



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 Forensic Guide

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

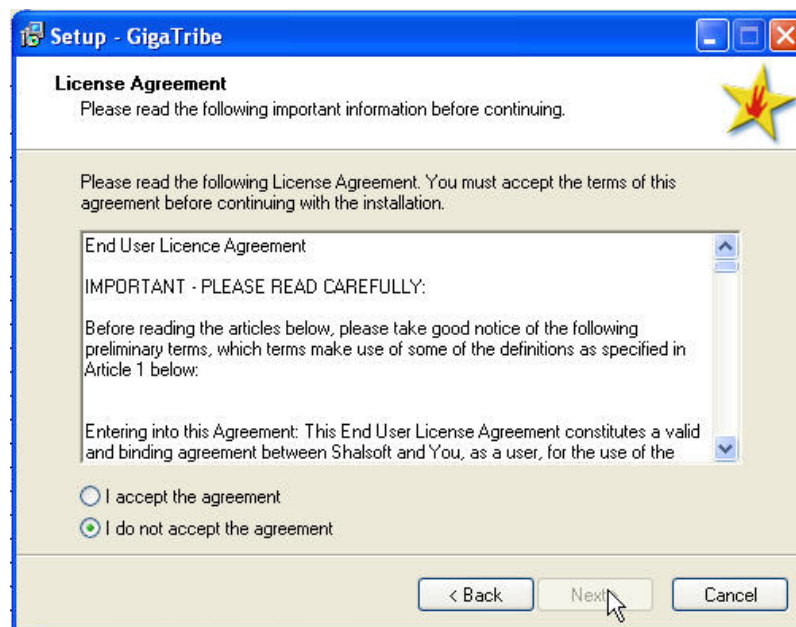


GIGATRIBE INSTALLATION:

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



A License Agreement screen follows:



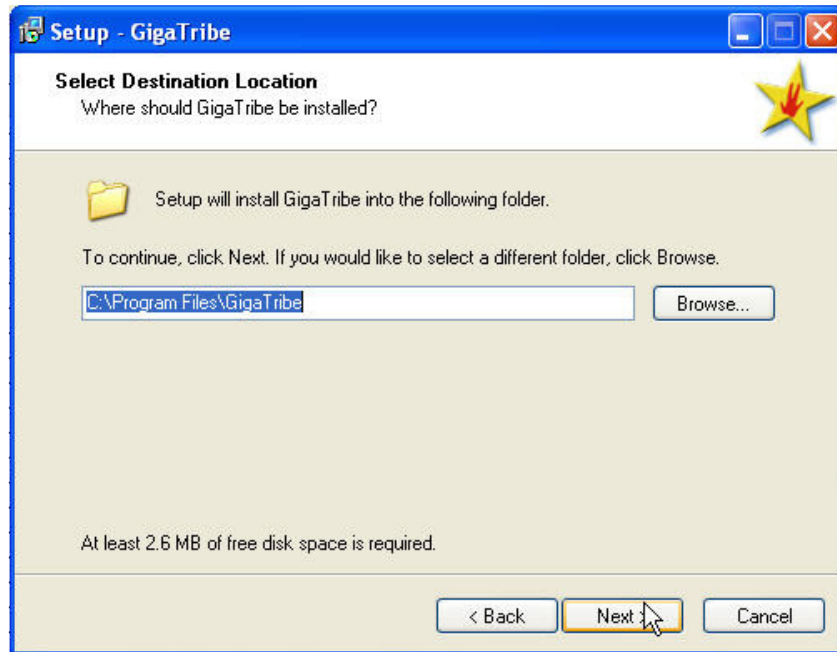


GigaTribe Forensic Guide

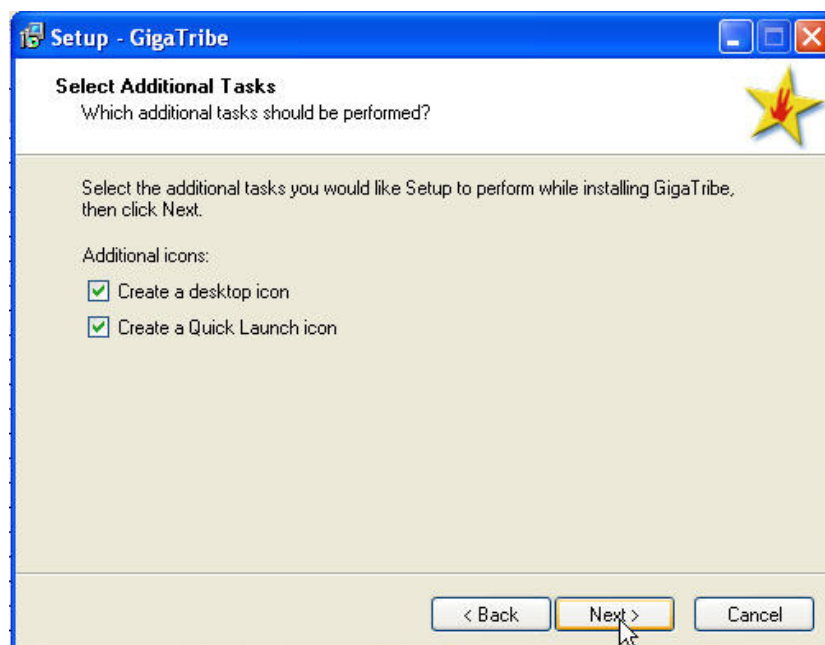
D/Sgt. Les Vuyk #9937
Niagara Regional Police Service
Technological Crime Unit



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



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.



