GigaTribe Forensic Guide

D/Sgt. Les Vuyk #9937
Niagara Regional Police Service
Technological Crime Unit

PURPOSE:

The purpose of this paper is to analyze and document the history, installation and function of the GigaTribe client for Windows. Changes to the Windows Registry and files created by the installation and operation of this program were analyzed. Significant files and registry keys will be highlighted to assist in the forensic analysis and investigation of GigaTribe.

Version 2.50 of GigaTribe was downloaded from www.gigatribe.com on Wednesday, March 25, 2009 and used in this testing. Note that all testing was done using the free version of GigaTribe. The "Ultimate Version" costs $4.99 per month or $29.95 for a 1 year subscription, and was not tested.

TOOLS USED:

- The installation process was monitored using the InCtrl5, a process monitoring tool released by Ziff-Davis Media.
- Changes made to the file system and Windows Registry were tracked by the ProcMon tool released by Microsoft.
- Screen captures were created using SnagIt 7.2 released by Techsmith Corporation.
- Tests were conducted under Windows XP Professional 32 Bit (SP 3) in a Virtual Machine using Microsoft Virtual PC. I created a second account on a different computer in order to test the search and file transfer functionality.

HISTORY :

GigaTribe was founded in 2005, according to information on the GigaTribe website. It is published by Shalsoft, with a copyright date of 2005. Numerous web references link GigaTribe to an earlier software called "TribalWeb". Apparently the name of the product changed in 2005.

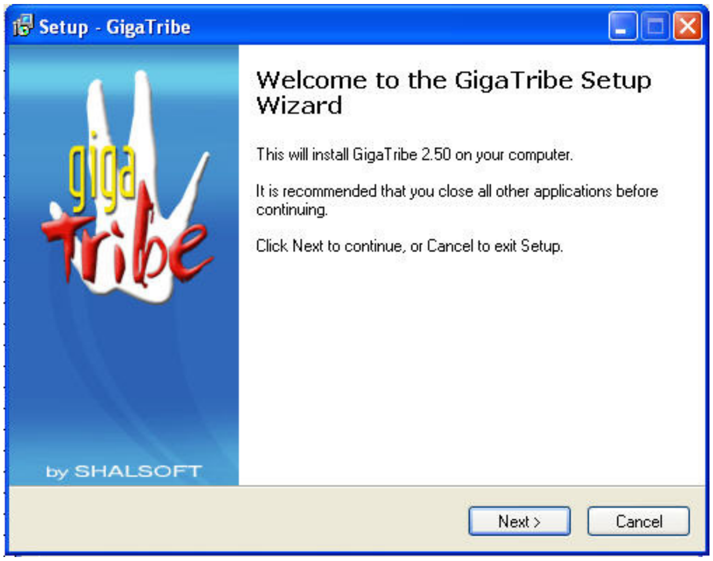
WHOIS records link GigaTribe to Shalsoft, with an administrative contact of Alexis Lesigneur, 5 rue Salomon de Rothschild, Suresnes, France (+33.146972533), as of 2008-05-12.

WHOIS records link TribalWeb to Christophe Sorine, 26 rue Guillaume Tell, Paris (+33.140540223). The domain "tribalweb.com" was registered on July 12, 1996.

I found little information on GigaTribe and the parent company, Shalsoft. GigaTribe appears to be Shalsoft's only product. The domain "www.shalsoft.com" links directly to www.gigatribe.com.

GIGATRIBE INSTALLATION:

GigaTribe installation is straight-forward. Setup is done in a Wizard style and starts with a welcome screen:



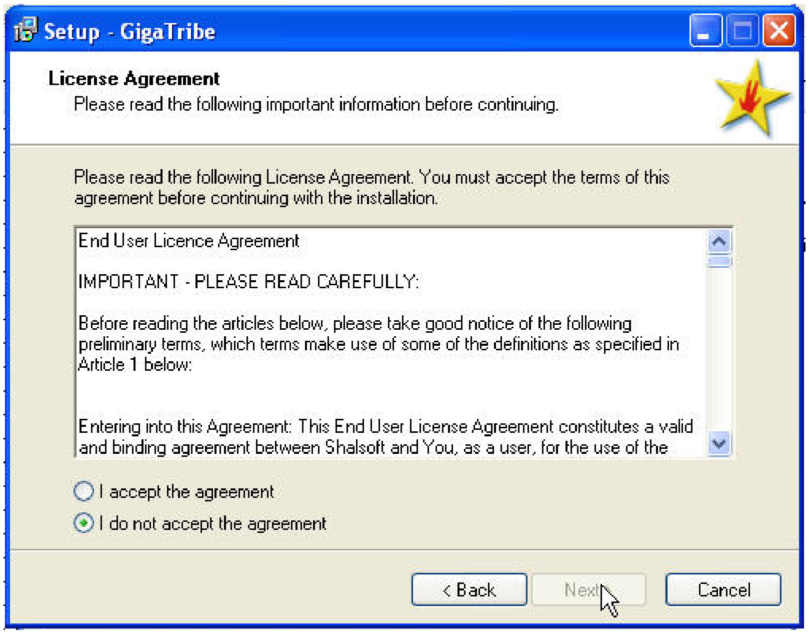
Welcome to the GigaTribe Setup Wizard

This will install GigaTribe 2.50 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

A License Agreement screen follows:



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

End User Licence Agreement

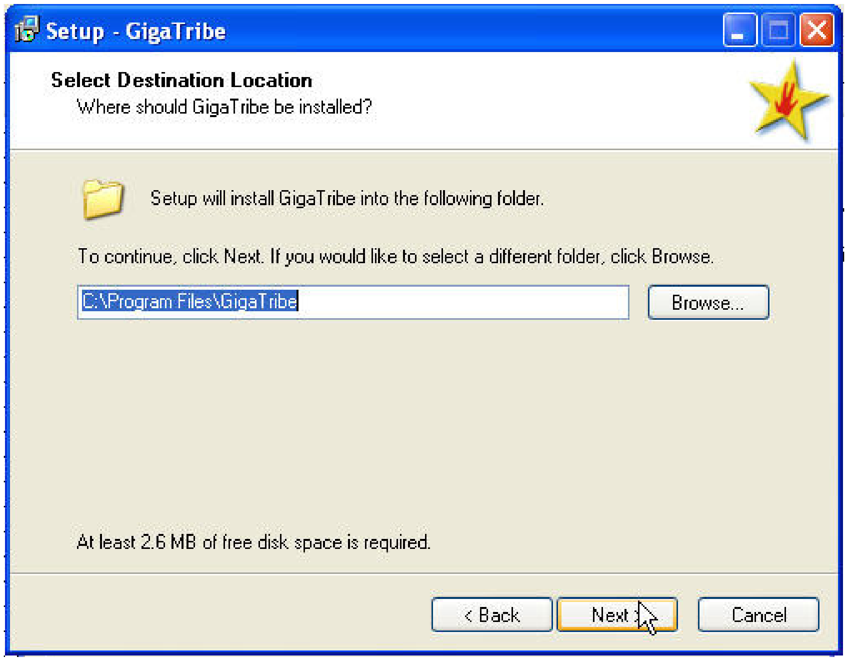
IMPORTANT - PLEASE READ CAREFULLY:

Before reading the articles below, please take good notice of the following preliminary terms, which terms make use of some of the definitions as specified in Article 1 below:

Entering into this Agreement: This End User License Agreement constitutes a valid and binding agreement between Shalsoft and You, as a user, for the use of the

○ I accept the agreement
● I do not accept the agreement

The Default Installation Location screen is next. The installation location can be modified by the user.



Select Destination Location

Where should GigaTribe be installed?

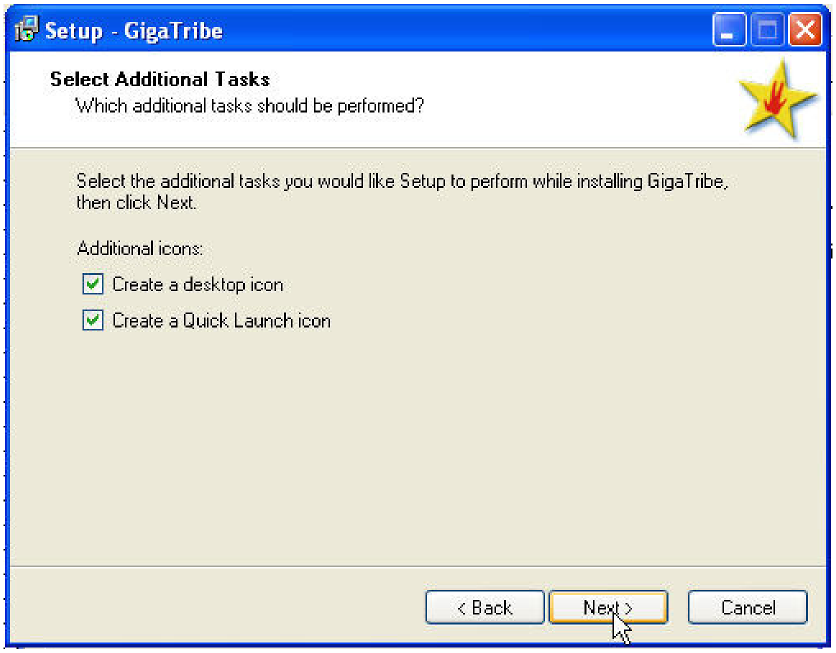
Setup will install GigaTribe into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\GigaTribe

At least 2.6 MB of free disk space is required.

By default, GigaTribe creates a Start Menu Folder, a desktop icon and a Quick Launch icon. The second two options can be de-selected at the next screen.



Select Additional Tasks

Which additional tasks should be performed?

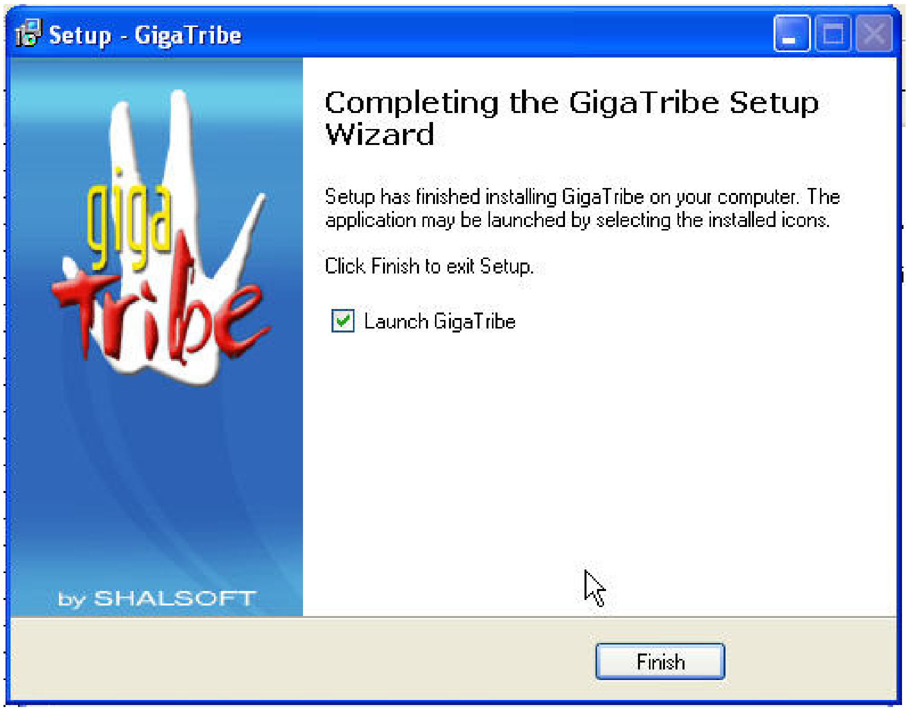
Select the additional tasks you would like Setup to perform while installing GigaTribe, then click Next.

