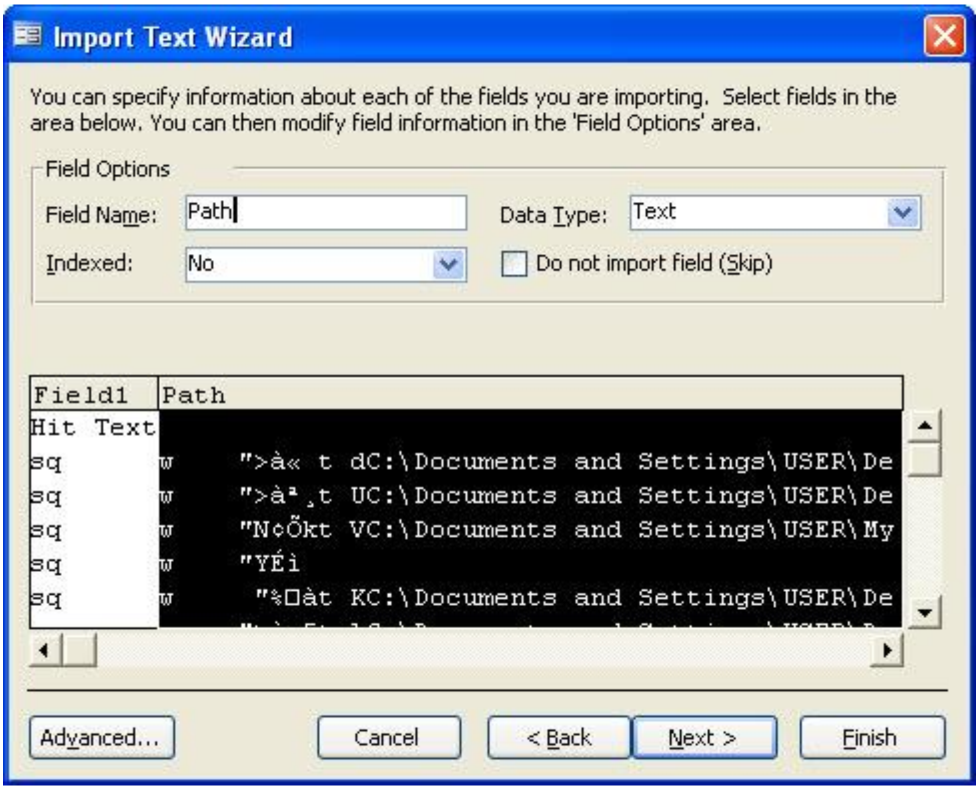
Where would you like to store your data?

● In a New Table

○ In an Existing Table:

```
Hit  Text
sq        w     ">à« t dC:\Documents and Settings\USER\De
sq        w     ">à² ¸t UC:\Documents and Settings\USER\De
sq        w     "N¢Ökt VC:\Documents and Settings\USER\My
sq        w     "YÉì
sq        w      "%□àt KC:\Documents and Settings\USER\De
```

Select <In a new table> - click <Next>



You can specify information about each of the fields you are importing. Select fields in the area below. You can then modify field information in the 'Field Options' area.

Field Options

Field Name: Path

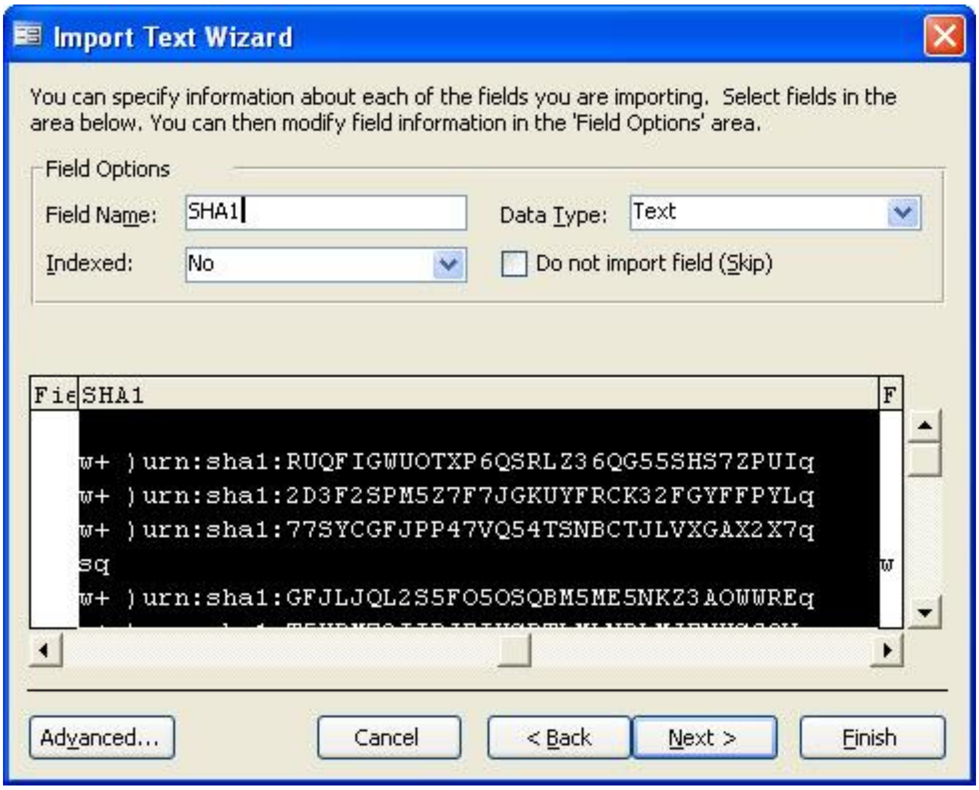
Data Type: Text

Indexed: No

□ Do not import field (Skip)

```
Field1   Path
Hit  Text
sq        w     ">à« t dC:\Documents and Settings\USER\De
sq        w     ">à² ¸t UC:\Documents and Settings\USER\De
sq        w     "N¢Ökt VC:\Documents and Settings\USER\My
sq        w     "YÉì
sq        w      "%□àt KC:\Documents and Settings\USER\De
```

In the next window you get the opportunity to name the single fields in the table. In Field1 you rename it to "Path"



You can specify information about each of the fields you are importing. Select fields in the area below. You can then modify field information in the 'Field Options' area.

Field Options

Field Name: SHA1

Data Type: Text

Indexed: No

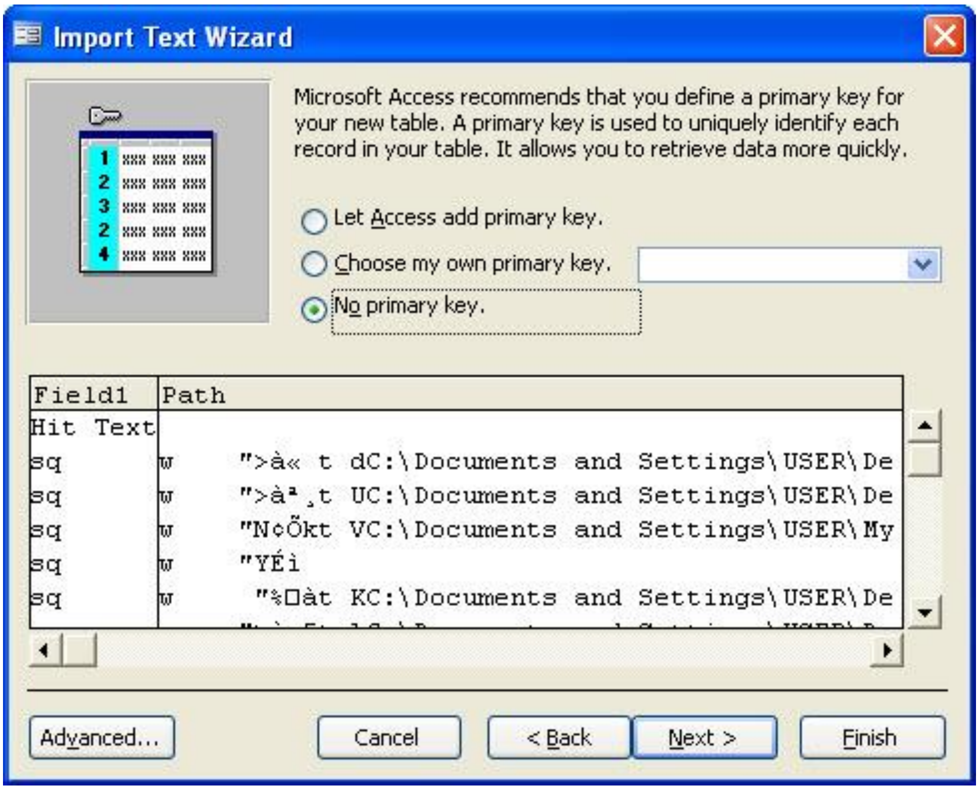
□ Do not import field (Skip)

```
Fie SHA1                                              F

w+ )urn:sha1:RUQFIGWUOTXP6QSRLZ36QG55SHS7ZPUIq
w+ )urn:sha1:2D3F2SPM5Z7F7JGKUYFRCK32FGYFFPYLq
w+ )urn:sha1:77SYCGFJPP47VQ54TSNBCTJLVXGAX2X7q
sq                                                    w
w+ )urn:sha1:GFJLJQL2S5FO5OSQBM5ME5NKZ3AOWWREq
```

Field5 you rename to "SHA1"

Click <Next>



Microsoft Access recommends that you define a primary key for your new table. A primary key is used to uniquely identify each record in your table. It allows you to retrieve data more quickly.