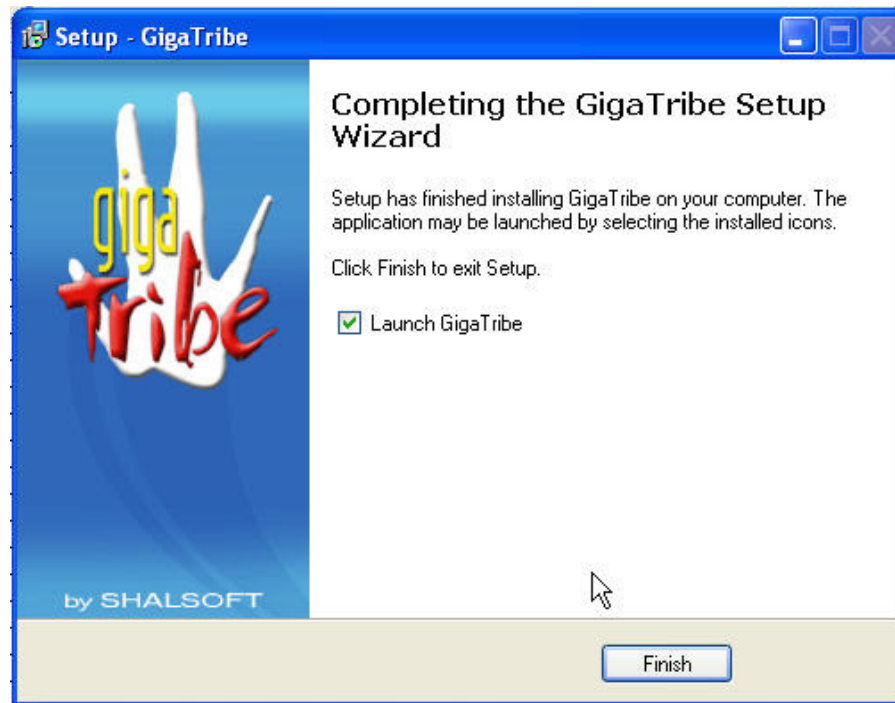


GigaTribe Forensic Guide

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



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





GigaTribe Forensic Guide

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



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.

Cancel Create

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:

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.

Cancel Create

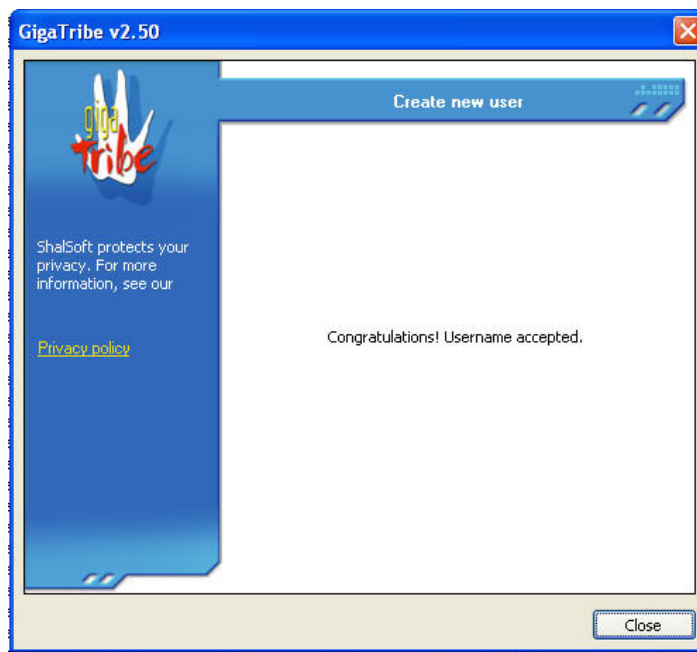
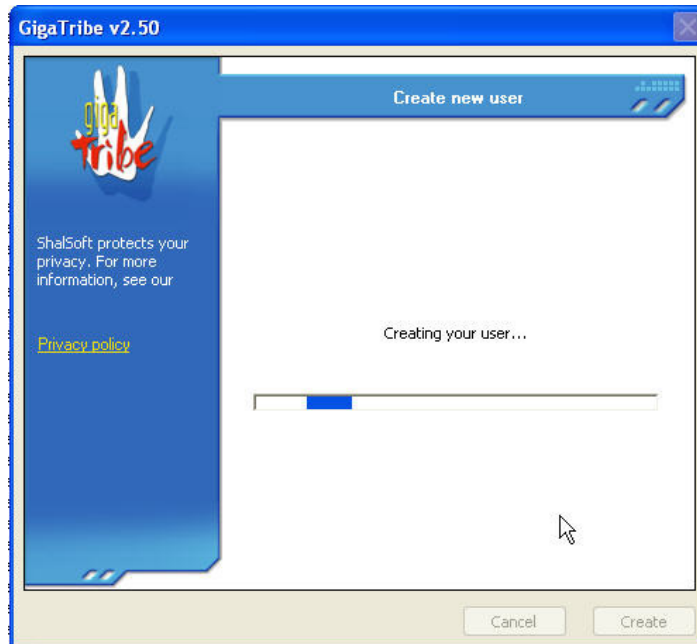