Additional icons:

☑ Create a desktop icon

☑ Create a Quick Launch icon

The program then installs, and a final screen gives you the option to Launch GigaTribe immediately:



Setup - GigaTribe

Completing the GigaTribe Setup Wizard

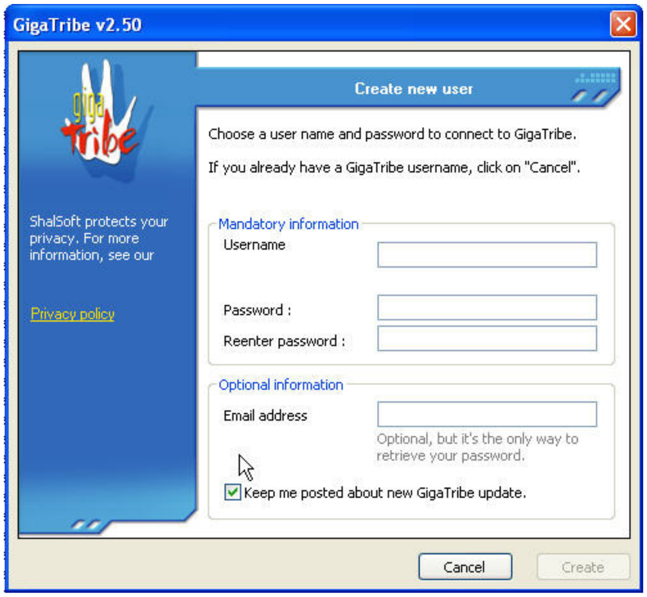
Setup has finished installing GigaTribe on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

☑ Launch GigaTribe

GIGATRIBE FIRST RUN:

The following screen captures document the first time the program was run. Before the program can be used, GigaTribe requires the user to create a new account, or enter existing account information after clicking "Cancel".



GigaTribe v2.50

Create new user

Choose a user name and password to connect to GigaTribe.

If you already have a GigaTribe username, click on "Cancel".

ShalSoft protects your privacy. For more information, see our Privacy policy

Mandatory information

Username:

Password :

Reenter password :

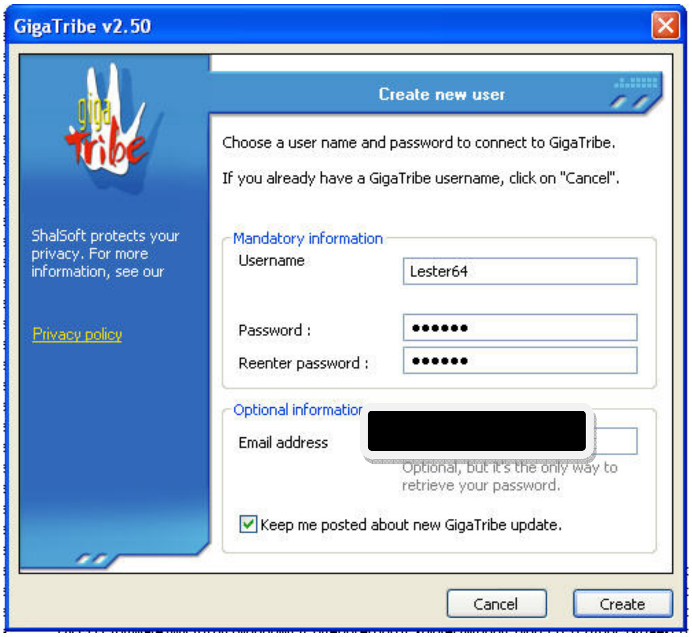
Optional information

Email address:

Optional, but it's the only way to retrieve your password.

☑ Keep me posted about new GigaTribe update.

I created a new account "Lester64":



GigaTribe v2.50

Create new user

Choose a user name and password to connect to GigaTribe.

If you already have a GigaTribe username, click on "Cancel".

ShalSoft protects your privacy. For more information, see our Privacy policy

Mandatory information

Username: Lester64

Password : ••••••

Reenter password : ••••••

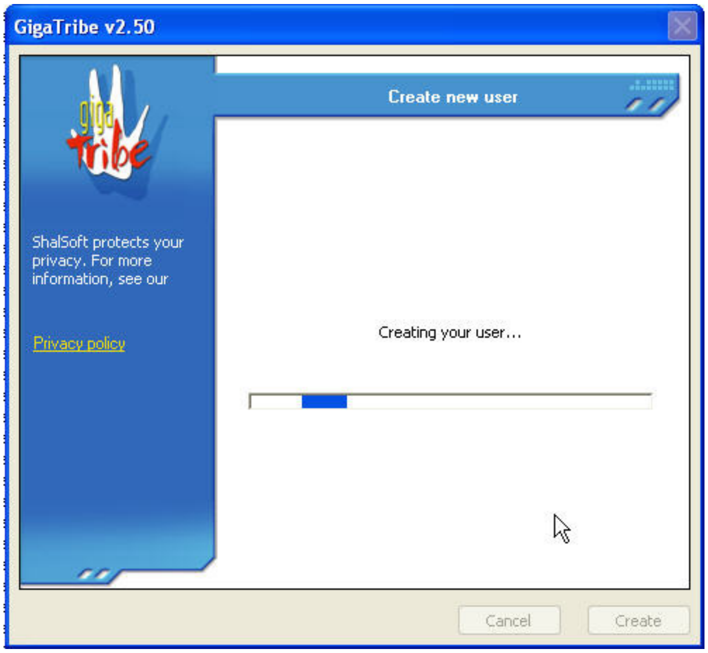
Optional information

Email address: [redacted]

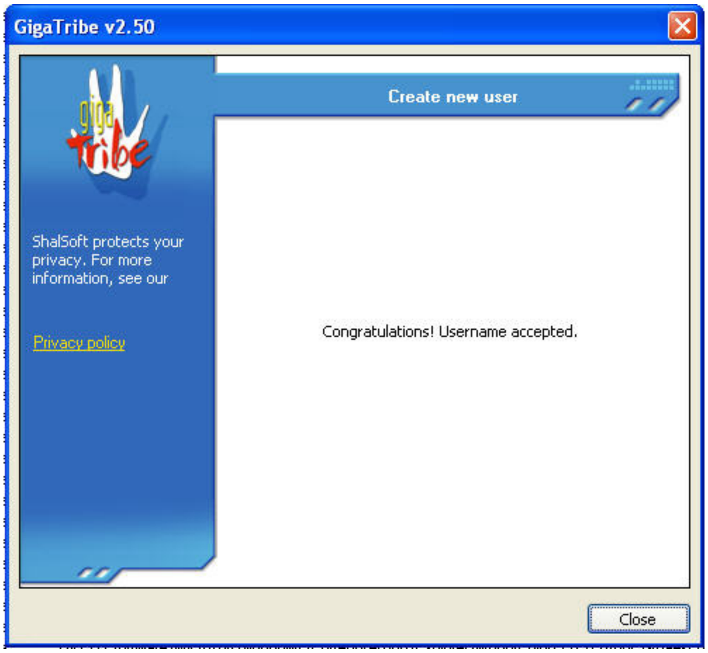
Optional, but it's the only way to retrieve your password.

☑ Keep me posted about new GigaTribe update.

My account was then created

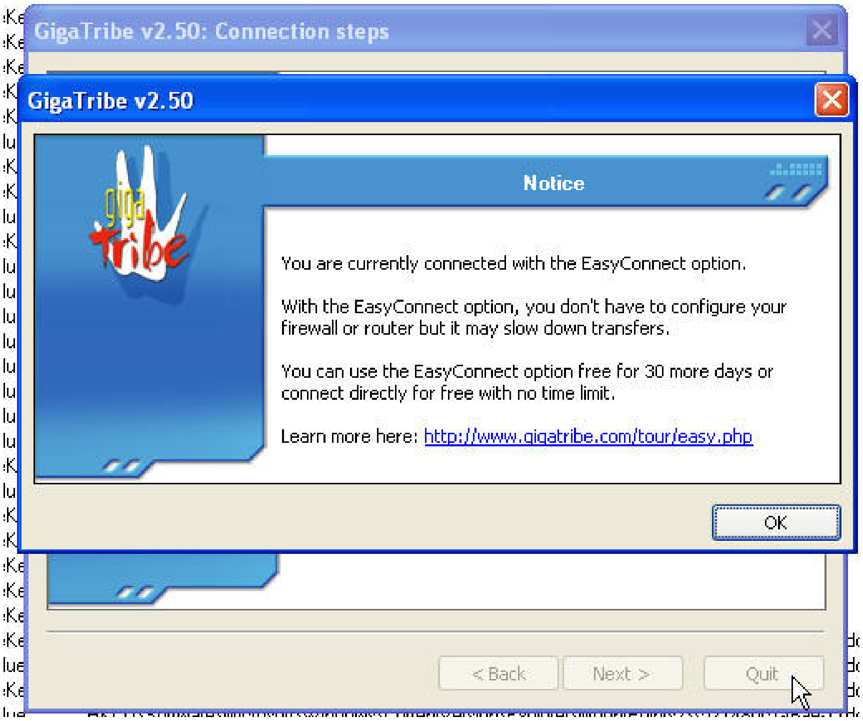


Creating your user...


GigaTribe v2.50
Create new user
giga tribe
ShalSoft protects your privacy. For more information, see our
Privacy policy
Close

Congratulations! Username accepted.

At that point the program started, and a short "notice" message was displayed.



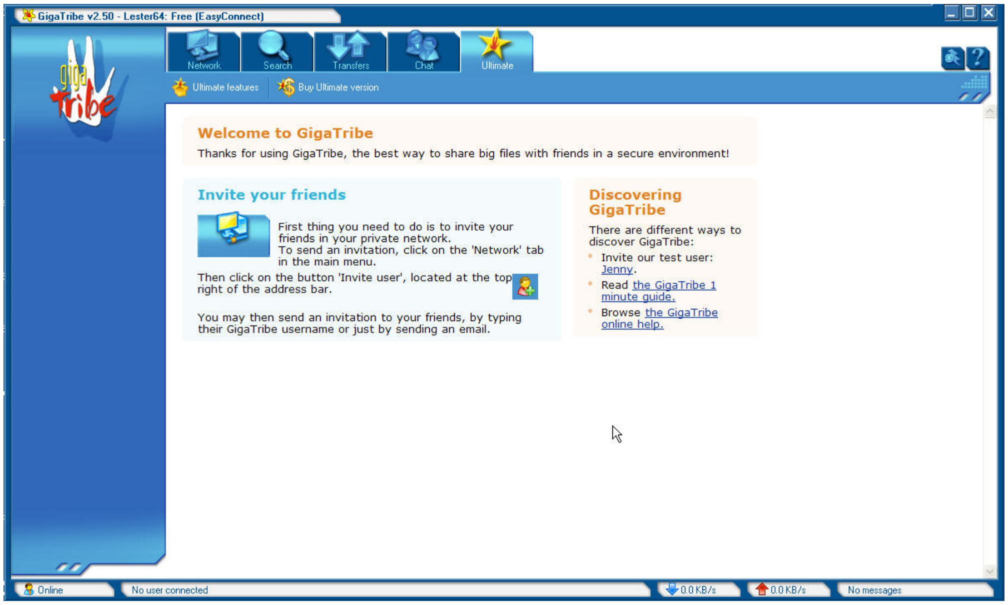
You are currently connected with the EasyConnect option.

With the EasyConnect option, you don't have to configure your firewall or router but it may slow down transfers.

You can use the EasyConnect option free for 30 more days or connect directly for free with no time limit.

Learn more here: http://www.gigatribe.com/tour/easy.php

From there, the program opened to the "Ultimate" tab and a Welcome greeting was displayed, with links to a user guide and online help.



Welcome to GigaTribe

Thanks for using GigaTribe, the best way to share big files with friends in a secure environment!

Invite your friends

First thing you need to do is to invite your friends in your private network.
To send an invitation, click on the 'Network' tab in the main menu.

Then click on the button 'Invite user', located at the top right of the address bar.

You may then send an invitation to your friends, by typing their GigaTribe username or just by sending an email.