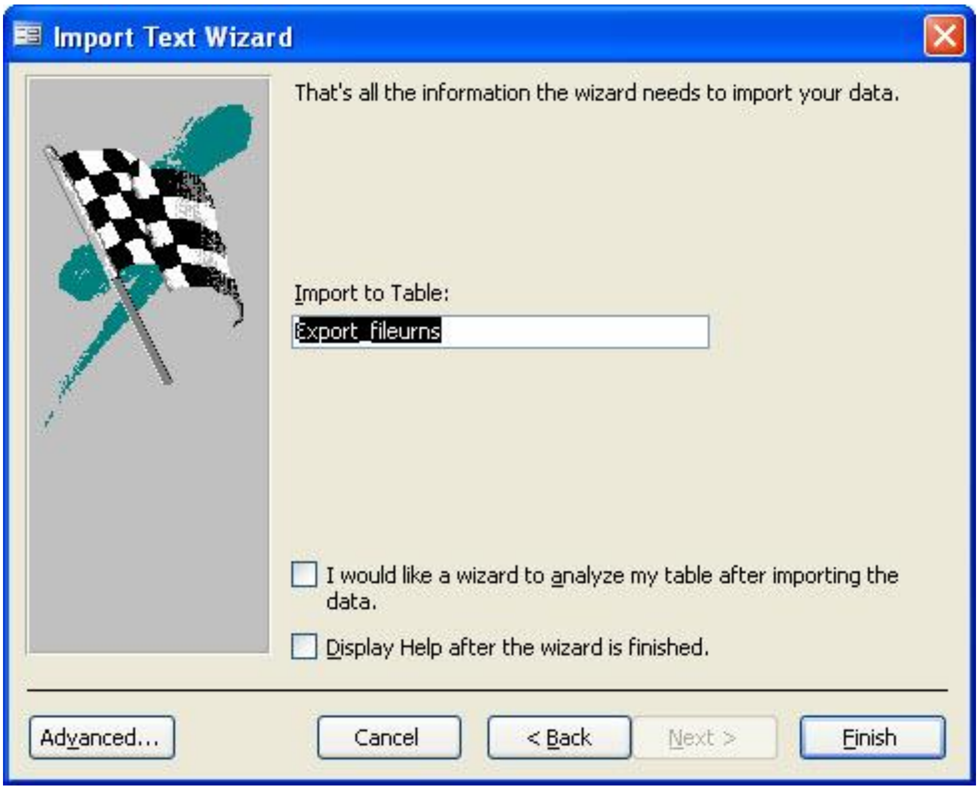
○ Let Access add primary key.

○ Choose my own primary key.

● No primary key.

```
Field1   Path
Hit  Text
sq       w     ">à« t dC:\Documents and Settings\USER\De
sq       w     ">à²¸t UC:\Documents and Settings\USER\De
sq       w     "N¢Õkt VC:\Documents and Settings\USER\My
sq       w     "YÉì
sq       w      "%□àt KC:\Documents and Settings\USER\De
```

Select <No primary key> - Click <Next>



That's all the information the wizard needs to import your data.

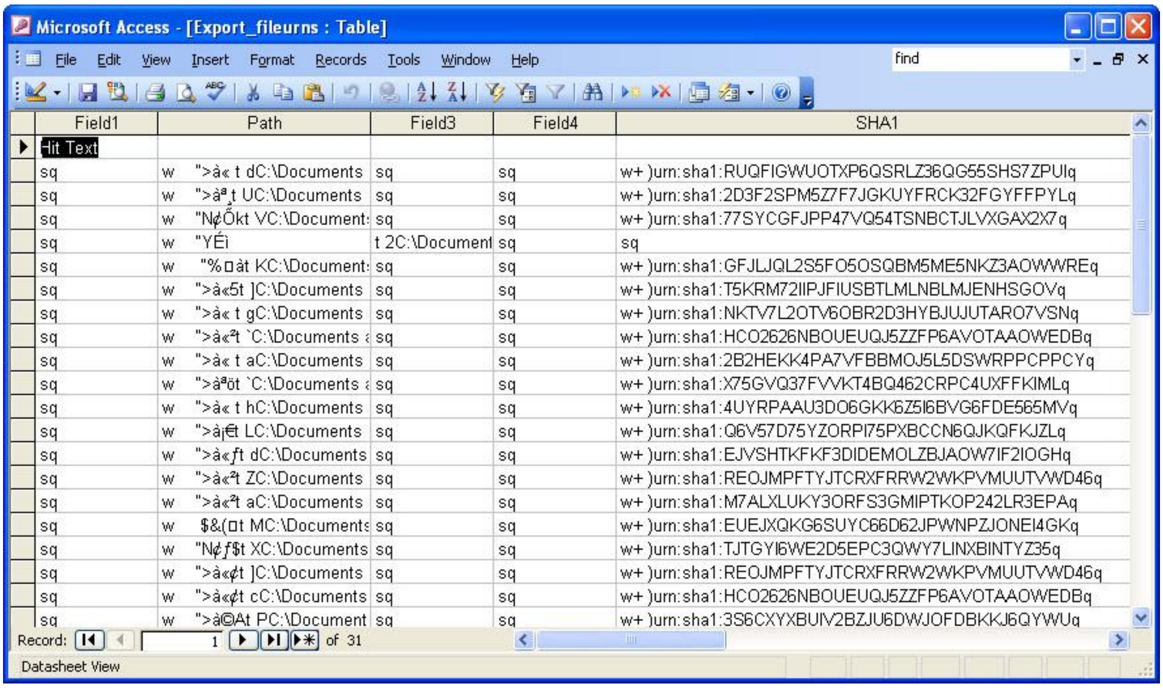
Import to Table:

Export_fileurns

□ I would like a wizard to analyze my table after importing the data.

□ Display Help after the wizard is finished.

You have now imported the data. Click <Finish>


Microsoft Access - [Export_fileurns : Table]
File Edit View Insert Format Records Tools Window Help
find

Field1	Path	Field3	Field4	SHA1
Hit Text				
sq	w ">à« t dC:\Documents	sq	sq	w+)urn:sha1:RUQFIGWUOTXP6QSRLZ36QG55SHS7ZPUIq
sq	w ">àª¸t UC:\Documents	sq	sq	w+)urn:sha1:2D3F2SPM5Z7F7JGKUYFRCK32FGYFFPYLq
sq	w "N¢Őkt VC:\Document:	sq	sq	w+)urn:sha1:77SYCGFJPP47VQ54TSNBCTJLVXGAX2X7q
sq	w "YÉì	t 2C:\Document	sq	sq
sq	w "%□àt KC:\Document:	sq	sq	w+)urn:sha1:GFJLJQL2S5FO5OSQBM5ME5NKZ3AOWWREq
sq	w ">à«5t]C:\Documents	sq	sq	w+)urn:sha1:T5KRM72IIPJFIUSBTLMLNBLMJENHSGOVq
sq	w ">à« t gC:\Documents	sq	sq	w+)urn:sha1:NKTV7L2OTV6OBR2D3HYBJUJUTARO7VSNq
sq	w ">à«²t `C:\Documents ;	sq	sq	w+)urn:sha1:HCO2626NBOUEUQJ5ZZFP6AVOTAAOWEDBq
sq	w ">à« t aC:\Documents	sq	sq	w+)urn:sha1:2B2HEKK4PA7VFBBMOJ5L5DSWRPPCPPCYq
sq	w ">àªöt `C:\Documents ;	sq	sq	w+)urn:sha1:X75GVQ37FVVKT4BQ462CRPC4UXFFKIMLq
sq	w ">à« t hC:\Documents	sq	sq	w+)urn:sha1:4UYRPAAU3DO6GKK6Z5I6BVG6FDE565MVq
sq	w ">à¡€t LC:\Documents	sq	sq	w+)urn:sha1:Q6V57D75YZORPI75PXBCCN6QJKQFKJZLq
sq	w ">à«ƒt dC:\Documents	sq	sq	w+)urn:sha1:EJVSHTKFKF3DIDEMOLZBJAOW7IF2IOGHq
sq	w ">à«²t ZC:\Documents	sq	sq	w+)urn:sha1:REOJMPFTYJTCRXFRRW2WKPVMUUTVWD46q
sq	w ">à«²t aC:\Documents	sq	sq	w+)urn:sha1:M7ALXLUKY3ORFS3GMIPTKOP242LR3EPAq
sq	w $&(□t MC:\Documents	sq	sq	w+)urn:sha1:EUEJXQKG6SUYC66D62JPWNPZJONEI4GKq
sq	w "N¢ƒ$t XC:\Documents	sq	sq	w+)urn:sha1:TJTGYI6WE2D5EPC3QWY7LINXBINTYZ35q
sq	w ">à«¢t]C:\Documents	sq	sq	w+)urn:sha1:REOJMPFTYJTCRXFRRW2WKPVMUUTVWD46q
sq	w ">à«¢t cC:\Documents	sq	sq	w+)urn:sha1:HCO2626NBOUEUQJ5ZZFP6AVOTAAOWEDBq
sq	w ">à©At PC:\Document	sq	sq	w+)urn:sha1:3S6CXYXBUIV2BZJU6DWJOFDBKKJ6QYWUq

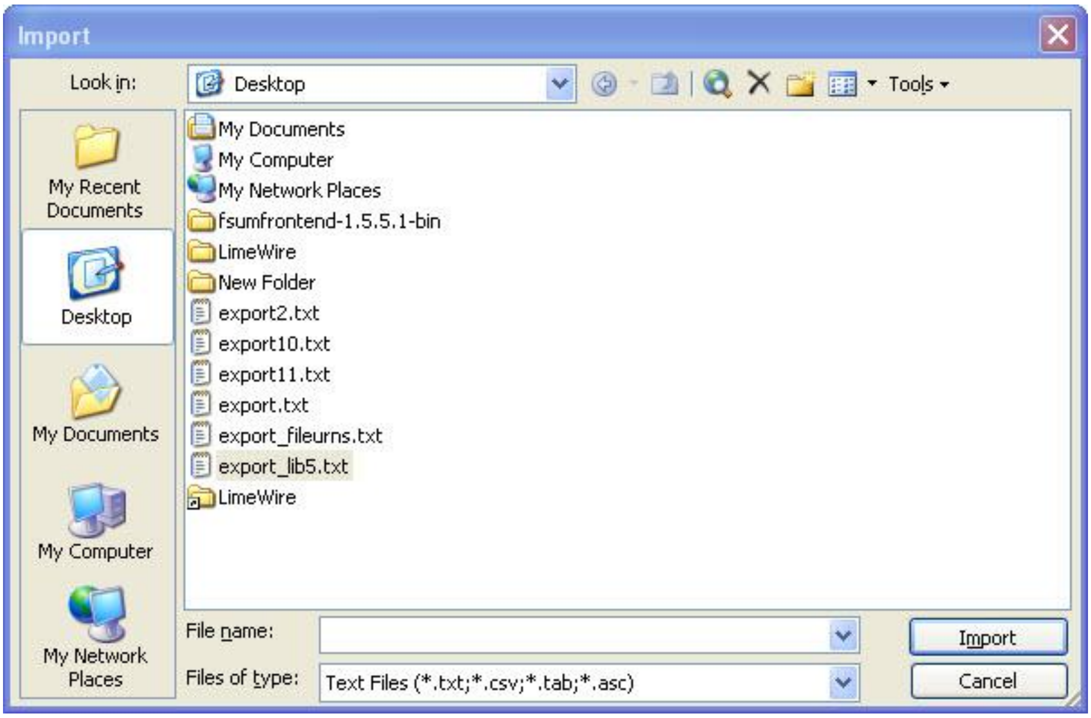
Record: 1 of 31

Datasheet View

Go to the main window and open the table and see the imported data. As you can see, there are data, which needs to be removed