GigaTribe Forensic Guide

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



My account was then created



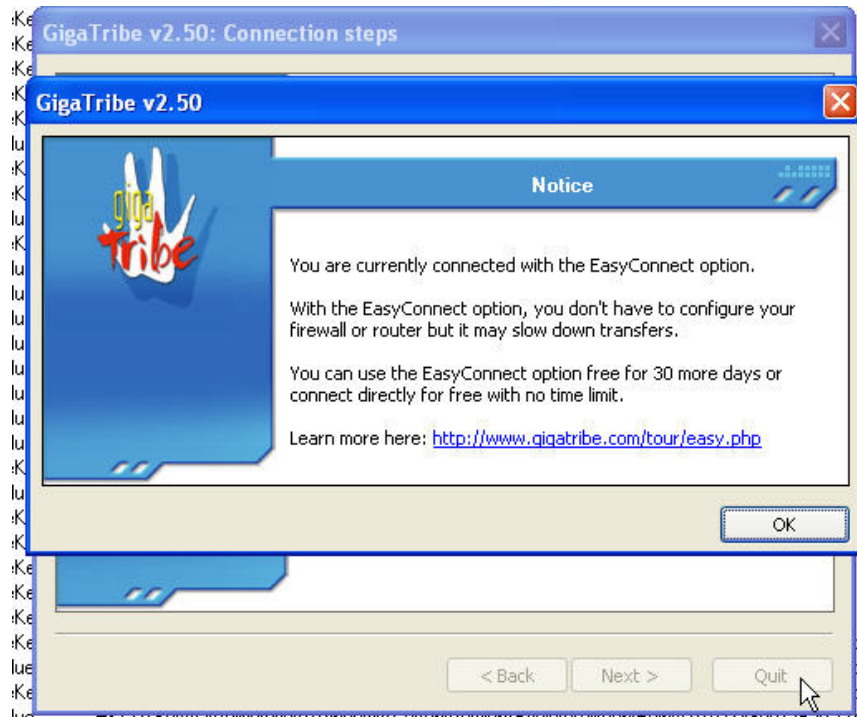


GigaTribe Forensic Guide

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



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



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





GigaTribe Forensic Guide

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

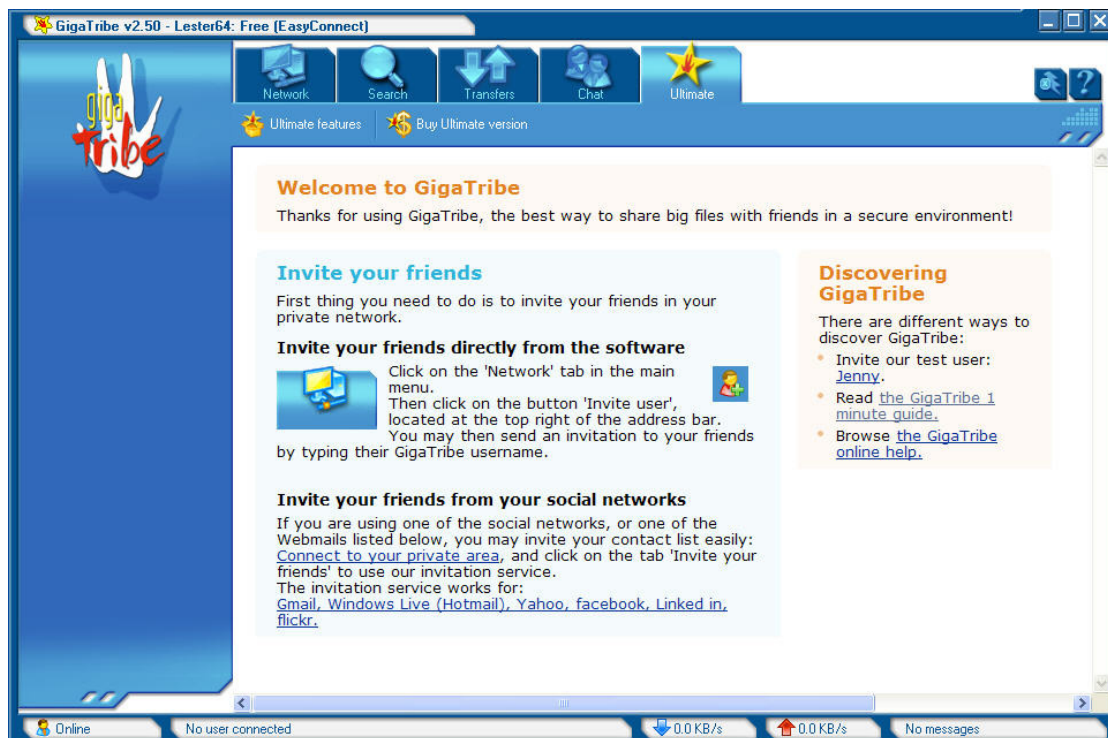


ADDITIONAL SET UP (Free Version):

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.





GigaTribe Forensic Guide

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



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)

< Back Next > Cancel

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):

< Back Next > Cancel

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

GigaTribe v2.50

Group properties

Group name:

☐ Automatically accept invitations when access code is provided

How to automatically accept invitations with an access code?

Cancel Create

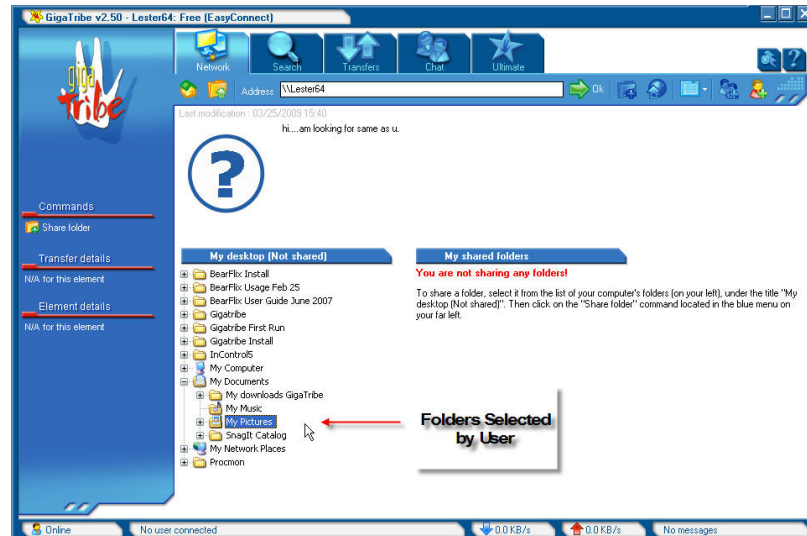


GigaTribe Forensic Guide



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

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.



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





GigaTribe Forensic Guide

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



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 Forensic Guide

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

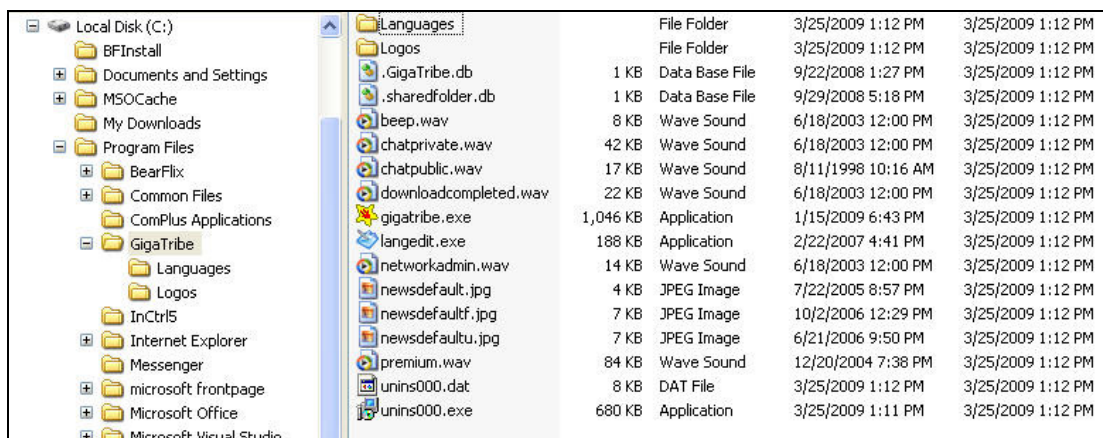


GIGATRIBE INSTALLATION DETAILS:

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:

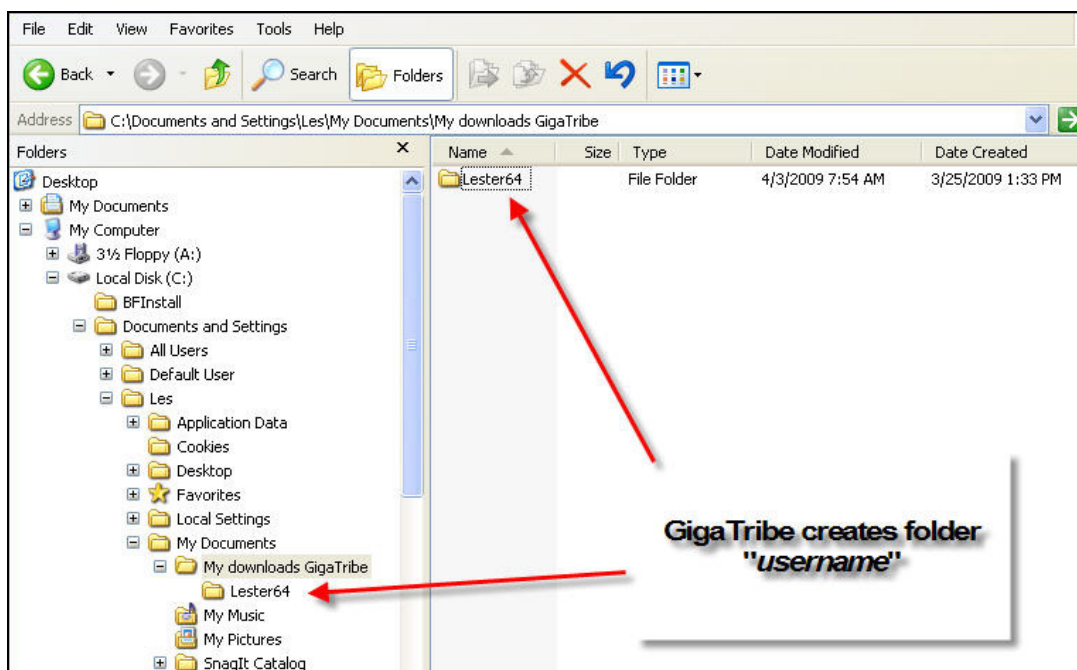
C:\Program Files\Gigatribe (assuming "C" is where Windows is installed)



Local Disk (C:)	Languages	File Folder	3/25/2009 1:12 PM	3/25/2009 1:12 PM
BFInstall	Logos	File Folder	3/25/2009 1:12 PM	3/25/2009 1:12 PM
Documents and Settings	.GigaTribe.db	1 KB Data Base File	9/22/2008 1:27 PM	3/25/2009 1:12 PM
MSOCache	.sharedfolder.db	1 KB Data Base File	9/29/2008 5:18 PM	3/25/2009 1:12 PM
My Downloads	beep.wav	8 KB Wave Sound	6/18/2003 12:00 PM	3/25/2009 1:12 PM
Program Files	chatprivate.wav	42 KB Wave Sound	6/18/2003 12:00 PM	3/25/2009 1:12 PM
BearFlix	chatpublic.wav	17 KB Wave Sound	8/11/1998 10:16 AM	3/25/2009 1:12 PM
Common Files	downloadcompleted.wav	22 KB Wave Sound	6/18/2003 12:00 PM	3/25/2009 1:12 PM
ComPlus Applications	gigatribe.exe	1,046 KB Application	1/15/2009 6:43 PM	3/25/2009 1:12 PM
GigaTribe	langedit.exe	188 KB Application	2/22/2007 4:41 PM	3/25/2009 1:12 PM
Languages	networkadmin.wav	14 KB Wave Sound	6/18/2003 12:00 PM	3/25/2009 1:12 PM
Logos	newsdefault.jpg	4 KB JPEG Image	7/22/2005 8:57 PM	3/25/2009 1:12 PM
InCtrl5	newsdefaultf.jpg	7 KB JPEG Image	10/2/2006 12:29 PM	3/25/2009 1:12 PM
Internet Explorer	newsdefaultu.jpg	7 KB JPEG Image	6/21/2006 9:50 PM	3/25/2009 1:12 PM
Messenger	premium.wav	84 KB Wave Sound	12/20/2004 7:38 PM	3/25/2009 1:12 PM
microsoft frontpage	unins000.dat	8 KB DAT File	3/25/2009 1:12 PM	3/25/2009 1:12 PM
Microsoft Office	unins000.exe	680 KB Application	3/25/2009 1:11 PM	3/25/2009 1:12 PM
Microsoft Visual Studio				