Discovering GigaTribe

There are different ways to discover GigaTribe:

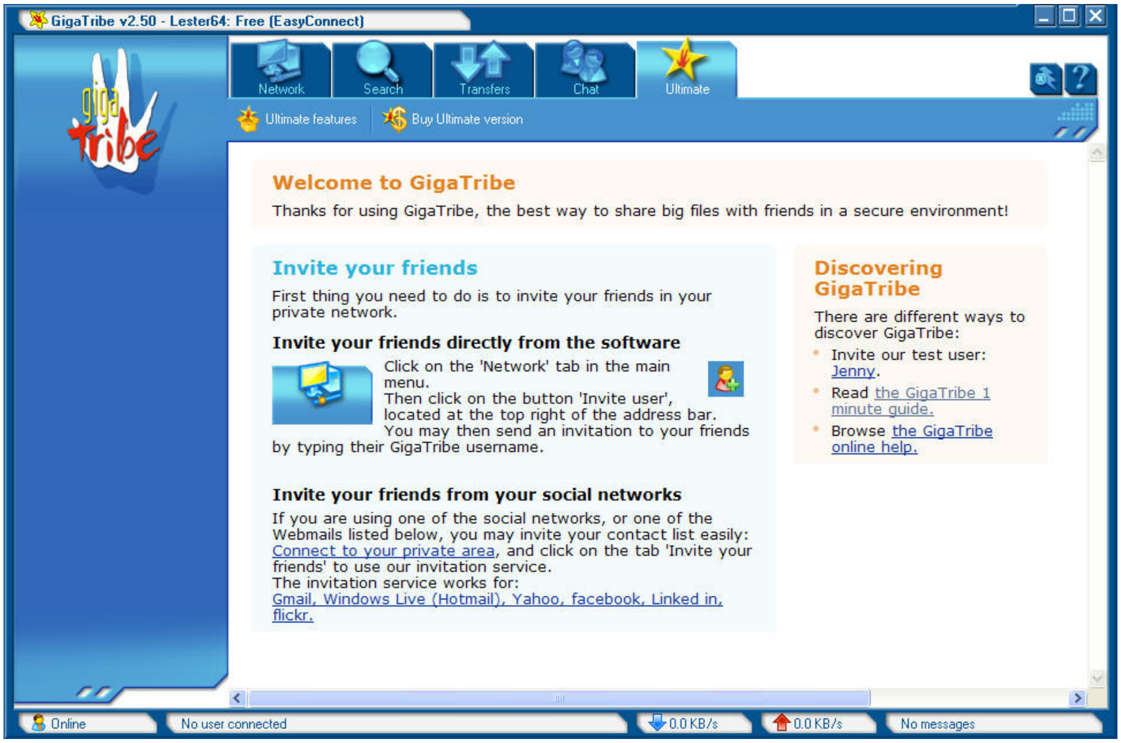
- Invite our test user: Jenny.
- Read the GigaTribe 1 minute guide.
- Browse the GigaTribe online help.

ADDITIONAL SET UP (Free Version):

GigaTribe is a private file sharing program that operates using a variation on the peer to peer (P2P) network model, which is sometimes referred to as a "friend-to-friend" network (F2F) or "Private P2P". It is distinct from P2P clients that connect to the Gnutella network in that users can only connect with people they know and trust.

In order to connect to the GigaTribe network, users must create an account and "log in" to the GigaTribe network with a valid username and password. This authenticates against a GigaTribe network server prior to allowing access to the network. In essence, the program is not useable until a user has successfully connected to the network.

Once connected, the user is greeted and links are provided to help familiarize the user with the program.



Welcome to GigaTribe

Thanks for using GigaTribe, the best way to share big files with friends in a secure environment!

Invite your friends

First thing you need to do is to invite your friends in your private network.

Invite your friends directly from the software

Click on the 'Network' tab in the main menu.
Then click on the button 'Invite user', located at the top right of the address bar.
You may then send an invitation to your friends by typing their GigaTribe username.

Invite your friends from your social networks

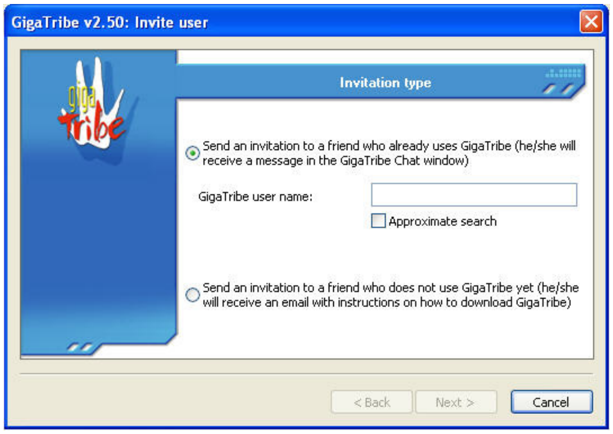
If you are using one of the social networks, or one of the Webmails listed below, you may invite your contact list easily: Connect to your private area, and click on the tab 'Invite your friends' to use our invitation service.
The invitation service works for:
Gmail, Windows Live (Hotmail), Yahoo, facebook, Linked in, flickr.

Discovering GigaTribe

There are different ways to discover GigaTribe:

- Invite our test user: Jenny.
- Read the GigaTribe 1 minute guide.
- Browse the GigaTribe online help.

Once connected the user must invite or be invited in order to connect to other users, and must then add them to their GigaTribe network. Users can invite other GigaTribe users or can send invitations to friends who do not use GigaTribe.


GigaTribe v2.50: Invite user

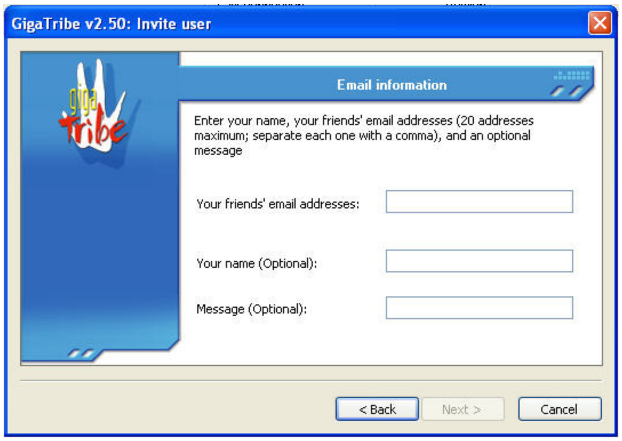
Invitation type

● Send an invitation to a friend who already uses GigaTribe (he/she will receive a message in the GigaTribe Chat window)

GigaTribe user name:

☐ Approximate search

○ Send an invitation to a friend who does not use GigaTribe yet (he/she will receive an email with instructions on how to download GigaTribe)


GigaTribe v2.50: Invite user

Email information

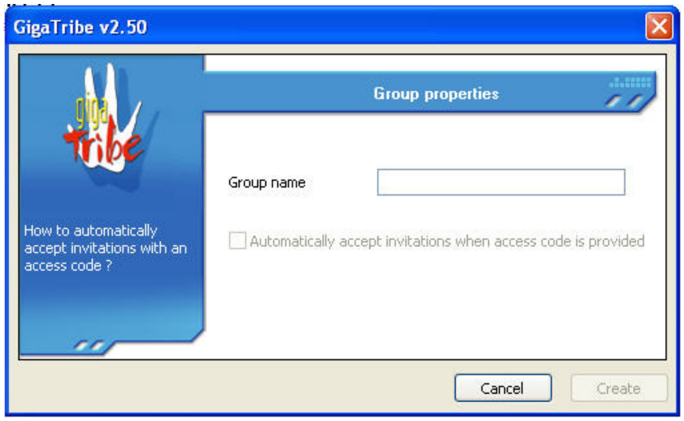
Enter your name, your friends' email addresses (20 addresses maximum; separate each one with a comma), and an optional message

Your friends' email addresses:

Your name (Optional):

Message (Optional):

New Groups can be created to segregate GigaTribe users into different categories. The default group is "Others".


GigaTribe v2.50

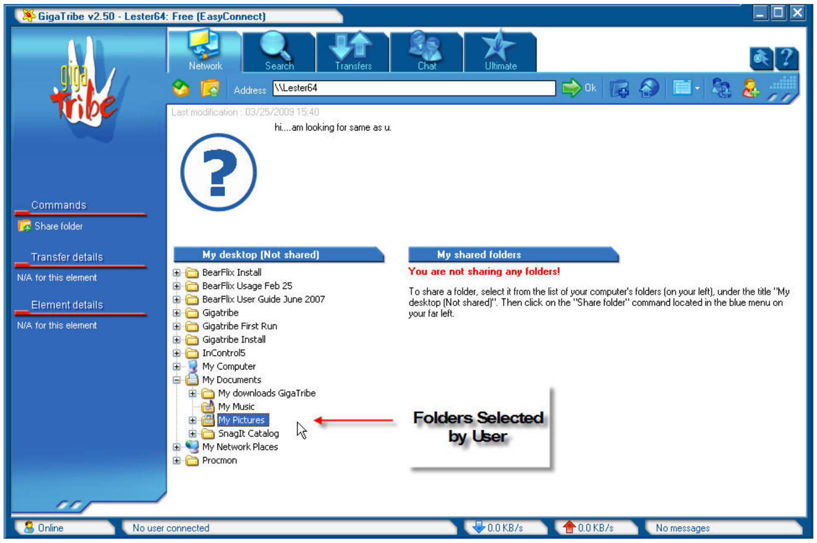
Group properties

How to automatically accept invitations with an access code ?

Group name

☐ Automatically accept invitations when access code is provided

Once connected to other GigaTribe users, the program allows for one-to-one chat and the transfer of files between users. In order to share files, folders must be selected for sharing from within the program.



Address: \\Lester64

Last modification : 03/25/2009 15:40

hi....am looking for same as u.

My desktop (Not shared)

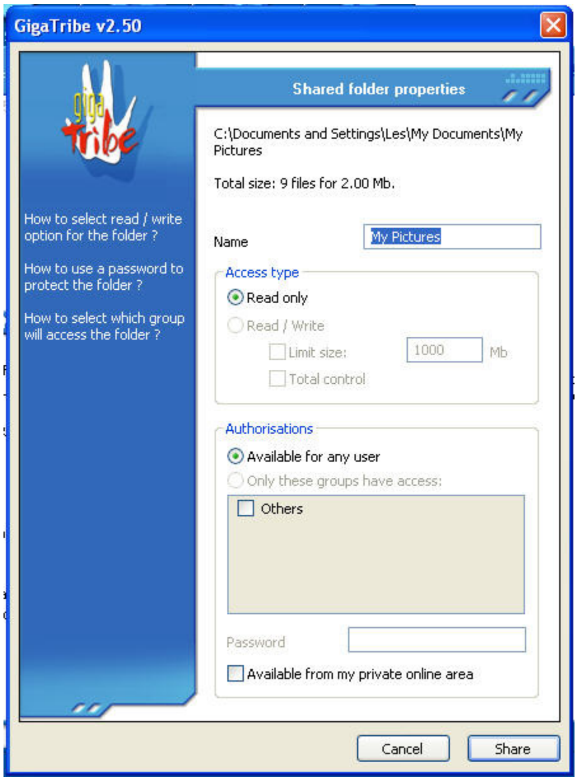
- BearFlix Install
- BearFlix Usage Feb 25
- BearFlix User Guide June 2007
- Gigatribe
- Gigatribe First Run
- Gigatribe Install
- InControl5
- My Computer
- My Documents
  - My downloads GigaTribe
  - My Music
  - My Pictures
  - SnagIt Catalog
- My Network Places
- Procmon

My shared folders

You are not sharing any folders!

To share a folder, select it from the list of your computer's folders (on your left), under the title "My desktop (Not shared)". Then click on the "Share folder" command located in the blue menu on your far left.

The user simply right-clicks on the folder he/she wishes to share and sets the "Shared folder properties."


GigaTribe v2.50
Shared folder properties
How to select read / write option for the folder ?
How to use a password to protect the folder ?
How to select which group will access the folder ?
Access type
Authorisations
Cancel
Share

C:\Documents and Settings\Les\My Documents\My Pictures

Total size: 9 files for 2.00 Mb.