We now need to import the data from the “Libray5.dat” file

Go to <File> -> <Get External data> -> <Import>

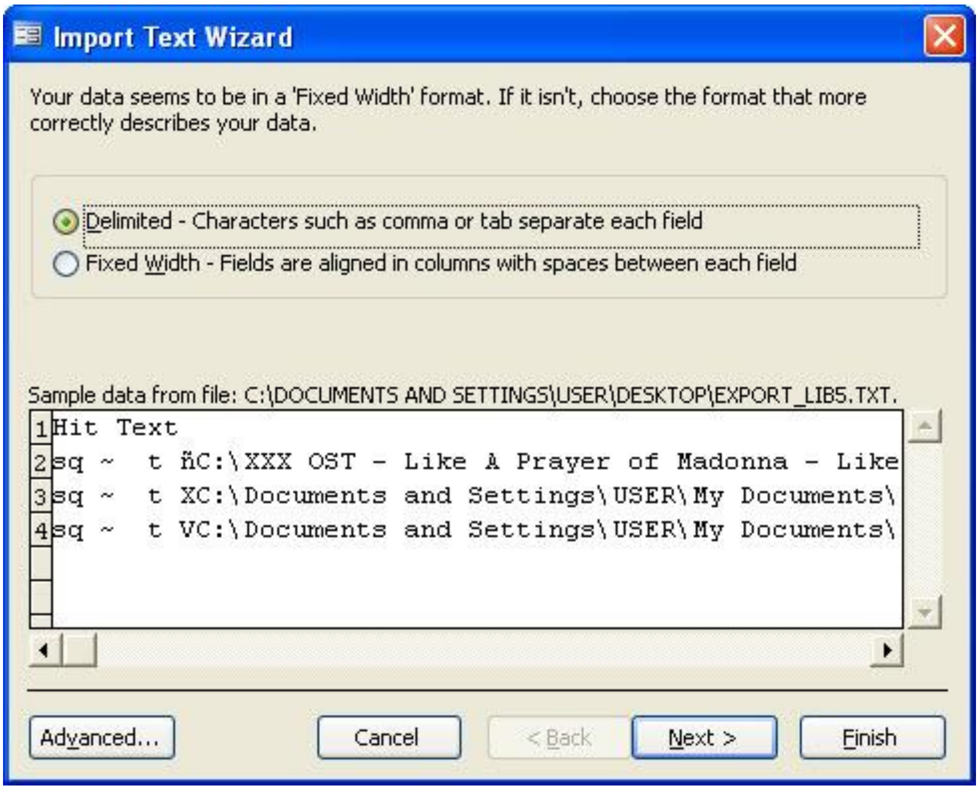


Look in: Desktop

File name:

Files of type: Text Files (*.txt;*.csv;*.tab;*.asc)

Click <Import>



Import Text Wizard

Your data seems to be in a 'Fixed Width' format. If it isn't, choose the format that more correctly describes your data.

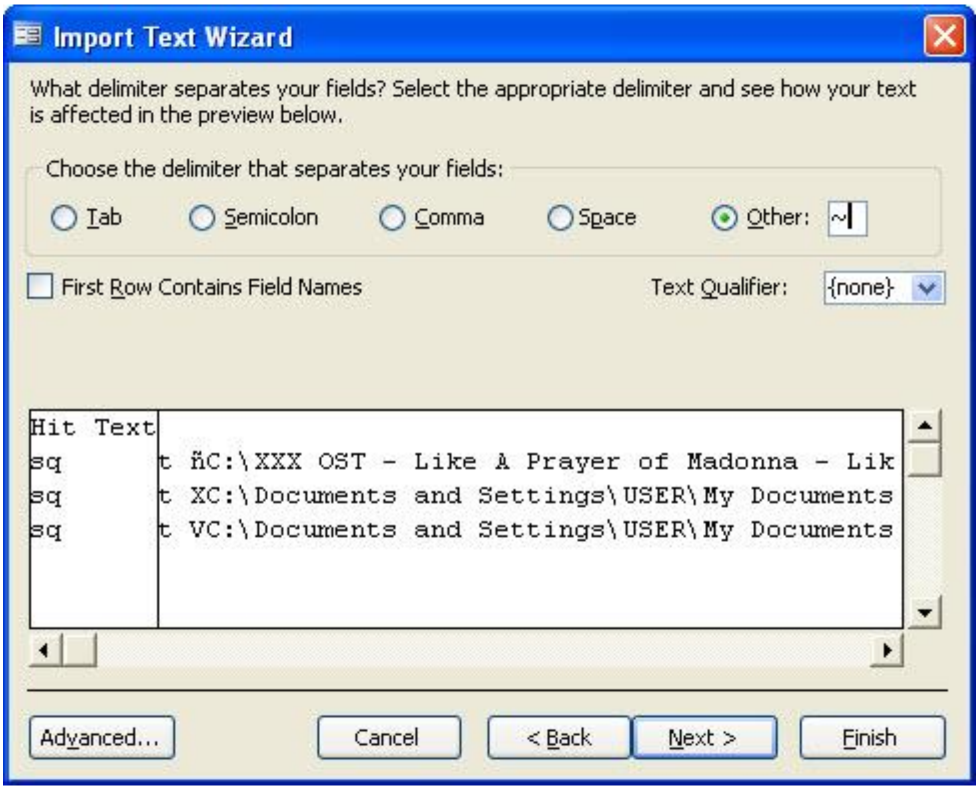
● Delimited - Characters such as comma or tab separate each field

○ Fixed Width - Fields are aligned in columns with spaces between each field

Sample data from file: C:\DOCUMENTS AND SETTINGS\USER\DESKTOP\EXPORT_LIB5.TXT.

```
1 Hit  Text
2 sq  ~   t ñC:\XXX OST - Like A Prayer of Madonna - Like
3 sq  ~   t XC:\Documents and Settings\USER\My Documents\
4 sq  ~   t VC:\Documents and Settings\USER\My Documents\
```

Like previous import – select <Delimited> import – Click <Next>



Import Text Wizard

What delimiter separates your fields? Select the appropriate delimiter and see how your text is affected in the preview below.

Choose the delimiter that separates your fields:

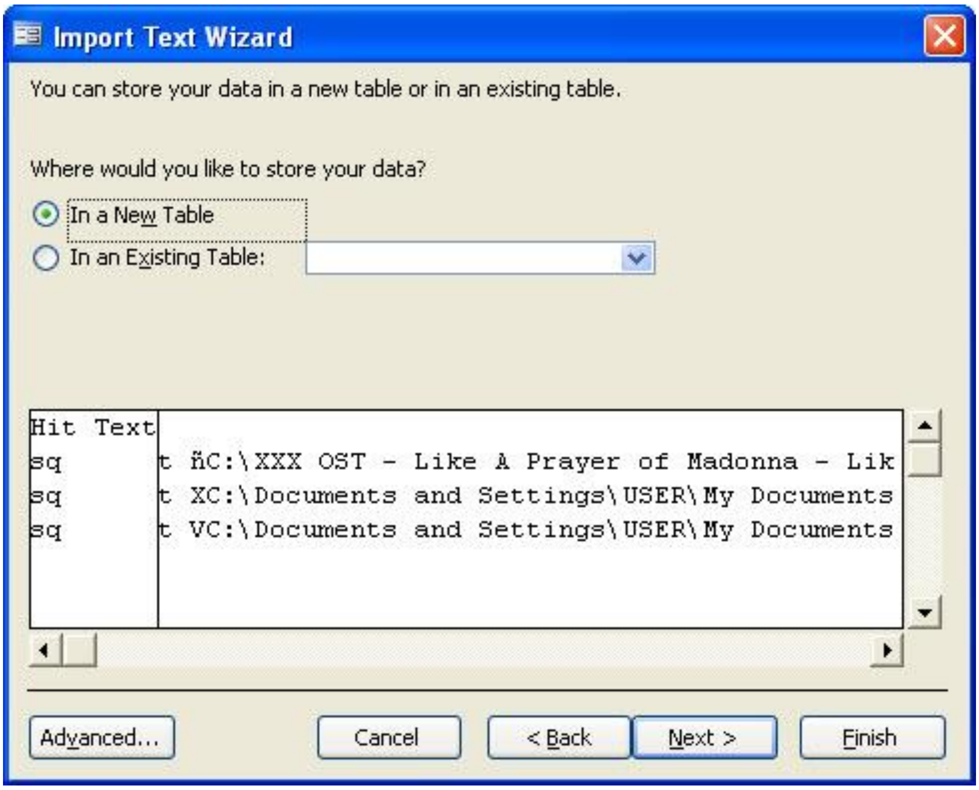
○ Tab ○ Semicolon ○ Comma ○ Space ● Other: ~

□ First Row Contains Field Names

Text Qualifier: {none}

```
Hit  Text
sq        t ñC:\XXX OST - Like A Prayer of Madonna - Lik
sq        t XC:\Documents and Settings\USER\My Documents
sq        t VC:\Documents and Settings\USER\My Documents
```

Again – choose the "~" as your separator – Click <Next>



You can store your data in a new table or in an existing table.

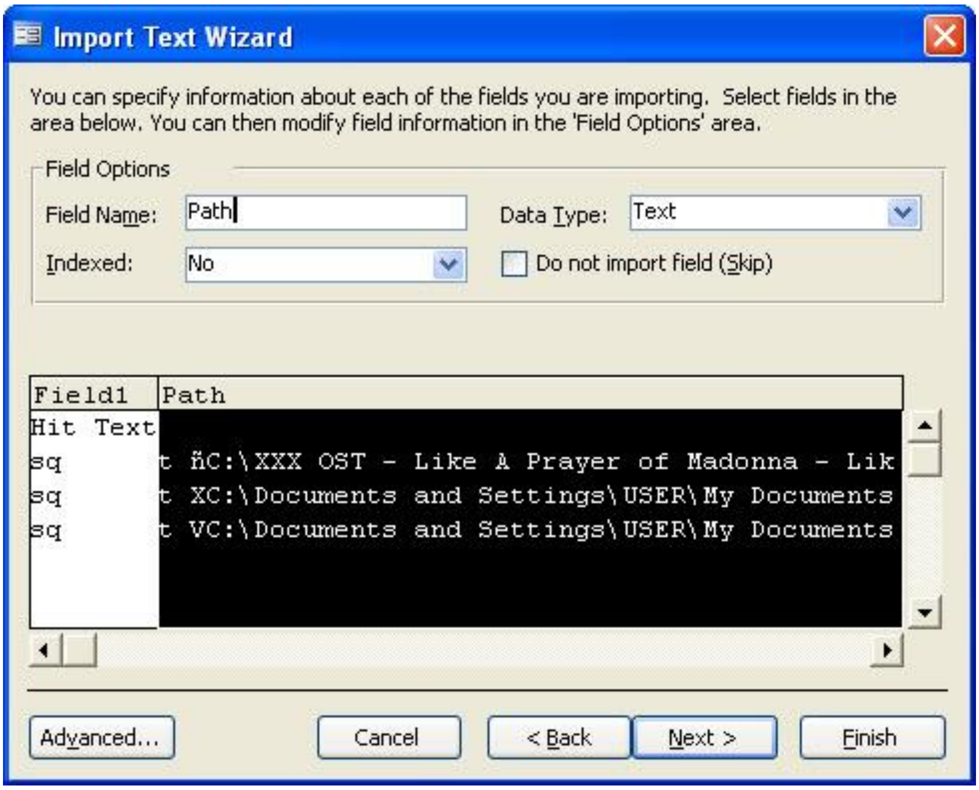
Where would you like to store your data?