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

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





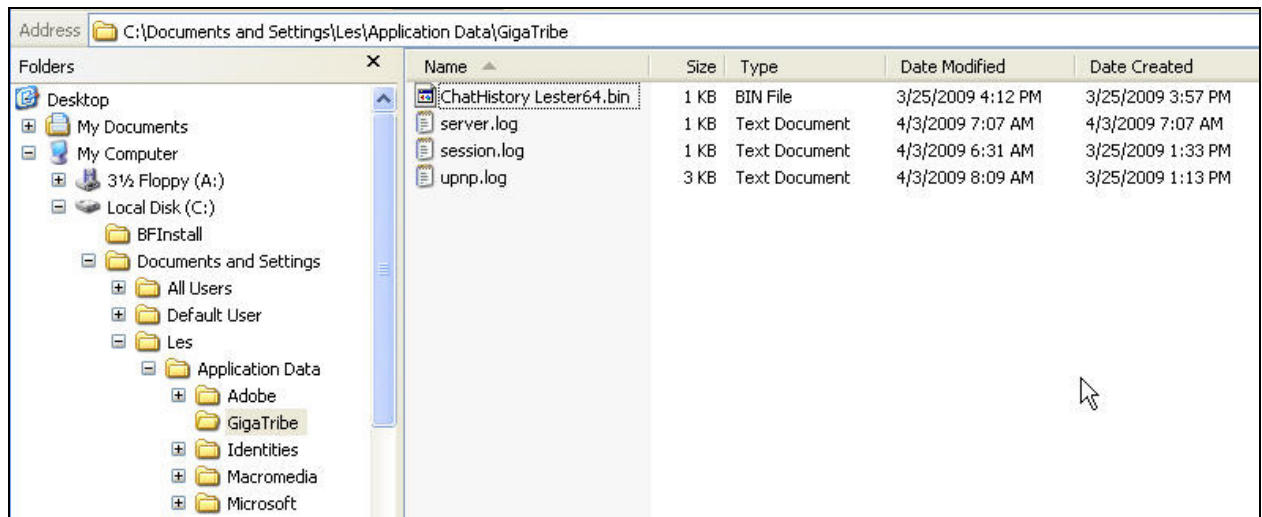
GigaTribe Forensic Guide

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



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

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



- 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)

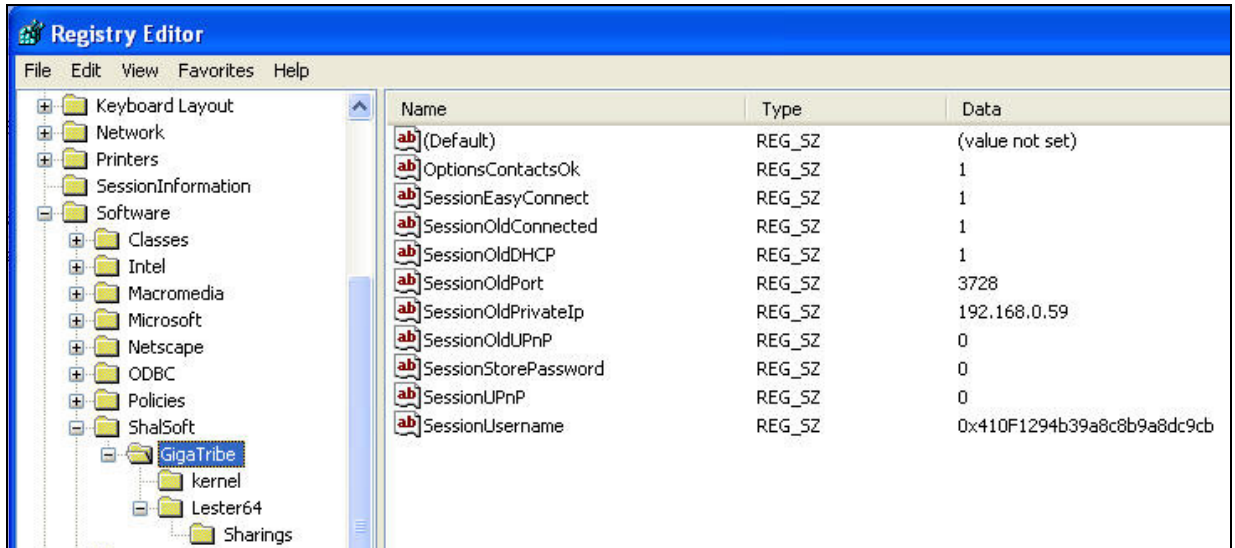


GigaTribe Forensic Guide

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

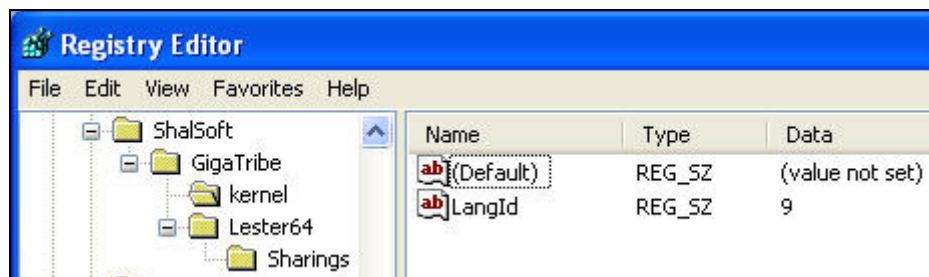


SessionOldPrivateIP:	Shows IP address of host computer
SessionOldPort:	Shows Port (appears to be 3728 by default - un-confirmed)
SessionOldUPnP:	Off or On (value 0 or 1) (default "0") (may be more values allowed)
SessionOldDHCP:	Off or On (value 0 or 1) (default "0") (may be more values allowed)
OptionsContactsOk: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



Sub-Key "kernel":