Name: My Pictures

Access type

● Read only

○ Read / Write

☐ Limit size: 1000 Mb

☐ Total control

Authorisations

● Available for any user

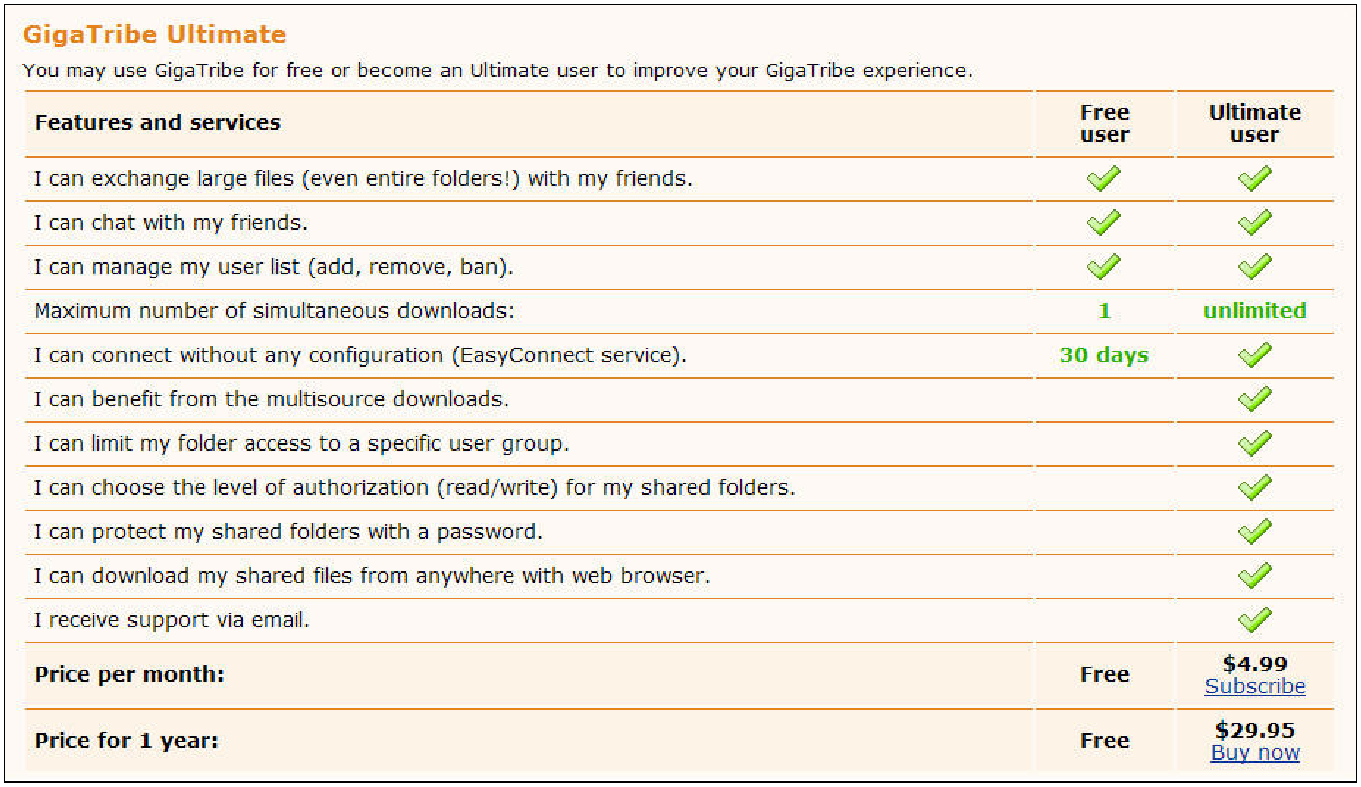
○ Only these groups have access:

☐ Others

Password:

☐ Available from my private online area

Note that the free version which I evaluated does not allow for granular control of the shared folders. Shared folders are simply set as "Read Only", and are available to any user. A comparison of the features of the two versions are as follows:



GigaTribe Ultimate

You may use GigaTribe for free or become an Ultimate user to improve your GigaTribe experience.

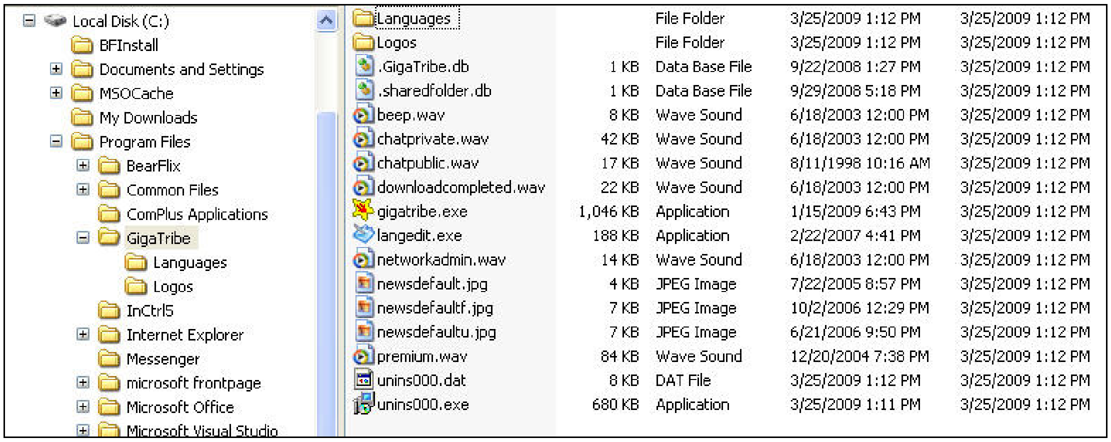
Features and services	Free user	Ultimate user
I can exchange large files (even entire folders!) with my friends.	✓	✓
I can chat with my friends.	✓	✓
I can manage my user list (add, remove, ban).	✓	✓
Maximum number of simultaneous downloads:	1	unlimited
I can connect without any configuration (EasyConnect service).	30 days	✓
I can benefit from the multisource downloads.		✓
I can limit my folder access to a specific user group.		✓
I can choose the level of authorization (read/write) for my shared folders.		✓
I can protect my shared folders with a password.		✓
I can download my shared files from anywhere with web browser.		✓
I receive support via email.		✓
Price per month:	**Free**	**$4.99** Subscribe
Price for 1 year:	**Free**	**$29.95** Buy now

GIGATRIBE INSTALLATION DETAILS:

Changes to the file system and Windows Registry were documented during the above installation and initial run of the program. Results are documented below.

- By default, Gigatribe **installs** in the location:

  C:\Program Files\Gigatribe (assuming "C" is where Windows is installed)

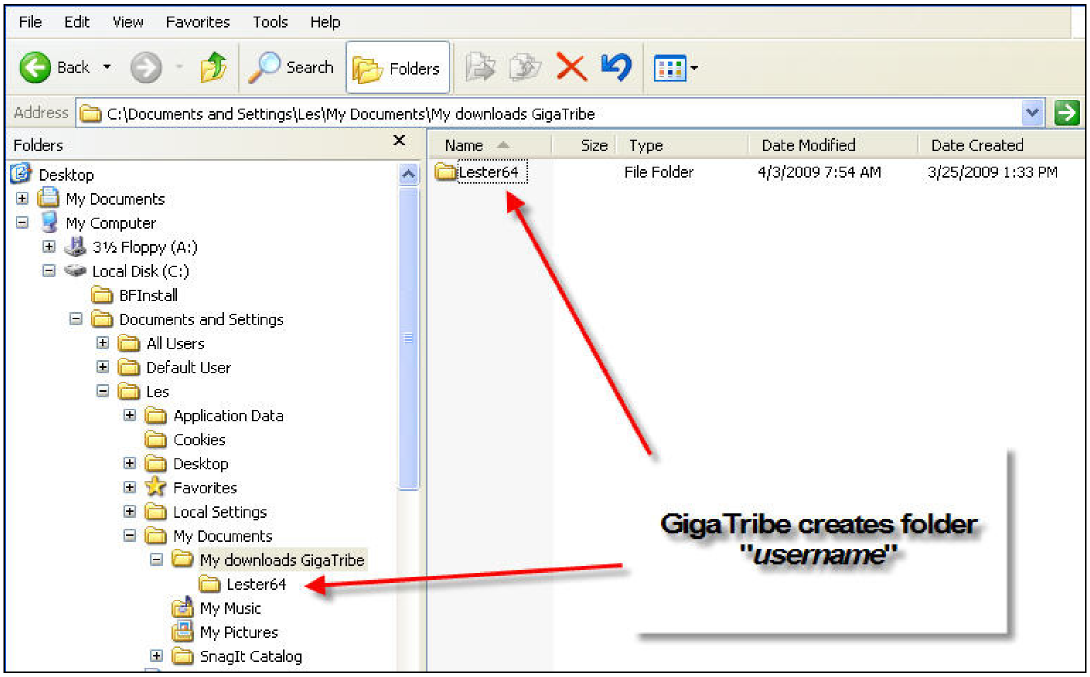


- Local Disk (C:)
  - BFInstall
  - Documents and Settings
  - MSOCache
  - My Downloads
  - Program Files
    - BearFlix
    - Common Files
    - ComPlus Applications
    - GigaTribe
      - Languages
      - Logos
    - InCtrl5
    - Internet Explorer
    - Messenger
    - microsoft frontpage
    - Microsoft Office
    - Microsoft Visual Studio

Languages		File Folder	3/25/2009 1:12 PM	3/25/2009 1:12 PM
Logos		File Folder	3/25/2009 1:12 PM	3/25/2009 1:12 PM
.GigaTribe.db	1 KB	Data Base File	9/22/2008 1:27 PM	3/25/2009 1:12 PM
.sharedfolder.db	1 KB	Data Base File	9/29/2008 5:18 PM	3/25/2009 1:12 PM
beep.wav	8 KB	Wave Sound	6/18/2003 12:00 PM	3/25/2009 1:12 PM
chatprivate.wav	42 KB	Wave Sound	6/18/2003 12:00 PM	3/25/2009 1:12 PM
chatpublic.wav	17 KB	Wave Sound	8/11/1998 10:16 AM	3/25/2009 1:12 PM
downloadcompleted.wav	22 KB	Wave Sound	6/18/2003 12:00 PM	3/25/2009 1:12 PM
gigatribe.exe	1,046 KB	Application	1/15/2009 6:43 PM	3/25/2009 1:12 PM
langedit.exe	188 KB	Application	2/22/2007 4:41 PM	3/25/2009 1:12 PM
networkadmin.wav	14 KB	Wave Sound	6/18/2003 12:00 PM	3/25/2009 1:12 PM
newsdefault.jpg	4 KB	JPEG Image	7/22/2005 8:57 PM	3/25/2009 1:12 PM
newsdefaultf.jpg	7 KB	JPEG Image	10/2/2006 12:29 PM	3/25/2009 1:12 PM
newsdefaultu.jpg	7 KB	JPEG Image	6/21/2006 9:50 PM	3/25/2009 1:12 PM
premium.wav	84 KB	Wave Sound	12/20/2004 7:38 PM	3/25/2009 1:12 PM
unins000.dat	8 KB	DAT File	3/25/2009 1:12 PM	3/25/2009 1:12 PM
unins000.exe	680 KB	Application	3/25/2009 1:11 PM	3/25/2009 1:12 PM

- The default **download** directory is created at the following location:

  C:\Documents and Settings\{user}\My Documents\My downloads GigaTribe\{gigatribe username}