● In a New Table

○ In an Existing Table:

```
Hit Text
sq      t ñC:\XXX OST - Like A Prayer of Madonna - Lik
sq      t XC:\Documents and Settings\USER\My Documents
sq      t VC:\Documents and Settings\USER\My Documents
```

Select <In a new table> and create a new table for the data Click <Next>



You can specify information about each of the fields you are importing. Select fields in the area below. You can then modify field information in the 'Field Options' area.

Field Options

Field Name: Path

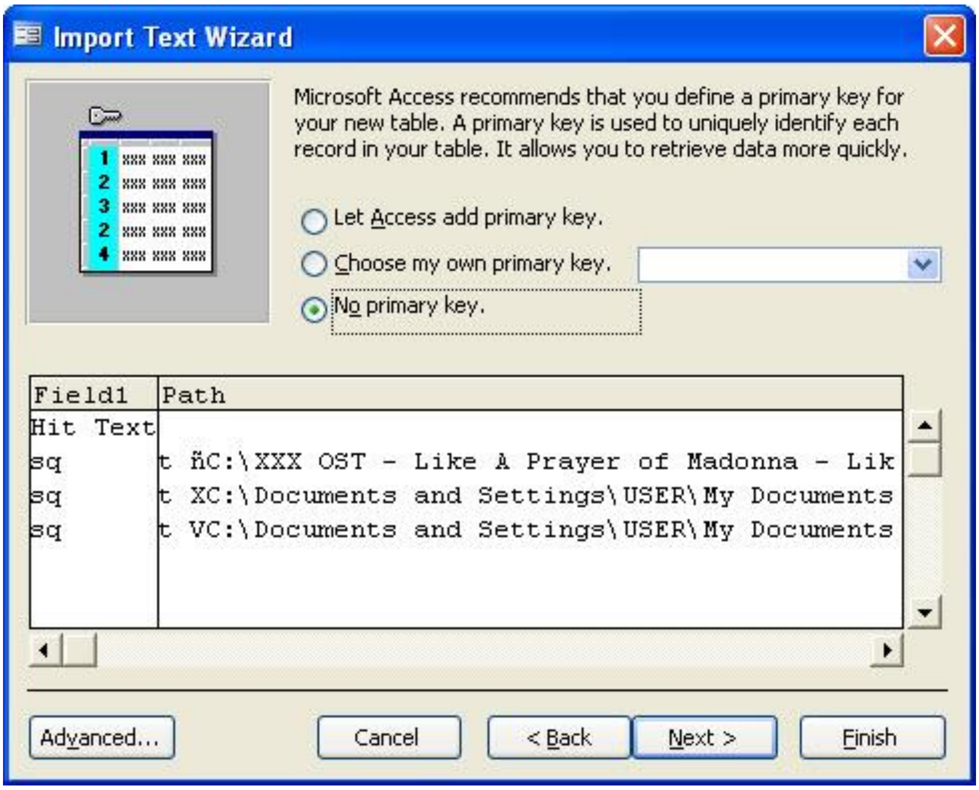
Data Type: Text

Indexed: No

□ Do not import field (Skip)

```
Field1  Path
Hit Text
sq      t ñC:\XXX OST - Like A Prayer of Madonna - Lik
sq      t XC:\Documents and Settings\USER\My Documents
sq      t VC:\Documents and Settings\USER\My Documents
```

Rename “Field2” to “Path” – click <Next>



Import Text Wizard

Microsoft Access recommends that you define a primary key for your new table. A primary key is used to uniquely identify each record in your table. It allows you to retrieve data more quickly.

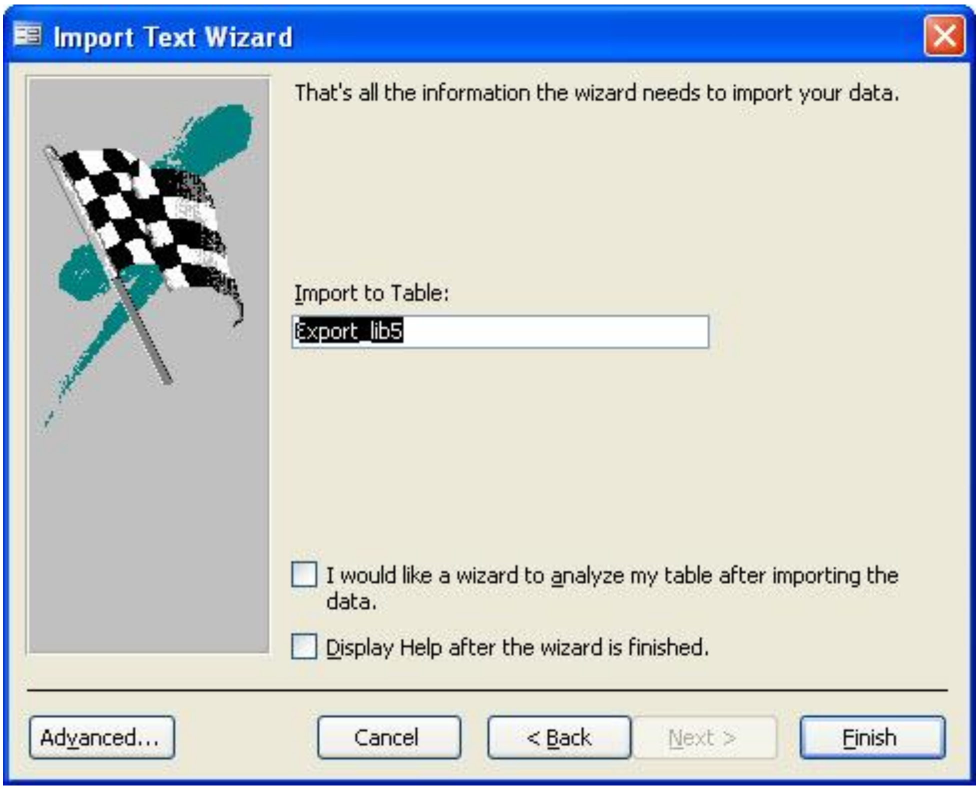
○ Let Access add primary key.

○ Choose my own primary key.

● No primary key.

```
Field1     Path
Hit Text
sq         t ñC:\XXX OST - Like A Prayer of Madonna - Lik
sq         t XC:\Documents and Settings\USER\My Documents
sq         t VC:\Documents and Settings\USER\My Documents
```

Choose <No primary key> - Click <Next>



Import Text Wizard

That's all the information the wizard needs to import your data.

Import to Table:

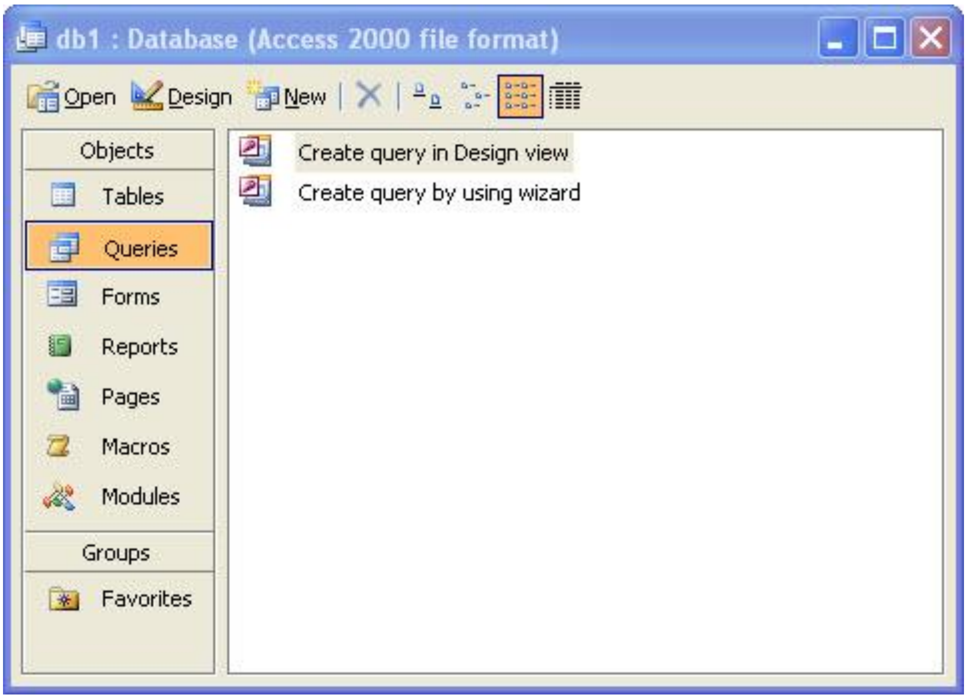
Export_lib5

□ I would like a wizard to analyze my table after importing the data.

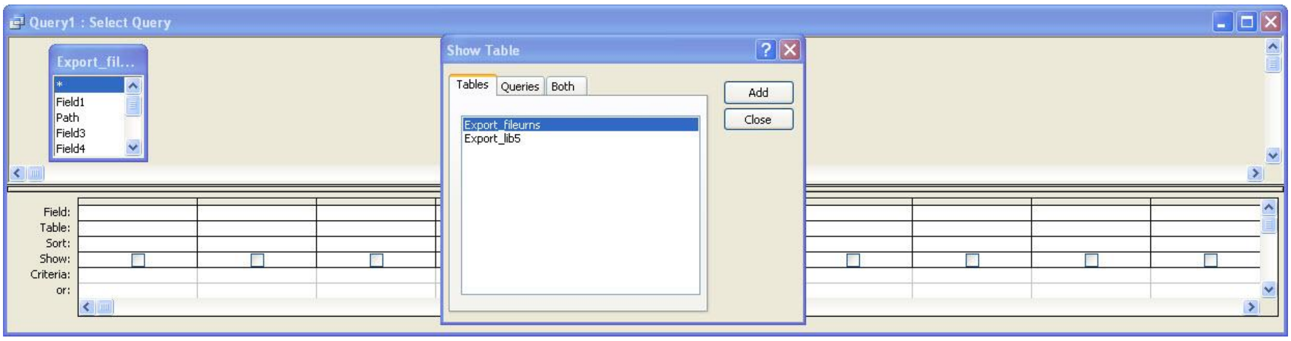
□ Display Help after the wizard is finished.