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

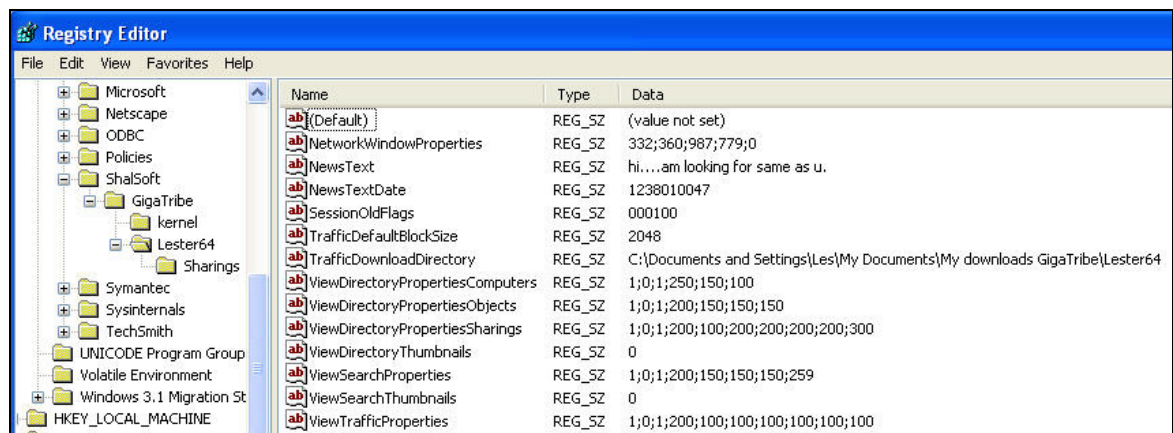


GigaTribe Forensic Guide

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



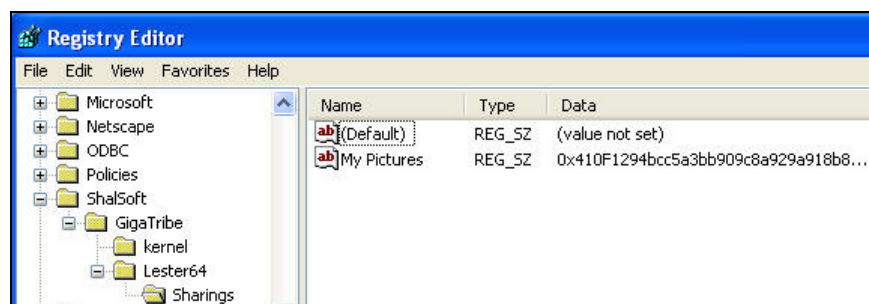
TrafficMaxDownloadsUI	Unknown numerical value
TrafficMaxSpeedUploads	Off or On (value 0 or 1) (may be more values allowed)
TrafficMaxSpeedUploadsUI	Unknown numerical value
TrafficMaxSpeedWhenAfk	Off or On (value 0 or 1) (may be more values allowed)
TrafficMaxUploads	Numerical Value
TrafficMaxUploadsPerComputer	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



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.





GigaTribe Forensic Guide

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



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.

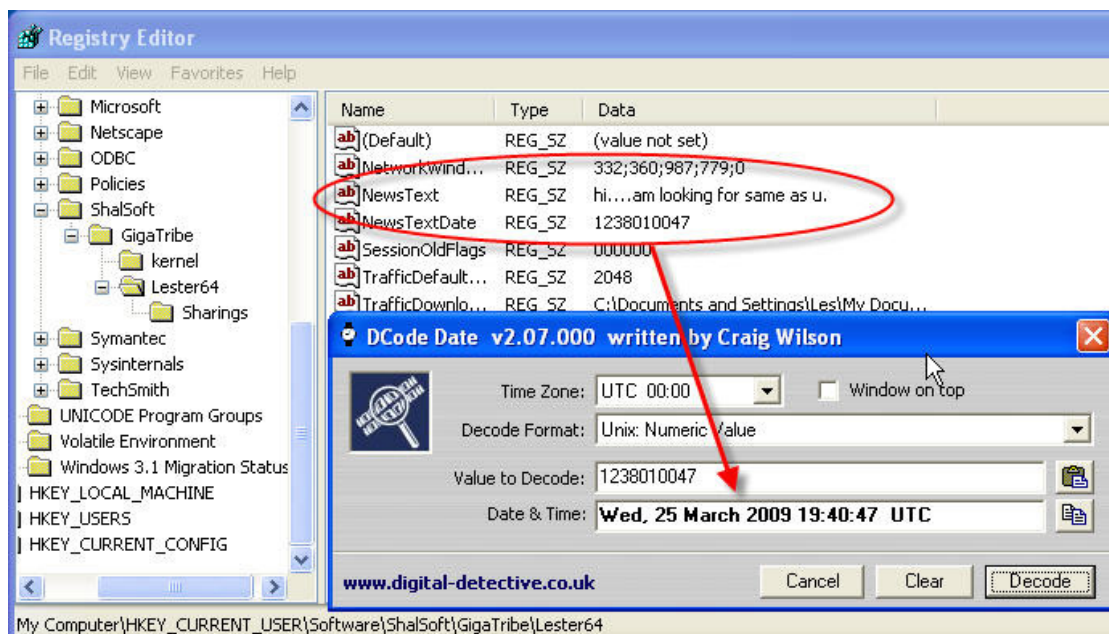
Sub-Key "Uploads"

(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:

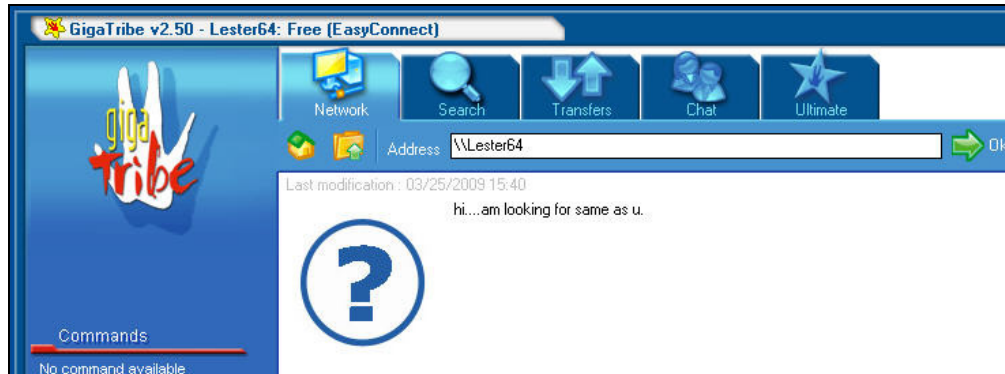
- In the free version of GigaTribe, there is no option to password protect shared folders. In other words, users can freely download material from the shared folders of other users in your group. Password options are available only in the "Ultimate" version of GigaTribe.
- A custom "greeting message"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





GigaTribe Forensic Guide

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



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.