Address: C:\Documents and Settings\Les\My Documents\My downloads GigaTribe

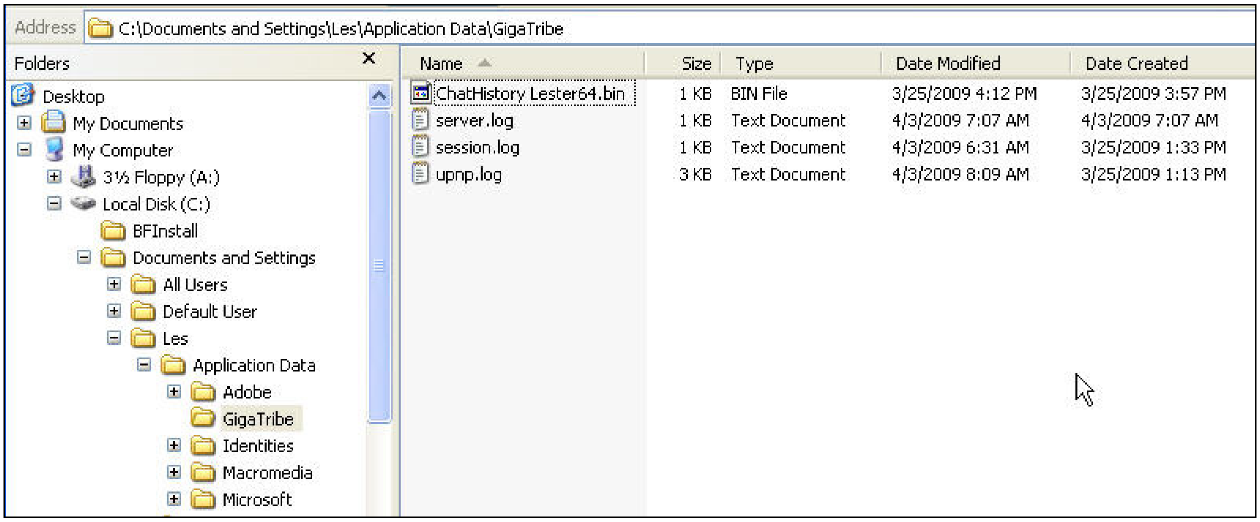
- Desktop
  - My Documents
  - My Computer
    - 3½ Floppy (A:)
    - Local Disk (C:)
      - BFInstall
      - Documents and Settings
        - All Users
        - Default User
        - Les
          - Application Data
          - Cookies
          - Desktop
          - Favorites
          - Local Settings
          - My Documents
            - My downloads GigaTribe
              - Lester64
            - My Music
            - My Pictures
            - SnagIt Catalog

Name	Size	Type	Date Modified	Date Created
Lester64		File Folder	4/3/2009 7:54 AM	3/25/2009 1:33 PM

GigaTribe creates folder *"username"*

- An **Application Data** Folder is created at the following location:

  C:\Documents and Settings\{user}\Application Data\Gigatribe



Address C:\Documents and Settings\Les\Application Data\GigaTribe

Name	Size	Type	Date Modified	Date Created
ChatHistory Lester64.bin	1 KB	BIN File	3/25/2009 4:12 PM	3/25/2009 3:57 PM
server.log	1 KB	Text Document	4/3/2009 7:07 AM	4/3/2009 7:07 AM
session.log	1 KB	Text Document	4/3/2009 6:31 AM	3/25/2009 1:33 PM
upnp.log	3 KB	Text Document	4/3/2009 8:09 AM	3/25/2009 1:13 PM

- This folder contains four log files. These log files are:
  - **upnp.log**: Unknown function. Does not appear to contain relevant data
  - **session.log**: Contains log records of previous connection attempts, may be relevant
  - **server.log**: Created the first time you log into your "private area" via the web interface from GigaTribe. Contains the IP Address you logged in from and a "Get" request.
  - **ChatHistory {*gigatribe username*}.bin**: This is a chat log. Note that it can be deleted from within the Gigatribe program.

- **Windows Registry**: A number of changes were made in the Windows Registry by the installation of this program.

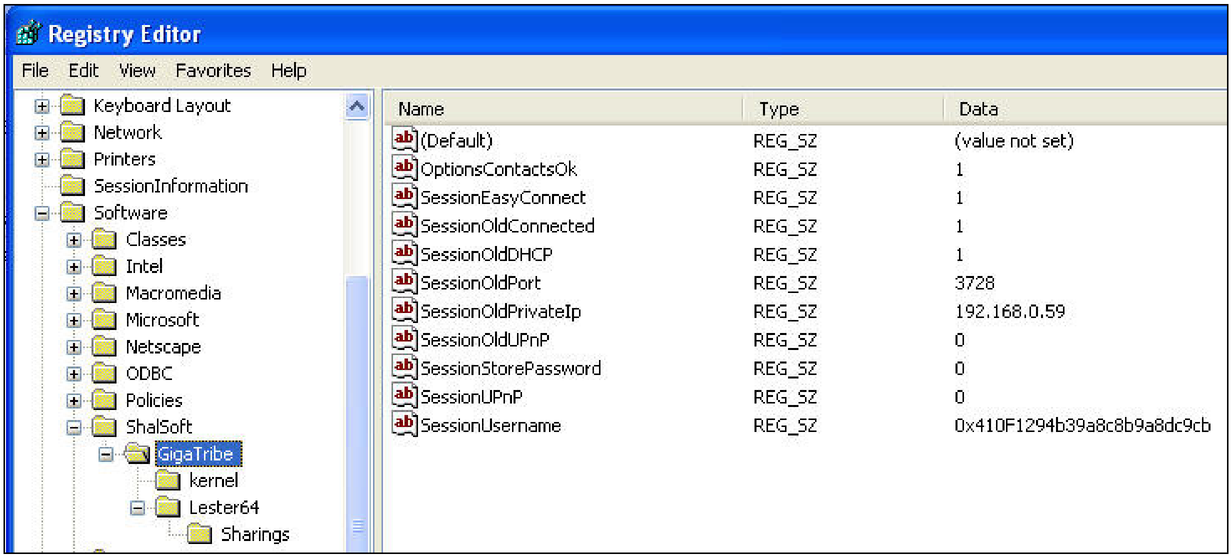
- Configuration settings are stored in the Windows Registry in the following key:

  HKCU\Software\Shalit\Gigatribe (NTUSER.DAT)

- Registry Keys are as follows:

SessionUPnP:	Off or On (value 0 or 1) (default "0") (May allow more values)
SessionEasyConnect:	Off or On (value 0 or 1) (default "1") ("1" corresponds with this function being enabled)
SessionUsername	Appears to be an encrypted hex value corresponding to username pre-pended with "0x410F1294"
SessionStorePassword:	Off or On (value 0 or 1) (default "1") (option to remember password)
SessionOldConnected	Off or On (value 0 or 1) (default "1") (unknown what this corresponds with)

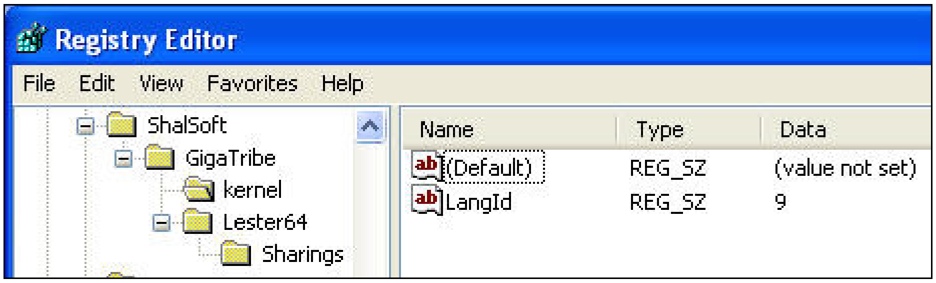
SessionOldPrivateIP:	Shows IP address of host computer
SessionOldPort:	Shows Port (appears to be 3728 by default - un-confirmed)
SessionOldUPnP:	Off or On (value 0 or 1) (default "0") (may be more values allowed)
SessionOldDHCP:	Off or On (value 0 or 1) (default "0") (may be more values allowed)
OptionsContactsOk:	Off or On (value 0 or 1) (default "1") (may be more values allowed)
SessionPort:	Shows Port Number



Name	Type	Data
(Default)	REG_SZ	(value not set)
OptionsContactsOk	REG_SZ	1
SessionEasyConnect	REG_SZ	1
SessionOldConnected	REG_SZ	1
SessionOldDHCP	REG_SZ	1
SessionOldPort	REG_SZ	3728
SessionOldPrivateIp	REG_SZ	192.168.0.59
SessionOldUPnP	REG_SZ	0
SessionStorePassword	REG_SZ	0
SessionUPnP	REG_SZ	0
SessionUsername	REG_SZ	0x410F1294b39a8c8b9a8dc9cb

Sub-Key "kernel":

LangId:	Numerical value ("9" for English) (default "9")

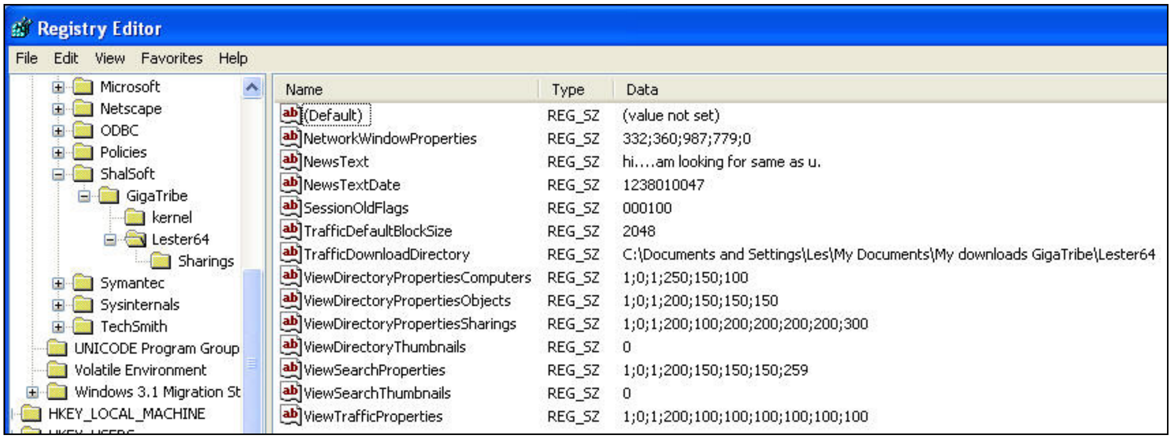


Name	Type	Data
(Default)	REG_SZ	(value not set)
LangId	REG_SZ	9

Sub-Key "{gigatribe Username}":

InactiveForced	Off or On (value 0 or 1) (may be more values allowed)
NetworkWindowProperties	Unknown value (default " 301;157;1203;725;0")
NewsText	User-generated text message (in plain text)
NewsTextDate	A 10 digit Unix Numeric Value
SessionOldFlags	Unknown numerical value (default " 000000")
TrafficDefaultBlockSize	Unknown numerical value (default "2048")
TrafficDownloadDirectory	path to download directory (in plain text)
TrafficDownloadSound	Off or On (value 0 or 1) (may be more values allowed)
TrafficMaxDownloads	Unknown numerical value - unknown default value
TrafficMaxDownloadsPerComputer	Unknown numerical value

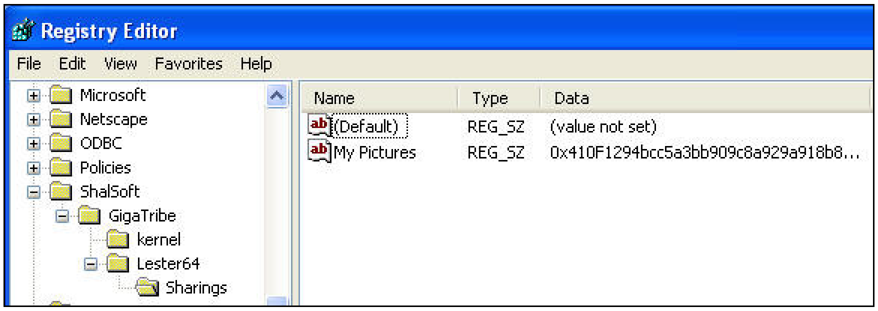
TrafficMaxDownloadsUI	Unknown numerical value
TrafficMaxSpeedUploads	Off or On (value 0 or 1) (may be more values allowed)
TrafficMaxSpeedUploadsUI	Unknown numerical value
TrafficMaxSpeedWhenAfk	Off or On (value 0 or 1) (may be more values allowed)
TrafficMaxUploads	Numerical Value
TrafficMaxUploadsPerComputer	Numerical Value
TrafficNetAccess	Off or On (value 0 or 1) (may be more values allowed)
TrafficSendDownloads	Off or On (value 0 or 1) (may be more values allowed)
ViewChatSplitY	Unknown Numerical Value
ViewDirectoryComputersDisplayed	Numerical Value
ViewDirectoryPropertiesComputers	Unknown Numerical Value
ViewDirectoryPropertiesObjects	Unknown Numerical Value
ViewDirectoryPropertiesSharings	Unknown Numerical Value
ViewDirectoryThumbnails	Numerical Value
ViewSearchProperties	Unknown Numerical Value
ViewSearchThumbnails	Numerical Value
ViewTrafficDownloadsExpanded	Numerical Value
ViewTrafficProperties	Unknown Numerical Value



Name	Type	Data
(Default)	REG_SZ	(value not set)
NetworkWindowProperties	REG_SZ	332;360;987;779;0
NewsText	REG_SZ	hi....am looking for same as u.
NewsTextDate	REG_SZ	1238010047
SessionOldFlags	REG_SZ	000100
TrafficDefaultBlockSize	REG_SZ	2048
TrafficDownloadDirectory	REG_SZ	C:\Documents and Settings\Les\My Documents\My downloads GigaTribe\Lester64
ViewDirectoryPropertiesComputers	REG_SZ	1;0;1;250;150;100
ViewDirectoryPropertiesObjects	REG_SZ	1;0;1;200;150;150;150
ViewDirectoryPropertiesSharings	REG_SZ	1;0;1;200;100;200;200;200;200;300
ViewDirectoryThumbnails	REG_SZ	0
ViewSearchProperties	REG_SZ	1;0;1;200;150;150;150;259
ViewSearchThumbnails	REG_SZ	0
ViewTrafficProperties	REG_SZ	1;0;1;200;100;100;100;100;100;100

Sub-Key "Sharings"	(contains shared folders)

Note that in this case, I shared a single folder, "*My Pictures*", located under "My Documents" in my user profile. The actual path to this folder appears to be stored in encrypted format in the Data value, pre-pended with "**0x410F1294**", which is the same value that pre-pends the username key in the root of the Registry entry.