You have now imported the data into the new table.

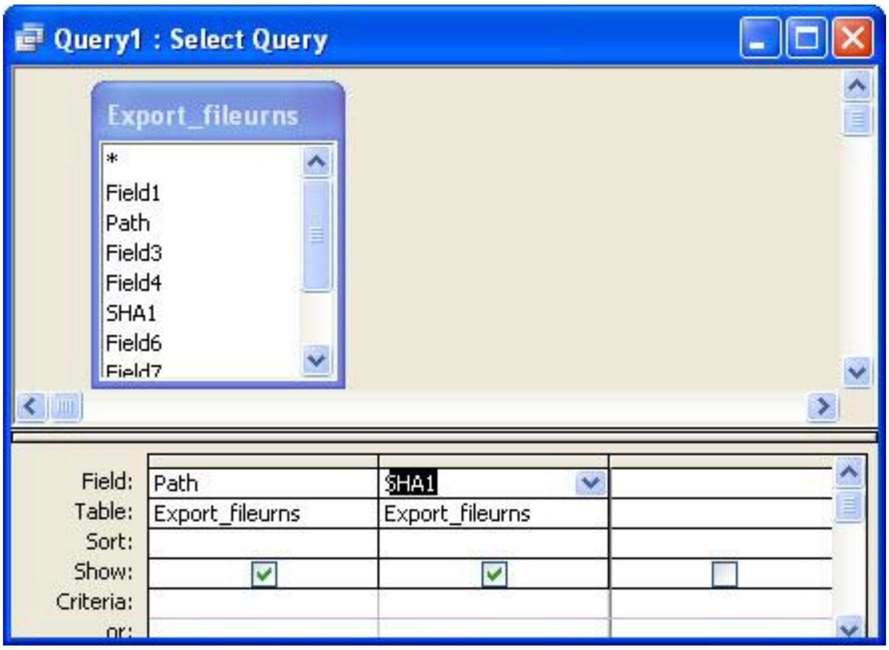
To clean out some of the data use the queries shown below


db1 : Database (Access 2000 file format)
Open
Design
New
Objects
Tables
Queries
Forms
Reports
Pages
Macros
Modules
Groups
Favorites
Create query in Design view
Create query by using wizard

Select <Queries> -> <Create a query in Design view>

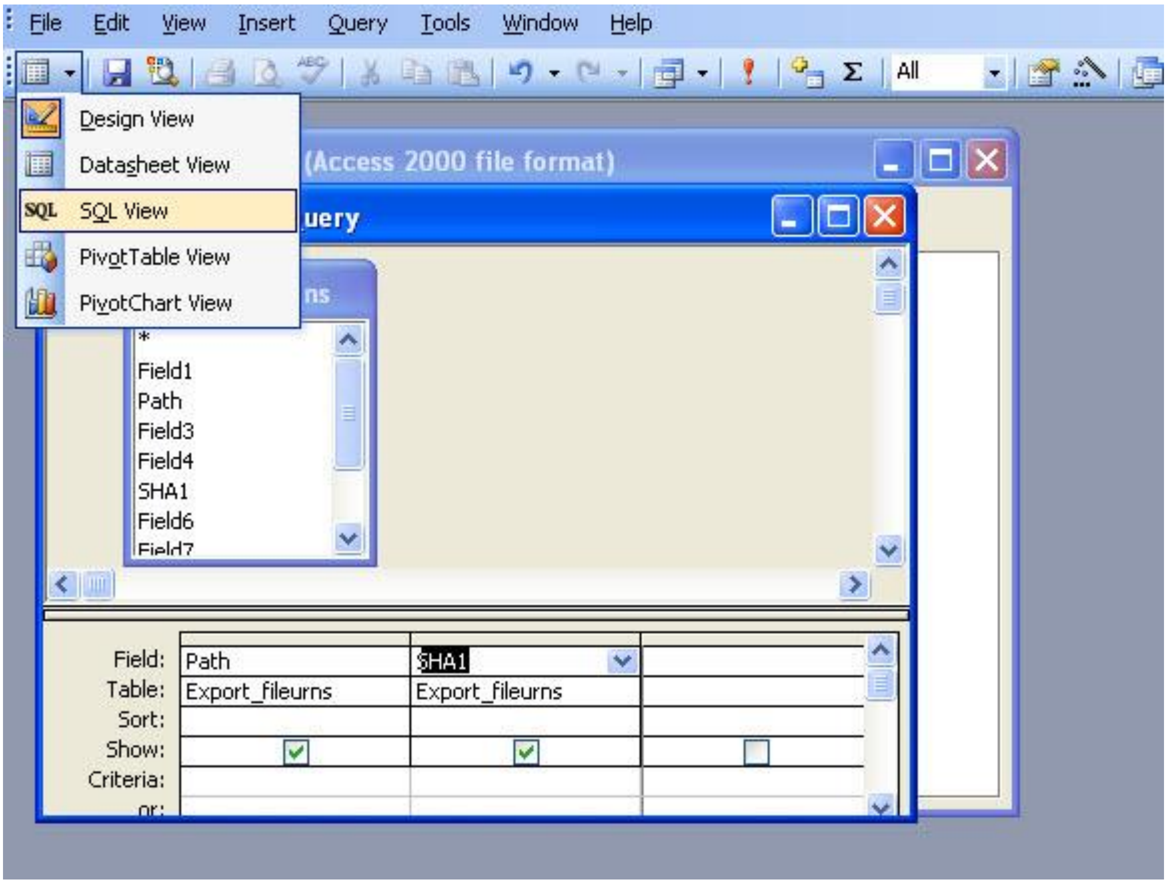


Doubleclick the “Export_fileurns” table and click <Close>



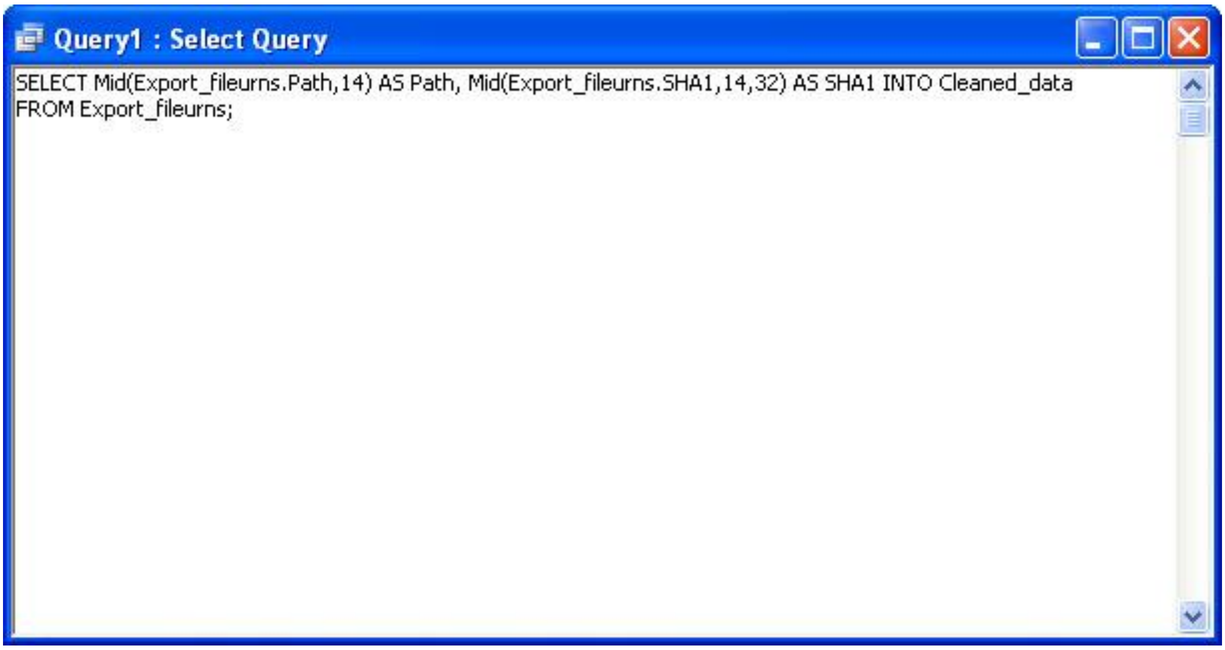
Field:	Path	SHA1	
Table:	Export_fileurns	Export_fileurns	
Sort:			
Show:	☑	☑	□
Criteria:			
or:			

Drag the fields “Path” and “SHA1” to the “Field box”



Field:	Path	SHA1	
Table:	Export_fileurns	Export_fileurns	
Sort:			
Show:	☑	☑	□
Criteria:			
or:			

Click the arrow next to the “View button” and select <SQL View>

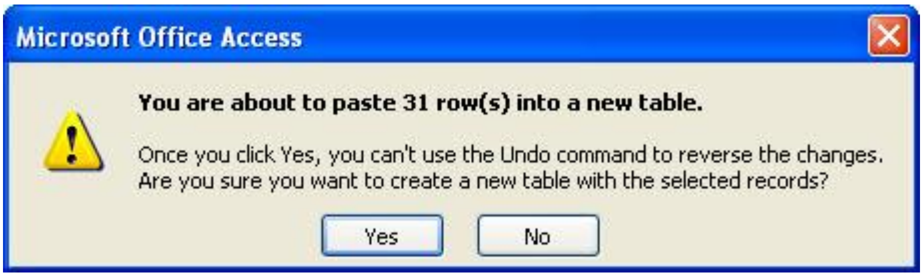


```
SELECT Mid(Export_fileurns.Path,14) AS Path, Mid(Export_fileurns.SHA1,14,32) AS SHA1 INTO Cleaned_data
FROM Export_fileurns;
```

Paste the following text in to the query window

SELECT Mid(Export_fileurns.Path,14) AS Path, Mid(Export_fileurns.SHA1,14,32) AS SHA1 INTO Cleaned_data FROM Export_fileurns;