GigaTribe Forensic Guide

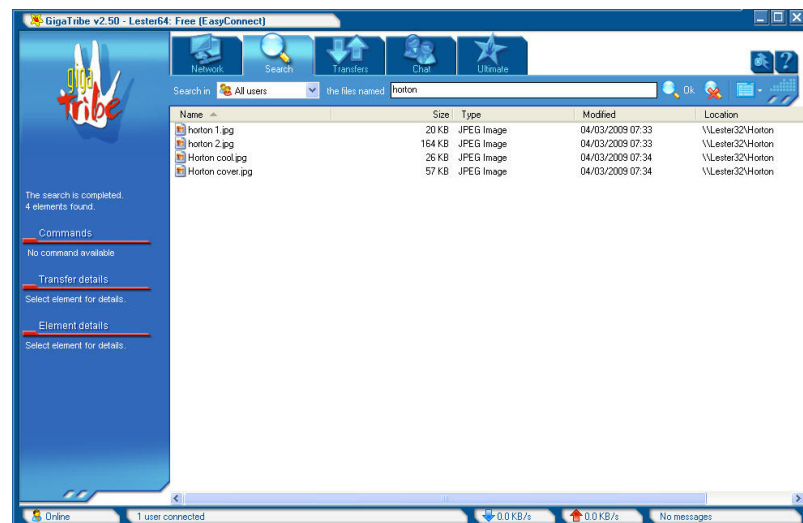


D/Sgt. Les Vuyk #9937
Niagara Regional Police Service
Technological Crime Unit

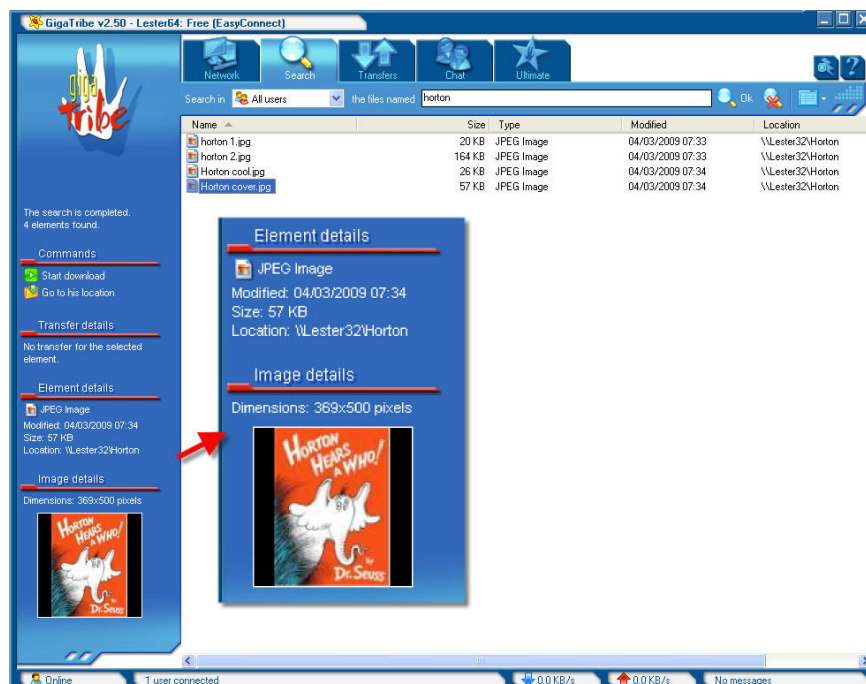
BASIC PROGRAM FUNCTIONS:

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:



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





GigaTribe Forensic Guide

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



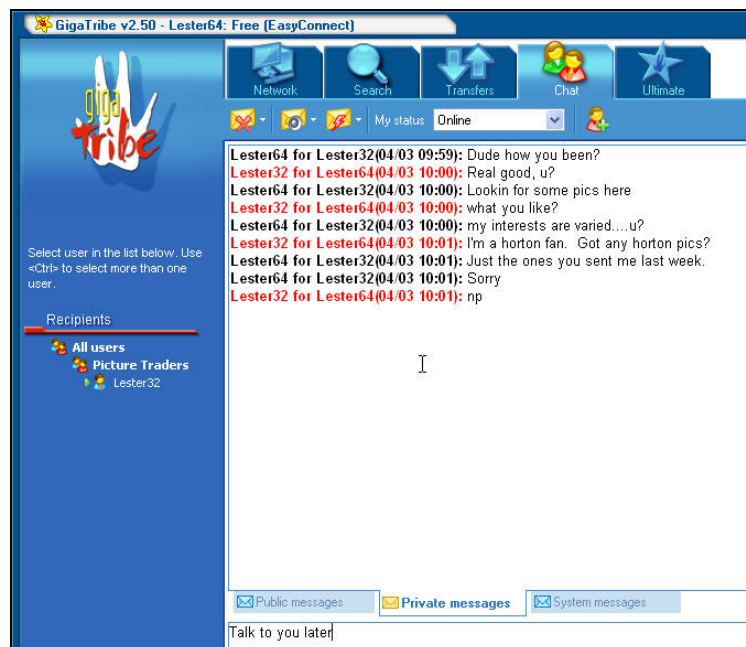
Files can then be selected for **download**.



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.





GigaTribe Forensic Guide

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



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

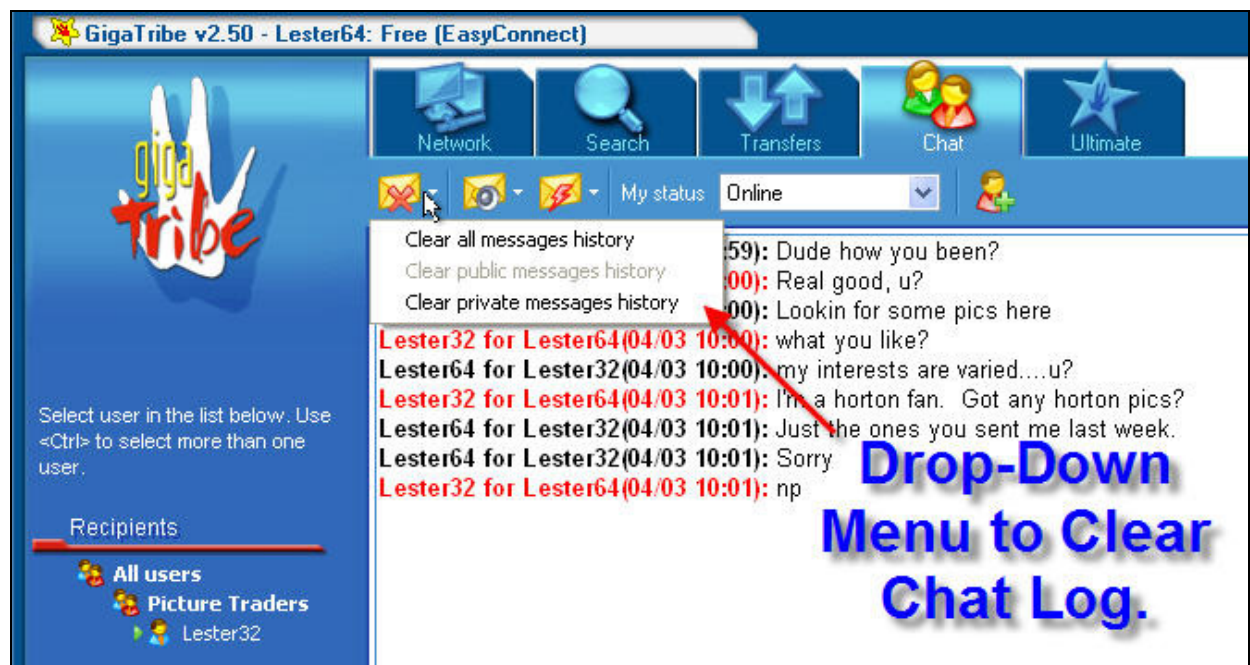
C:\Documents and Settings\{user}\Application Data\Gigatribe