Name	Type	Data
(Default)	REG_SZ	(value not set)
My Pictures	REG_SZ	0x410F1294bcc5a3bb909c8a929a918b8...

Other sub-keys which may be present:

Sub-Key "Groups" (may or may not be present)

This sub-key was present on a suspect's computer which I was examining. It was not present on my test computer. I created a new user group within GigaTribe called "Picture Traders", but this did not result in a corresponding change to the registry. This sub-key may only be present in the "Ultimate" (paid) version of the program.

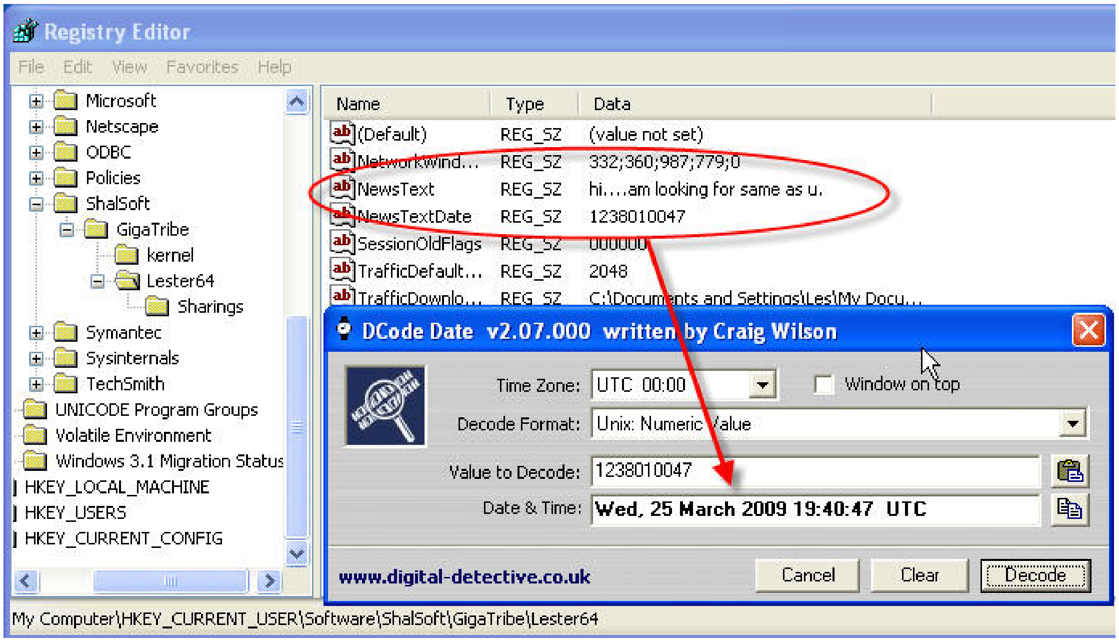
Sub-Key "Uploads" (may or may not be present)

This sub-key was present on a suspect's computer which I was examining. It was not present on my test computer. Even after uploading files to my 2nd test account, this sub-key was not created. This sub-key may only be present in the "Ultimate" (paid) version of the program.

ADDITIONAL FUNCTIONALITY:

- In the free version of Gigatribe, there is no option to password protect shared folders. In other words, users can freely download material from the shared folders of other users in your group. Password options are available only in the "*Ultimate*" version of Gigatribe.

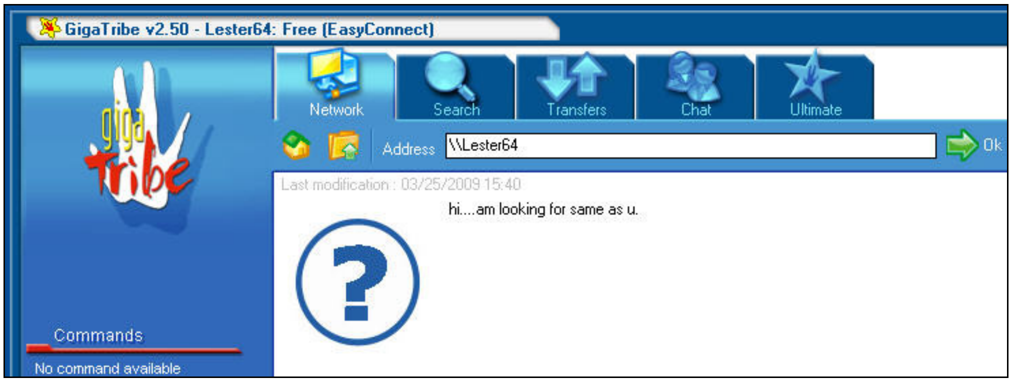
- A custom "greeting message" can be created in GigaTribe, and a profile picture can be inserted. The message and date it was created is stored in the Windows Registry. The date format is a Unix Numeric Value and easily decoded:



Name	Type	Data
(Default)	REG_SZ	(value not set)
NetworkWind...	REG_SZ	332;360;987;779;0
NewsText	REG_SZ	hi....am looking for same as u.
NewsTextDate	REG_SZ	1238010047
SessionOldFlags	REG_SZ	000000
TrafficDefault...	REG_SZ	2048
TrafficDownlo...	REG_SZ	C:\Documents and Settings\Les\My Docu...

Time Zone: UTC 00:00
☐ Window on top
Decode Format: Unix: Numeric Value
Value to Decode: 1238010047
Date & Time: Wed, 25 March 2009 19:40:47 UTC

My Computer\HKEY_CURRENT_USER\Software\ShalSoft\GigaTribe\Lester64



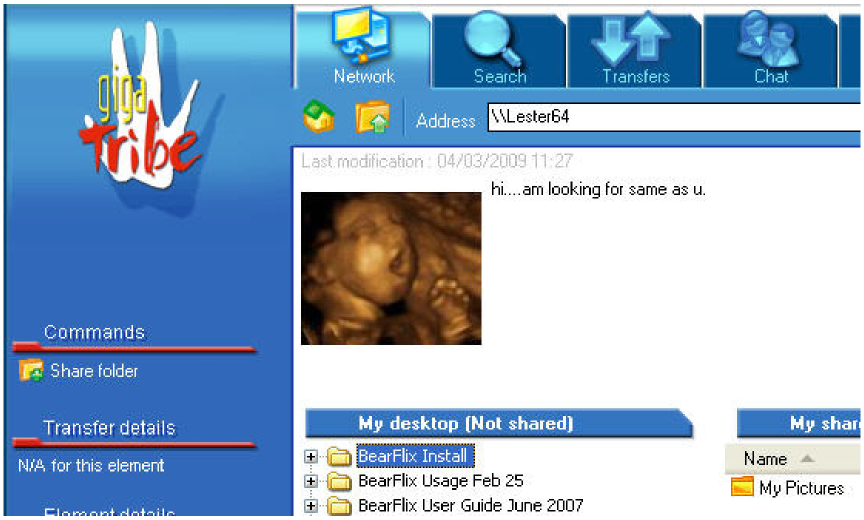
GigaTribe v2.50 - Lester64: Free (EasyConnect)

Address \\Lester64

Last modification : 03/25/2009 15:40

hi....am looking for same as u.

Note that if one chooses to put their picture into the program, this image is uploaded to the GigaTribe server and is stored there as an avatar, not on the local computer.



Address \\Lester64

Last modification : 04/03/2009 11:27

hi....am looking for same as u.

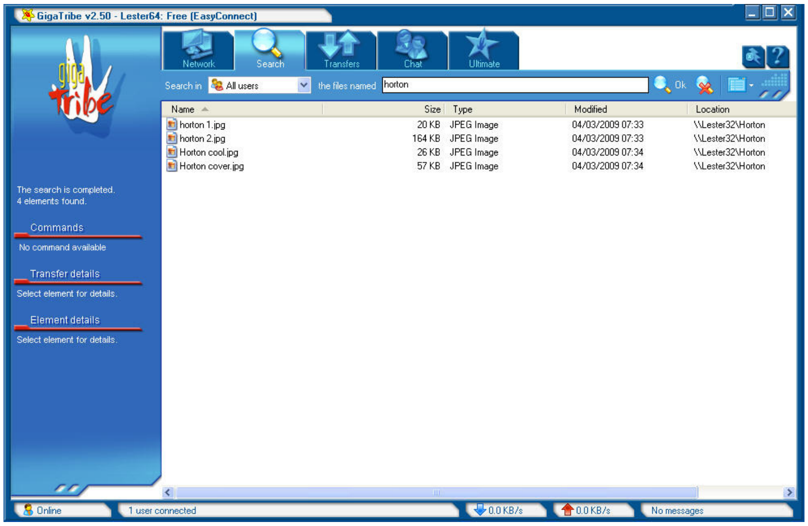
BearFlix Install
BearFlix Usage Feb 25
BearFlix User Guide June 2007

My Pictures

BASIC PROGRAM FUNCTIONS:

a. File Search and Download

GigaTribe has a **file search** function. I tested this by creating a second GigaTribe account on a different computer. The two accounts are "Lester64" and "Lester32". I created a shared folder on the remote computer and put four test pictures in it. In the following example, I searched my "friends network" for the term "horton", and the results were quickly displayed:



Search in: All users — the files named: horton

Name	Size	Type	Modified	Location
horton 1.jpg	20 KB	JPEG Image	04/03/2009 07:33	\\Lester32\Horton
horton 2.jpg	164 KB	JPEG Image	04/03/2009 07:33	\\Lester32\Horton
Horton cool.jpg	26 KB	JPEG Image	04/03/2009 07:34	\\Lester32\Horton
Horton cover.jpg	57 KB	JPEG Image	04/03/2009 07:34	\\Lester32\Horton

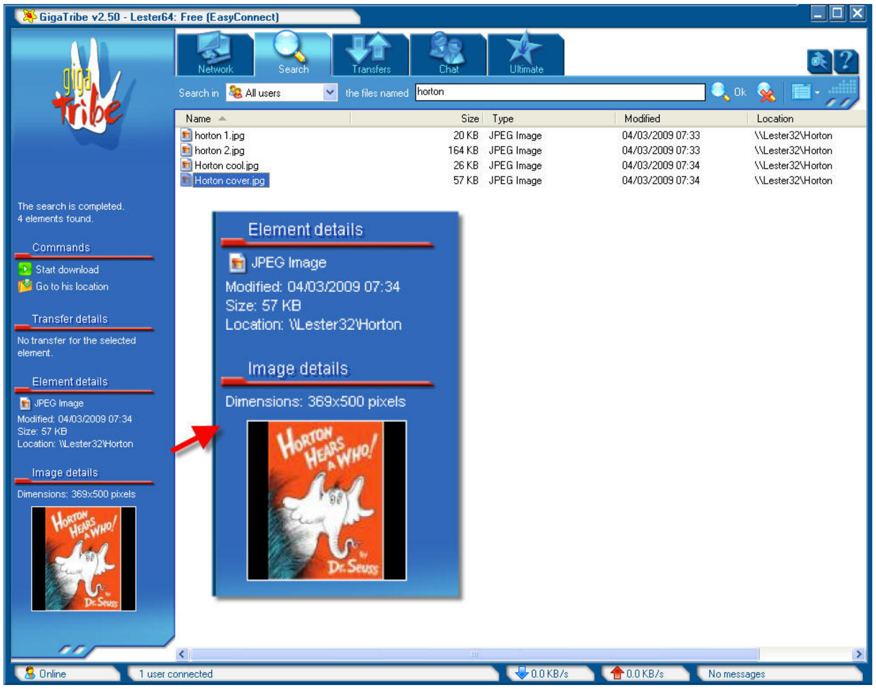
The search is completed.
4 elements found.