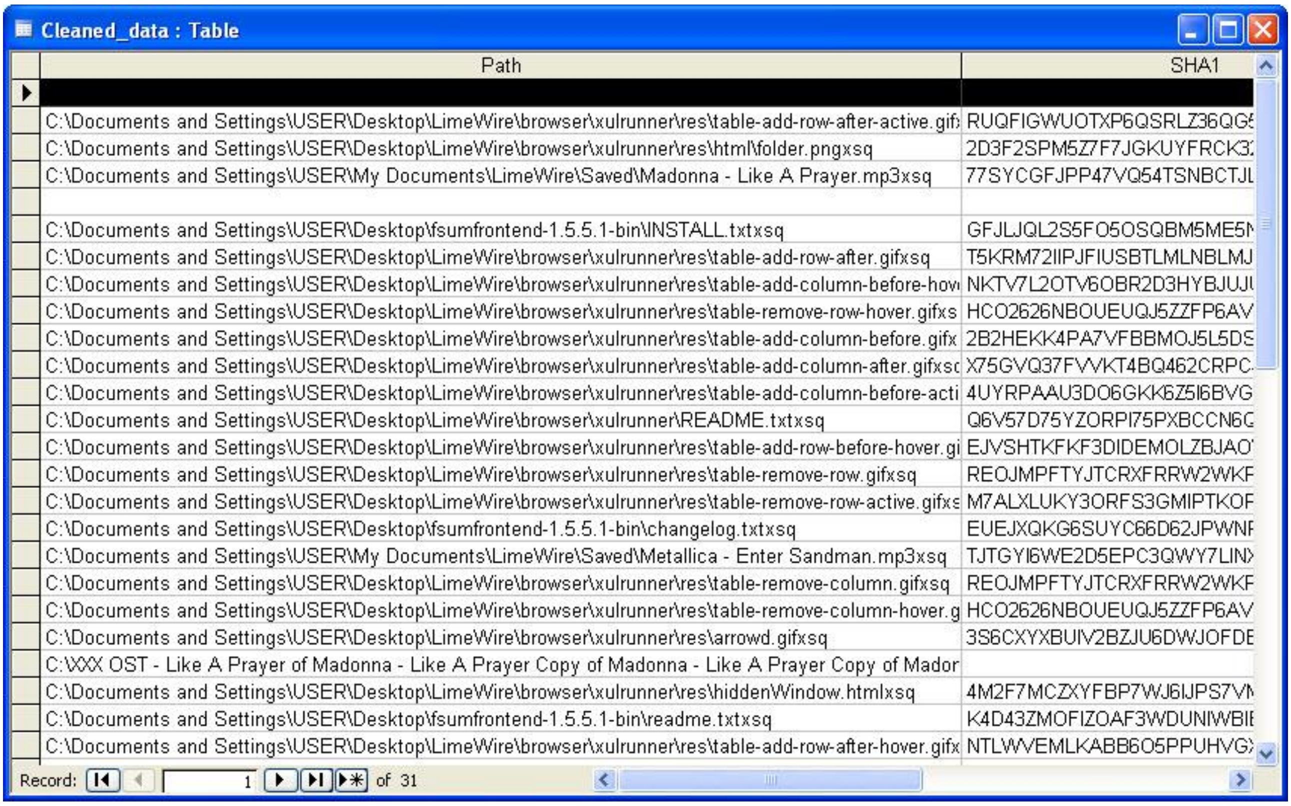
Click the read Exclamation mark on the top menu to run the query



You are about to paste 31 row(s) into a new table.

Once you click Yes, you can't use the Undo command to reverse the changes.
Are you sure you want to create a new table with the selected records?

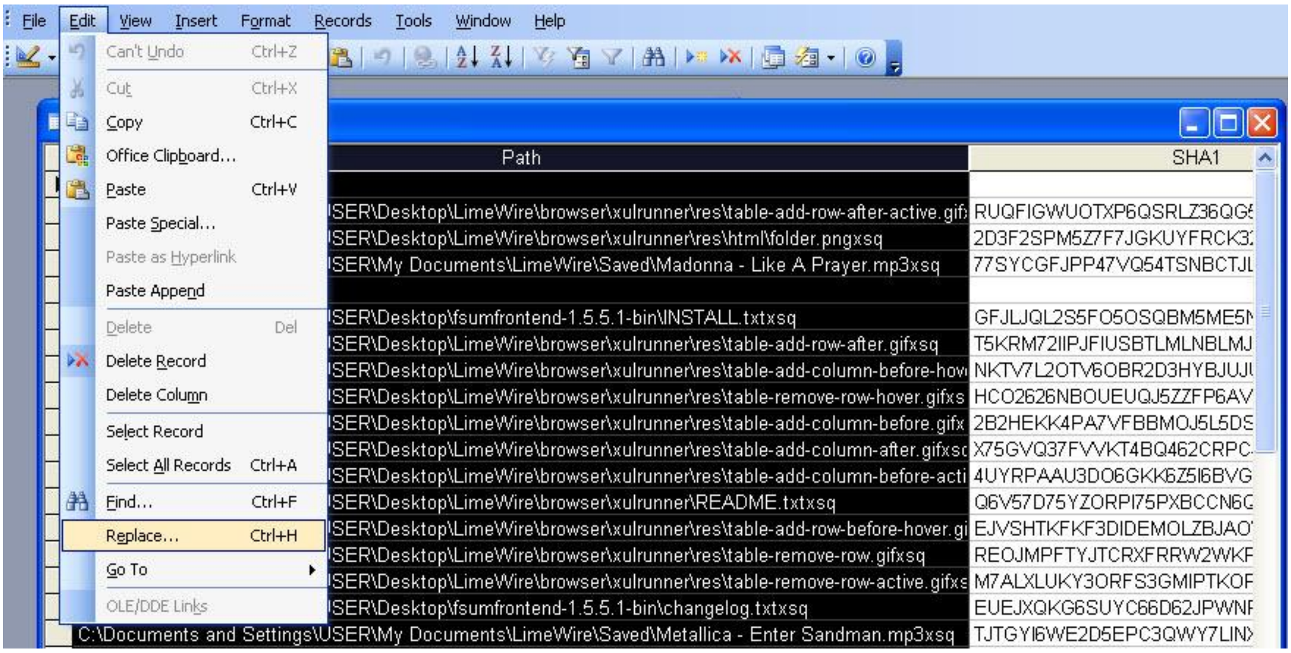
Select <Yes>



Cleaned_data : Table

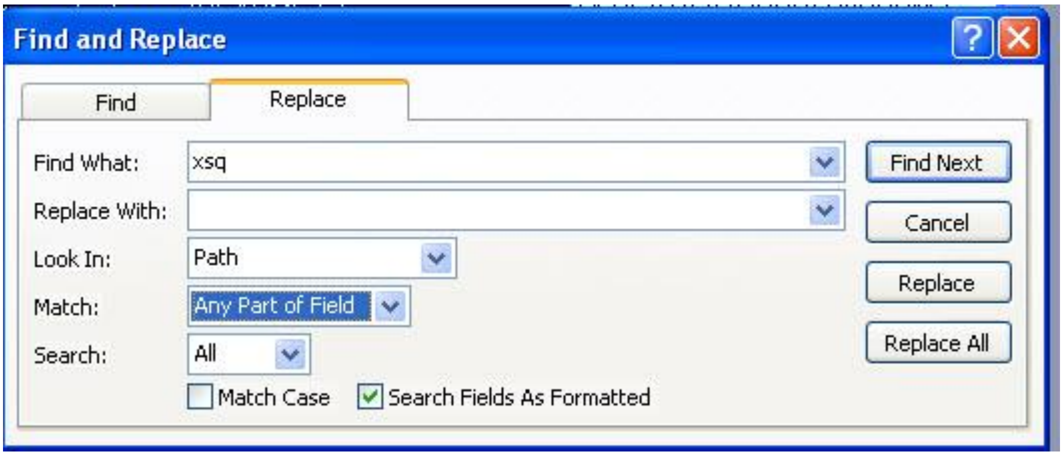
Path	SHA1
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-add-row-after-active.gif	RUQFIGWUOTXP6QSRLZ36QG
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\html\folder.pngxsq	2D3F2SPM5Z7F7JGKUYFRCK3
C:\Documents and Settings\USER\My Documents\LimeWire\Saved\Madonna - Like A Prayer.mp3xsq	77SYCGFJPP47VQ54TSNBCTJL
C:\Documents and Settings\USER\Desktop\fsumfrontend-1.5.5.1-bin\INSTALL.txtxsq	GFJLJQL2S5FO5OSQBM5ME5
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-add-row-after.gifxsq	T5KRM72IIPJFIUSBTLMLNBLMJ
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-add-column-before-hov	NKTV7L2OTV6OBR2D3HYBJUJ
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-remove-row-hover.gifxs	HCO2626NBOUEUQJ5ZZFP6AV
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-add-column-before.gifx	2B2HEKK4PA7VFBBMOJ5L5DS
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-add-column-after.gifxsc	X75GVQ37FVVKT4BQ462CRPC
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-add-column-before-acti	4UYRPAAU3DO6GKK6Z5I6BVG
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\README.txtxsq	Q6V57D75YZORPI75PXBCCN6C
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-add-row-before-hover.gi	EJVSHTKFKF3DIDEMOLZBJAO
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-remove-row.gifxsq	REOJMPFTYJTCRXFRRW2WKF
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-remove-row-active.gifxs	M7ALXLUKY3ORFS3GMIPTKOF
C:\Documents and Settings\USER\Desktop\fsumfrontend-1.5.5.1-bin\changelog.txtxsq	EUEJXQKG6SUYC66D62JPWNF
C:\Documents and Settings\USER\My Documents\LimeWire\Saved\Metallica - Enter Sandman.mp3xsq	TJTGYI6WE2D5EPC3QWY7LIN
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-remove-column.gifxsq	REOJMPFTYJTCRXFRRW2WKF
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-remove-column-hover.g	HCO2626NBOUEUQJ5ZZFP6AV
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\arrowd.gifxsq	3S6CXYXBUIV2BZJU6DWJOFDE
C:\XXX OST - Like A Prayer of Madonna - Like A Prayer Copy of Madonna - Like A Prayer Copy of Mador	
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\hiddenWindow.htmlxsq	4M2F7MCZXYFBP7WJ6IJPS7V
C:\Documents and Settings\USER\Desktop\fsumfrontend-1.5.5.1-bin\readme.txtxsq	K4D43ZMOFIZOAF3WDUNIWBI
C:\Documents and Settings\USER\Desktop\LimeWire\browser\xulrunner\res\table-add-row-after-hover.gifx	NTLWVEMLKABB6O5PPUHVG

You have now cleaned out most of the "clutter" in both fields – but you still need to remove some data from the "Path" collum