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 ...[.OI....Dude how you been?.$&
0360F 00 01 00 00 00 27 27 0F 00 6B 16 D6 49 0D 00 00 00 52 65 61 6C 20 67 6F 6F 64 2C 20 75 3F 27 27 0F 00 01 .....k.OI ...Real good, u?''''
07200 00 00 A7 26 0F 00 76 16 D6 49 19 00 00 00 4C 6F 6F 6B 69 6E 20 66 6F 72 20 73 6F 6D 65 20 70 69 63 73 20 ...$.v.OI....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$. ....}.OI....what you lik
14465 3F 27 27 0F 00 01 00 00 00 A7 26 0F 00 8D 16 D6 49 1D 00 00 00 6D 79 20 69 6E 74 65 72 65 73 74 73 20 61 e?''''''$.D.OI....my interests a
18072 65 20 76 61 72 69 65 64 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?$. ....}.OI....I
21627 6D 20 61 20 68 6F 72 74 6F 6E 20 66 61 6E 2E 20 20 47 6F 74 20 61 6E 79 20 68 6F 72 74 6F 6E 20 70 69 63 'm a horton fan. Got any horton pic
25273 3F 27 27 0F 00 01 00 00 00 A7 26 0F 00 B0 16 D6 49 24 00 00 00 4A 75 73 74 20 74 68 65 20 6F 6E 65 73 20 s?''''''$.*.OI...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.$&.....
324D6 49 05 00 00 00 53 6F 72 72 79 A7 26 0F 00 01 00 00 00 27 27 0F 00 B5 16 D6 49 02 00 00 00 6E 70 27 27 0F OI....Sorry$. ....p.OI....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 Forensic Guide

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



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



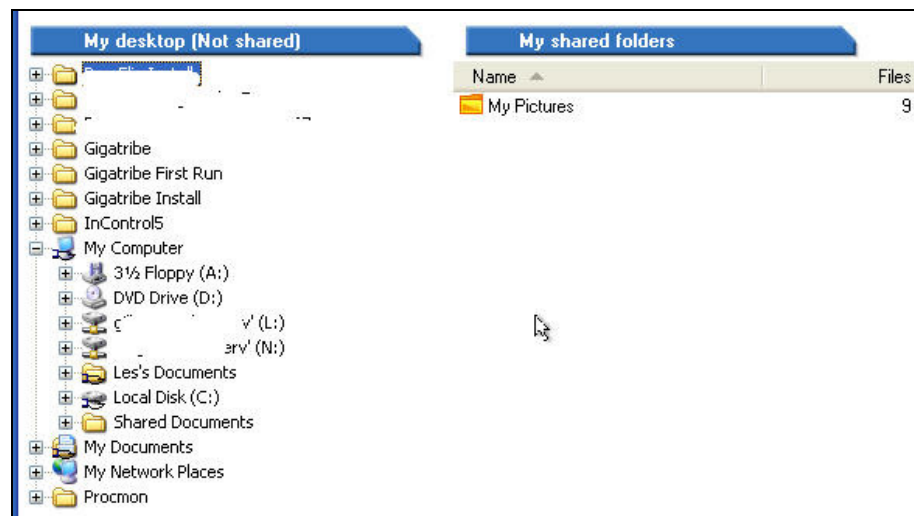
Security is, of course, GigaTribe's major concern

- 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.





GigaTribe Forensic Guide

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

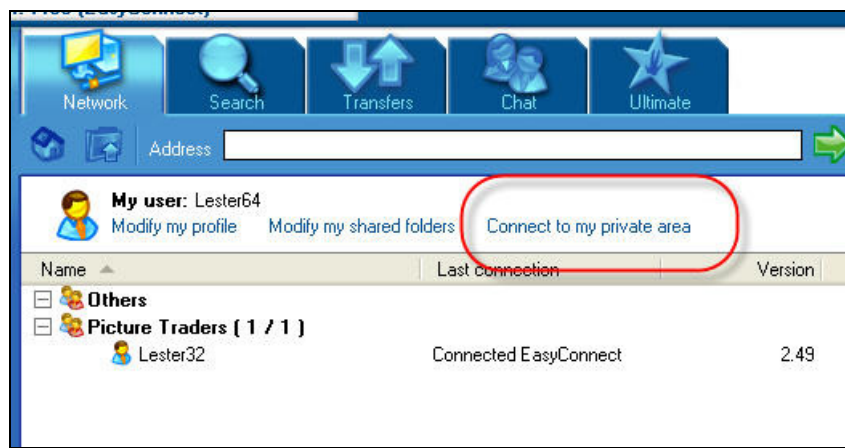


f. Friends List:

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".



GigaTribe Forensic Guide

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



GigaTribe [Free download](#) [Why GigaTribe](#) [Buy Ultimate](#) [Help](#) [Private area](#)

Private area

[Information](#) [Invite your friends](#) [My shared folders](#) Connected as: Lester64 [Disconnect](#)

Date of information update: **03/Apr/2009 - 05:28:02** [Update information](#)

User	Licence	Connection	Software
 Username: Lester64 Creation date: 25/Mar/2009 Maximun number of contacts: 1000	Ultimate Ultimate: No Buy the Ultimate version	Currently connected: Yes - EasyConnect Last connection: 03/Apr/2009 Public IP address: 91.121.133.145 Port (TCP): 80 Private IP address: Relayed	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.

FOR FURTHER STUDY:

- 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



GigaTribe Forensic Guide

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



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.