Commands
No command available

Transfer details
Select element for details.

Element details
Select element for details.

Selecting a particular file displays file details in the left pane:



Search in: All users — the files named: horton

Name	Size	Type	Modified	Location
horton 1.jpg	20 KB	JPEG Image	04/03/2009 07:33	\\Lester32\Horton
horton 2.jpg	164 KB	JPEG Image	04/03/2009 07:33	\\Lester32\Horton
Horton cool.jpg	26 KB	JPEG Image	04/03/2009 07:34	\\Lester32\Horton
Horton cover.jpg	57 KB	JPEG Image	04/03/2009 07:34	\\Lester32\Horton

The search is completed.
4 elements found.

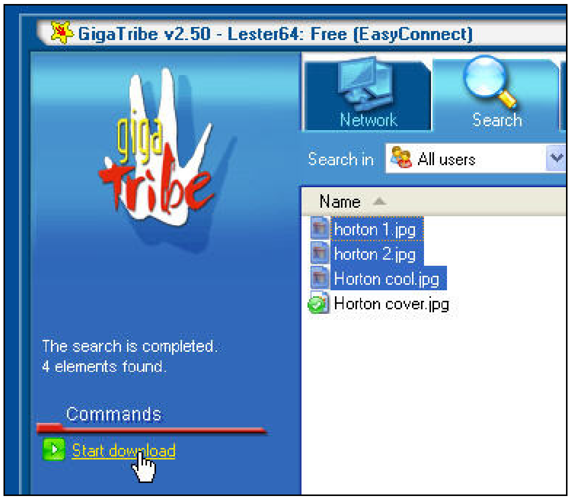
Commands

Transfer details
No transfer for the selected element.

Element details
JPEG Image
Modified: 04/03/2009 07:34
Size: 57 KB
Location: \\Lester32\Horton

Image details
Dimensions: 369x500 pixels

Files can then be selected for **download**.



Search in: All users

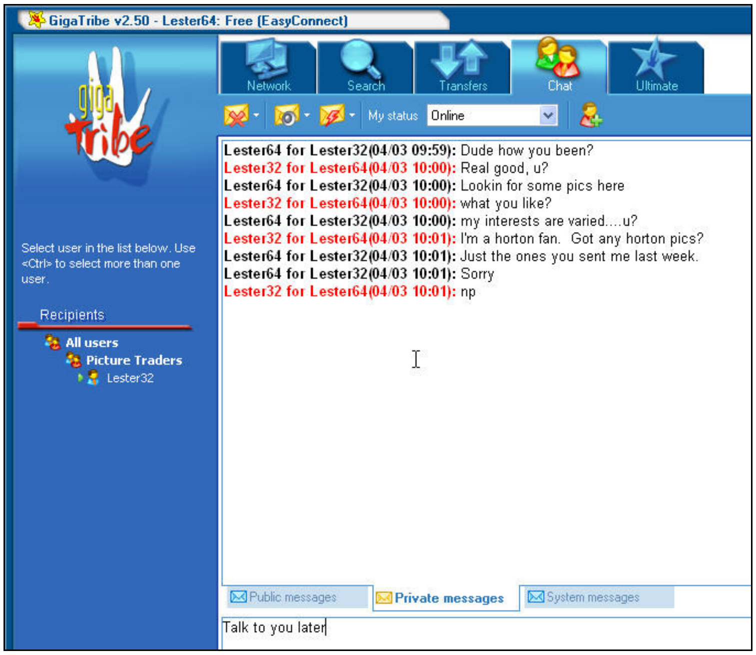
Name
horton 1.jpg
horton 2.jpg
Horton cool.jpg
Horton cover.jpg

The search is completed.
4 elements found.

At which point, the selected files are transferred to the user's GigaTribe download directory on the client computer.

b. Chat

GigaTribe has a built-in Chat client, which allows users to chat with other users in their groups.



My status: Online

Select user in the list below. Use <Ctrl> to select more than one user.

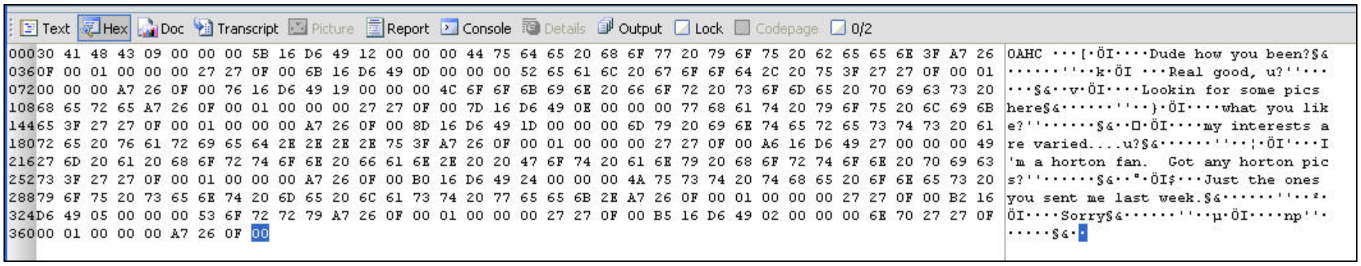
Lester64 for Lester32(04/03 09:59): Dude how you been?
Lester32 for Lester64(04/03 10:00): Real good, u?
Lester64 for Lester32(04/03 10:00): Lookin for some pics here
Lester32 for Lester64(04/03 10:00): what you like?
Lester64 for Lester32(04/03 10:00): my interests are varied....u?
Lester32 for Lester64(04/03 10:01): I'm a horton fan. Got any horton pics?
Lester64 for Lester32(04/03 10:01): Just the ones you sent me last week.
Lester64 for Lester32(04/03 10:01): Sorry
Lester32 for Lester64(04/03 10:01): np

Talk to you later

As stated previously, chat is logged in a file called "ChatHistory {username}.bin" at the following location:

C:\Documents and Settings\{user}\Application Data\Gigatribe

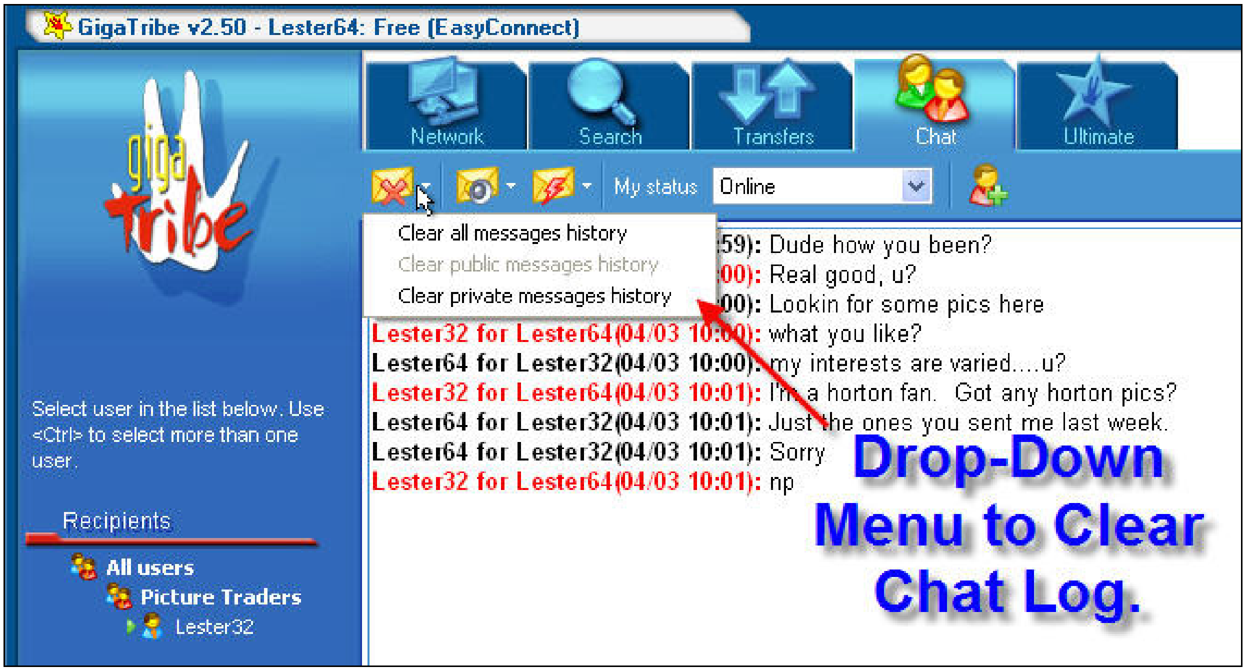
This file can be read in any text editor or a forensic program such as EnCase:



```
00030 41 48 43 09 00 00 00 5B 16 D6 49 12 00 00 00 44 75 64 65 20 68 6F 77 20 79 6F 75 20 62 65 65 6E 3F A7 26 0AHC ···[·ÖI····Dude how you been?§&
0360F 00 01 00 00 00 27 27 0F 00 6B 16 D6 49 0D 00 00 00 52 65 61 6C 20 67 6F 6F 64 2C 20 75 3F 27 27 0F 00 01 ·······''··k·ÖI ···Real good, u?''···
07200 00 00 A7 26 0F 00 76 16 D6 49 19 00 00 00 4C 6F 6F 6B 69 6E 20 66 6F 72 20 73 6F 6D 65 20 70 69 63 73 20 ···§&··v·ÖI····Lookin for some pics 
10868 65 72 65 A7 26 0F 00 01 00 00 00 27 27 0F 00 7D 16 D6 49 0E 00 00 00 77 68 61 74 20 79 6F 75 20 6C 69 6B here§&·······''··}·ÖI····what you lik
14465 3F 27 27 0F 00 01 00 00 00 A7 26 0F 00 8D 16 D6 49 1D 00 00 00 6D 79 20 69 6E 74 65 72 65 73 74 73 20 61 e?''·······§&··□·ÖI····my interests a
18072 65 20 76 61 72 69 65 64 2E 2E 2E 2E 75 3F A7 26 0F 00 01 00 00 00 27 27 0F 00 A6 16 D6 49 27 00 00 00 49 re varied....u?§&·······''··¦·ÖI'···I
21627 6D 20 61 20 68 6F 72 74 6F 6E 20 66 61 6E 2E 20 20 47 6F 74 20 61 6E 79 20 68 6F 72 74 6F 6E 20 70 69 63 'm a horton fan.  Got any horton pic
25273 3F 27 27 0F 00 01 00 00 00 A7 26 0F 00 B0 16 D6 49 24 00 00 00 4A 75 73 74 20 74 68 65 20 6F 6E 65 73 20 s?''·······§&··°·ÖI$···Just the ones 
28879 6F 75 20 73 65 6E 74 20 6D 65 20 6C 61 73 74 20 77 65 65 6B 2E A7 26 0F 00 01 00 00 00 27 27 0F 00 B2 16 you sent me last week.§&·······''··²·
324D6 49 05 00 00 00 53 6F 72 72 79 A7 26 0F 00 01 00 00 00 27 27 0F 00 B5 16 D6 49 02 00 00 00 6E 70 27 27 0F ÖI····Sorry§&·······''··µ·ÖI····np''·
36000 01 00 00 00 A7 26 0F 00                                                                                     ······§&··
```

Note that the date, time and user names appear to be encrypted.