Path	SHA1
SER\Desktop\LimeWire\browser\xulrunner\res\table-add-row-after-active.gif	RUQFIGWUOTXP6QSRLZ36QG
SER\Desktop\LimeWire\browser\xulrunner\res\html\folder.pngxsq	2D3F2SPM5Z7F7JGKUYFRCK3
SER\My Documents\LimeWire\Saved\Madonna - Like A Prayer.mp3xsq	77SYCGFJPP47VQ54TSNBCTJL
SER\Desktop\fsumfrontend-1.5.5.1-bin\INSTALL.txtxsq	GFJLJQL2S5FO5OSQBM5ME5
SER\Desktop\LimeWire\browser\xulrunner\res\table-add-row-after.gifxsq	T5KRM72IIPJFIUSBTLMLNBLMJ
SER\Desktop\LimeWire\browser\xulrunner\res\table-add-column-before-hov	NKTV7L2OTV6OBR2D3HYBJUJ
SER\Desktop\LimeWire\browser\xulrunner\res\table-remove-row-hover.gifxs	HCO2626NBOUEUQJ5ZZFP6AV
SER\Desktop\LimeWire\browser\xulrunner\res\table-add-column-before.gifx	2B2HEKK4PA7VFBBMOJ5L5DS
SER\Desktop\LimeWire\browser\xulrunner\res\table-add-column-after.gifxsc	X75GVQ37FVVKT4BQ462CRPC
SER\Desktop\LimeWire\browser\xulrunner\res\table-add-column-before-acti	4UYRPAAU3DO6GKK6Z5I6BVG
SER\Desktop\LimeWire\browser\xulrunner\README.txtxsq	Q6V57D75YZORPI75PXBCCN6C
SER\Desktop\LimeWire\browser\xulrunner\res\table-add-row-before-hover.gi	EJVSHTKFKF3DIDEMOLZBJAO
SER\Desktop\LimeWire\browser\xulrunner\res\table-remove-row.gifxsq	REOJMPFTYJTCRXFRRW2WKF
SER\Desktop\LimeWire\browser\xulrunner\res\table-remove-row-active.gifxs	M7ALXLUKY3ORFS3GMIPTKOF
SER\Desktop\fsumfrontend-1.5.5.1-bin\changelog.txtxsq	EUEJXQKG6SUYC66D62JPWNF
C:\Documents and Settings\USER\My Documents\LimeWire\Saved\Metallica - Enter Sandman.mp3xsq	TJTGYI6WE2D5EPC3QWY7LIN

Highlight the "Path" collum – Click <Edit> -> <Replace>



Find and Replace

Find What: xsq

Replace With:

Look In: Path

Match: Any Part of Field

Search: All

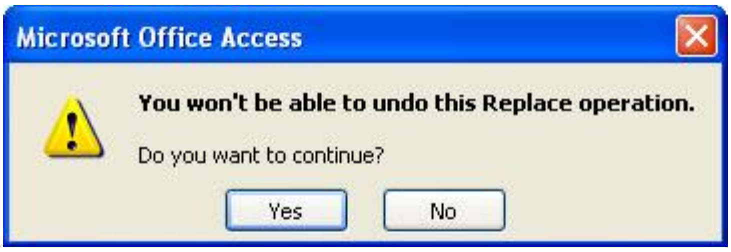
□ Match Case ☑ Search Fields As Formatted

Type “xsq” ind the “Find What” field

Leave “Replace With” empty

Choose “Any part of field” under “Match”

Click “Replace All”



Microsoft Office Access

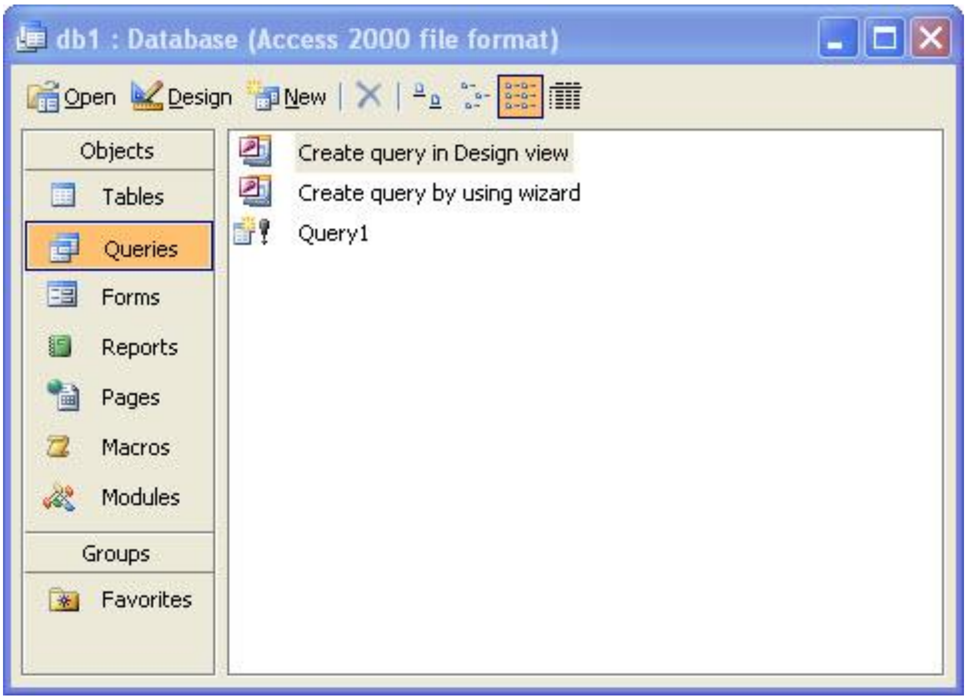
You won't be able to undo this Replace operation.

Do you want to continue?

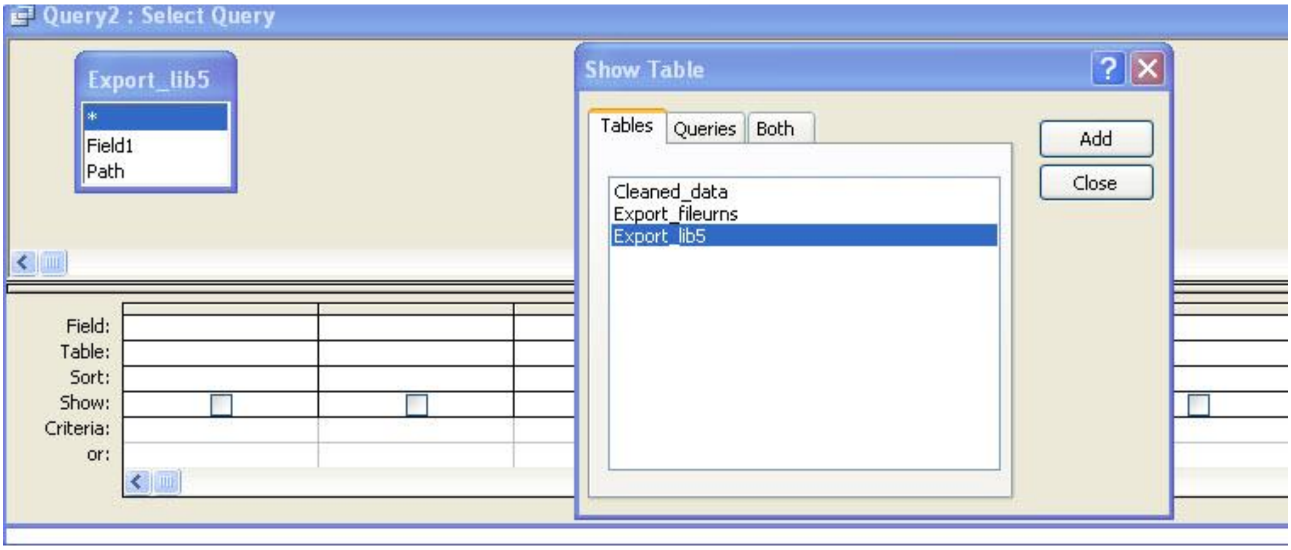
Click <Yes>

The “clutter data” has now been removed from the table.

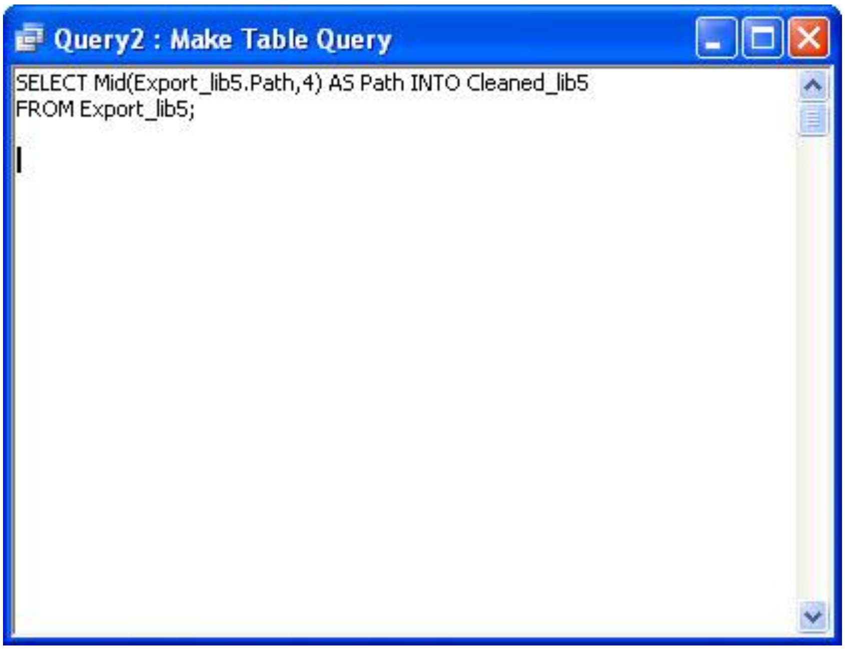
You now need to repeat the process to clean out clutter from the “library5.dat” file.


db1 : Database (Access 2000 file format)
Open
Design
New
Objects
Tables
Queries
Forms
Reports
Pages
Macros
Modules
Groups
Favorites
Create query in Design view
Create query by using wizard
Query1

Select <Queries>-><Create query in Design view>



Choose the “Export_lib5” table – click <Close>



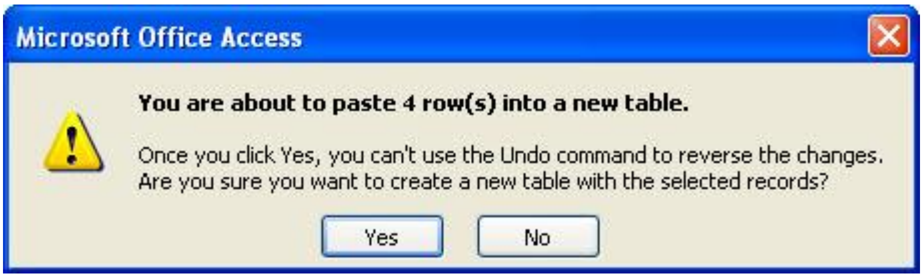
```
SELECT Mid(Export_lib5.Path,4) AS Path INTO Cleaned_lib5
FROM Export_lib5;
```

Click the “View button” to get to the <SQL view>

Paste the following into the query

SELECT Mid(Export_lib5.Path,4) AS Path INTO Cleaned_lib5 FROM Export_lib5;

Click the red exclamation mark in the menu and run the query



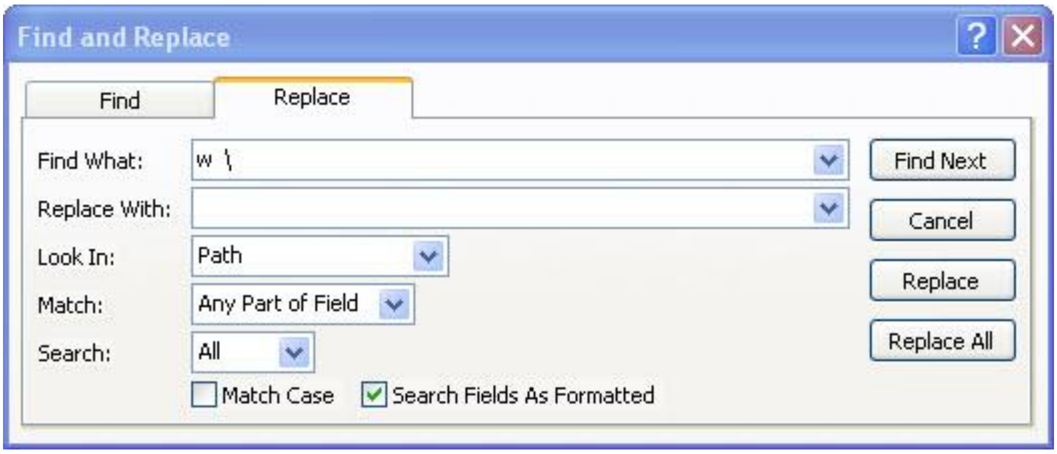
You are about to paste 4 row(s) into a new table.

Once you click Yes, you can't use the Undo command to reverse the changes. Are you sure you want to create a new table with the selected records?

Click <Yes>

Open the new table. Highlight the “path” collum

Click <Edit> -><Replace>



Find What: w \

Replace With:

Look In: Path

Match: Any Part of Field

Search: All

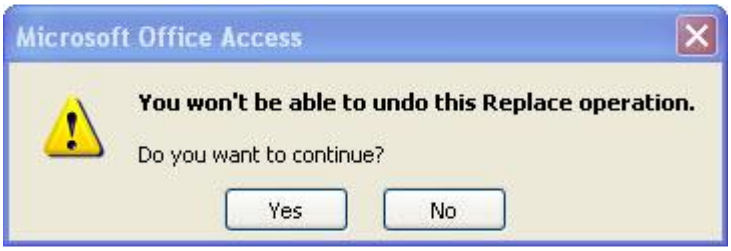
□ Match Case ☑ Search Fields As Formatted

Type in “w \” in the “Find What” field

Choose “Path” in the “Look in” field

“Any part of Field” in “Match”

Click <Replace All>



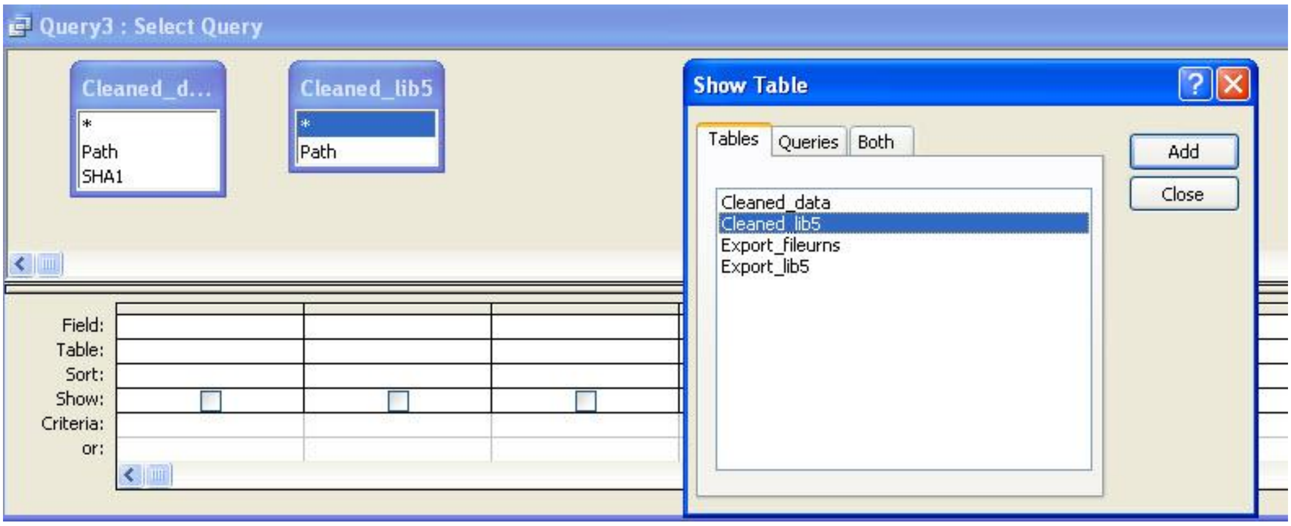
You won't be able to undo this Replace operation.

Do you want to continue?

Click <Yes>

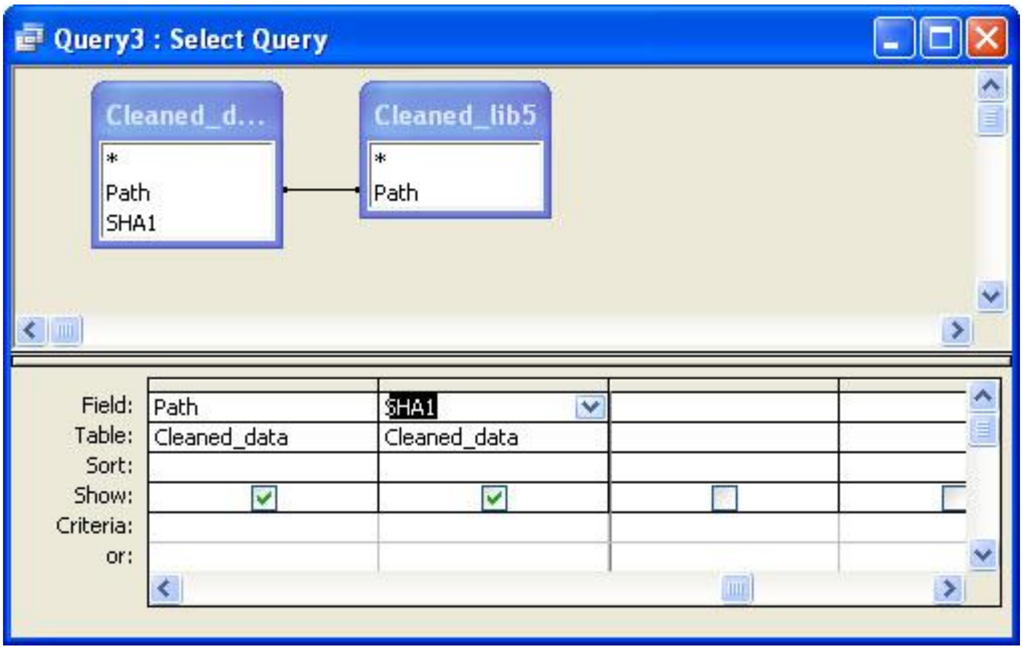
To compare the data you need to create a new query

Select <Queries>-><Create query in Design view> and create a new query



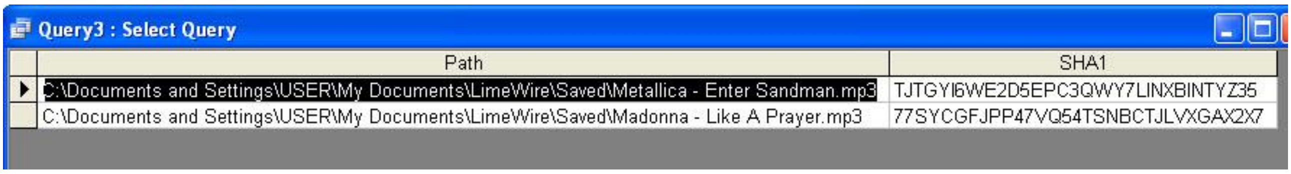
Select the two tables “Cleaned_data” and “Cleaned_lib5”

You have to create a relationship between the two tables. The data you want to “match” is the “Path” column in both tables. You create the relationship by selecting the “Path” field from one column and drag it on to the “Path” field in the other column. The relationship is created, and is shown by a line between the two fields



Field:	Path	SHA1		
Table:	Cleaned_data	Cleaned_data		
Sort:				
Show:	☑	☑	□	□
Criteria:				
or:				

From the “Cleaned_data” you select both fields and drag them on to the “Field” field. You have now created the query. Click the red exclamation mark and run the query. You will now get a result like below.



Query3 : Select Query

Path	SHA1
C:\Documents and Settings\USER\My Documents\LimeWire\Saved\Metallica - Enter Sandman.mp3	TJTGYI6WE2D5EPC3QWY7LINXBINTYZ35
C:\Documents and Settings\USER\My Documents\LimeWire\Saved\Madonna - Like A Prayer.mp3	77SYCGFJPP47VQ54TSNBCTJLVXGAX2X7

In this query you have now established the connection between the data in “fileurns.cache” and “library5.dat” and shown what files are shared (If you had chosen to only select files that had the share bit set to sharing)

Searching for data in unallocated clusters

The mentioned GREP searches can be used in unallocated clusters to find information on deleted files, previous downloads etc. The search hits can be extracted and “parsed” in the same way as mentioned above. This gives the possibility to prove earlier possession of the files (if you have a database of illegal material to compare with).

To prove the sharing of these files is not 100% possible/sure. This relys on the fact, that the user previously could have changed his “number of uploads at once” to “0”. As mentioned under “limewire.props” this will result in the creation of the line “HARD_MAX_UPLOADS=0”. It’s possible to make a GREP search for this line. If you don’t get any hits on this search, it’s quite possible, that the sharing not has been disabled by turning down the number of uploads – but you can not be absolutely sure (it depends on the situation, amount of data, size of unallocated clusters etc). The presence of SHA1 values in “fileurns.cache” entries from unallocated clusters will though constitute the evidence of, that this particular file previously has been in the “library” and there for in possession of the user

As the development of clients is ever growing, this is only a “snapshot” in time of what is possible to find. Some information might not be present in this version, but will be in the next.

The future examination of clients will go on, and all my discoveries will be published at www.filseshareforensics.org. Join, learn and contribute with your own discoveries. Remember – If we work together our knowledge increases – and the amount of time we have to use on an investigation decreases – It’s a real win-win-situation ☺

Søren Christensen

Detective Inspector – Special Consultant
National High Tech Crime Centre – Denmark
soeren.christensen@nitec.politi.dk
www.fileshareforensics.org