Chat can also be cleared at the click of a button. This erases chat both within the program and inside the chat log file.


GigaTribe v2.50 - Lester64: Free (EasyConnect)
Network
Search
Transfers
Chat
Ultimate
My status
Online
Clear all messages history
Clear public messages history
Clear private messages history
Select user in the list below. Use <Ctrl> to select more than one user.
Recipients
All users
Picture Traders
Lester32

:59): Dude how you been?
:00): Real good, u?
:00): Lookin for some pics here
Lester32 for Lester64(04/03 10:00): what you like?
Lester64 for Lester32(04/03 10:00): my interests are varied....u?
Lester32 for Lester64(04/03 10:01): I'm a horton fan. Got any horton pics?
Lester64 for Lester32(04/03 10:01): Just the ones you sent me last week.
Lester64 for Lester32(04/03 10:01): Sorry
Lester32 for Lester64(04/03 10:01): np

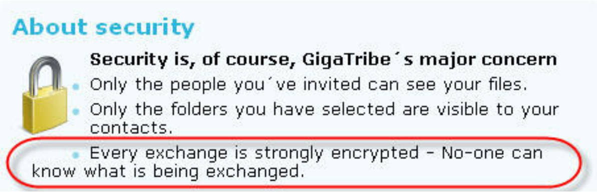
Drop-Down Menu to Clear Chat Log.

c. Search History:

Search History does not appear to be logged. There is no record of search terms used. This appears to exist only in memory while the search term is displayed.

d. Uploads:

There does not appear to be a log or other record of what has been uploaded. In fact, this seems to be a selling feature of the program. There is therefore, no way of knowing what has been shared with other users.



About security

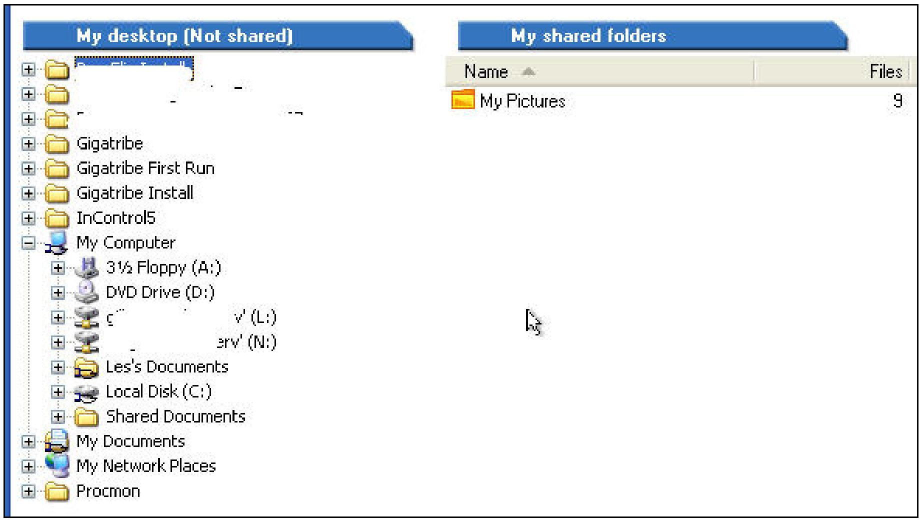
Security is, of course, GigaTribe´s major concern

- Only the people you´ve invited can see your files.
- Only the folders you have selected are visible to your contacts.
- Every exchange is strongly encrypted - No-one can know what is being exchanged.

e. Shared Folders:

The share names are stored in the Windows Registry in plain text as noted above. However, the path to these shares is encrypted. Other means of determining the actual folders being shared on a suspect's computer will be required. For instance, a unique folder name may allow you to draw an inference that that is the shared folder listed in the Registry.

Note that you cannot share a non-existent folder in GigaTribe. Gigatribe appears to hook the Explorer service in Windows and requires you to browse to the folders you wish to share.

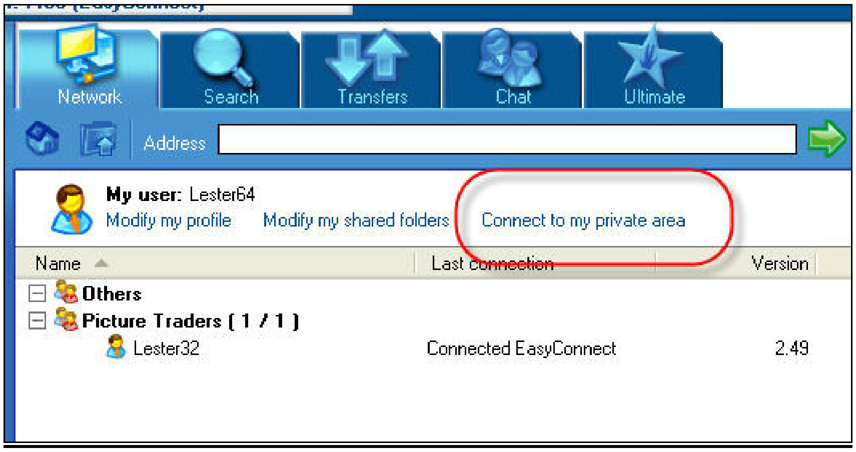


f. Friends List:

I could find no record of a "friends" or "contacts" list on the computer. This information appears to be stored on the server side, and would likely require judicial process to obtain this information from Shalsoft, which is located in France.

g. Web Interface "Private Area"

The user can connect to a "private area" via a web browser from within the GigaTribe program interface:



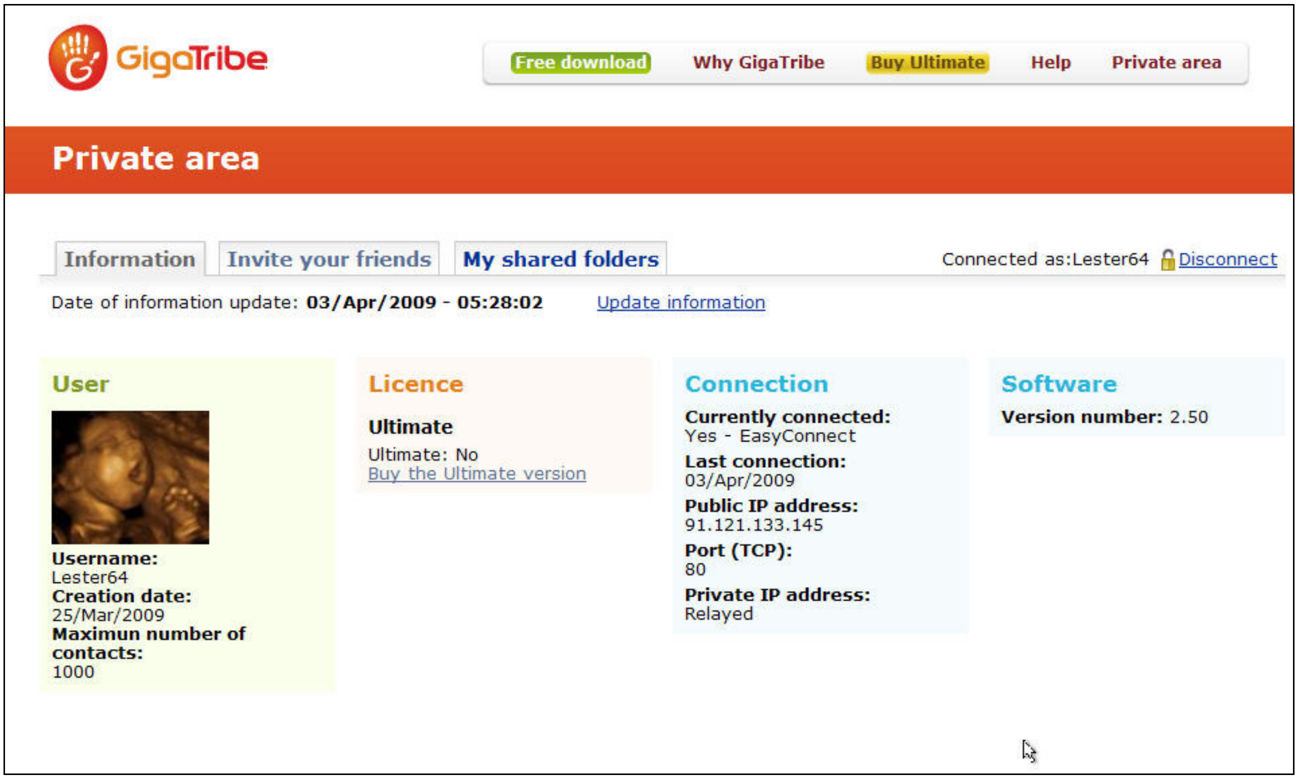
Clicking on this hyperlink opens a new window in the default web browser and logs the user into their "*private area*" on the GigaTribe server, at the following web address:

http://www.gigatribe.com/private/private_info.php

The first time this is done, a new file is created at:

C:\Documents and Settings\{user}\Application Data\Gigatribe

called "***server.log***". This file records a "Get" request and displays the IP address of the machine making the request. This file appears to contain historical information and may be of forensic value. It may contain information concerning files that are stored online in the "private area".



Private area

Connected as:Lester64 Disconnect

Date of information update: **03/Apr/2009 - 05:28:02** Update information

User

Username: Lester64
Creation date: 25/Mar/2009
Maximun number of contacts: 1000

Licence

Ultimate
Ultimate: No
Buy the Ultimate version

Connection

Currently connected: Yes - EasyConnect
Last connection: 03/Apr/2009
Public IP address: 91.121.133.145
Port (TCP): 80
Private IP address: Relayed

Software

Version number: 2.50

Clearly the Private Area contains a lot of useful information about the user, including shared folders. If this web page can be recovered on a suspect computer, it would be very valuable. If not present in the Web Cache, unique search expressions could be developed to find the file in unallocated space or other system files.

<u>FOR FURTHER STUDY:</u>

- I have not developed any search expressions to search for deleted chat, search terms, or upload file records which may be present in unallocated space or other system files.
- All of my testing to date has been on the "free" version of GigaTribe. I was not able to determine what files and folders are changed, added or deleted when one upgrades to the "Ultimate" version, if any. I suspect that most of the additional program functionality of the "Ultimate" version is enabled on the GigaTribe server side when one starts the program and logs into the GigaTribe network.
- I encountered GigaTribe for the first time during a Child Pornography investigation in which the suspect had installed GigaTribe and used it to trade Child Pornography with other GigaTribe users. I suspect the suspect had the Ultimate version of GigaTribe, due to the presence of several registry keys not present on my "free" installation test machine. However, I was unable to confirm this. I could not locate an "installation log file" or other artifact which stated version information. I therefore do not have a

method for determining which version is installed on a specific computer.

- The encryption scheme used to encrypt the username and shared folder paths is unknown. If this encryption algorithm were better understood or broken, additional information would be available to investigators from the Windows Registry.

- Develop search terms to find the GigaTribe "Private Area" web page in unallocated space or other system files.

- Clarify the ways in which a user can interact with their online "Private Area" and whether or not users can access this area.

CONCLUSION and SUMMARY:

GigaTribe is an interesting program from a forensic standpoint. While many aspects of the program are encrypted, easily deleted or not recorded at all, there is substantial information to be gathered from server logs and registry keys, as noted above.

- In particular, chat, if not erased, is stored in the "ChatHistory{*username*}.bin" file.
- The user's custom greeting message is save in the Windows Registry in plain text.
- A record of shared folder names is stored in the Windows Registry. These folders can be identified on the suspect computer and if it is ascertained that Child Pornography is present, this can help to support a charge of "making available".
- Historical program usage information is available from the "session.log" file.
- Determine if the user connected to their web-based "private area" on the GigaTribe server, based on the presence of the "*server.log*" file.
- The "Private Area" web page could potentially be recovered from the Web Cache on a suspect computer.