Longitudinal Employer - Household Dynamics

Informational Document No. ID-2003-01

How to use FTP and PGP to send files to LEHD

Date : December 31, 2003
Prepared by : Lars Vilhuber
Contact : U.S. Census Bureau, LEHD Program
FB 2138-3
4700 Silver Hill Rd.
Suitland, MD 20233 USA

This document contains information provided to LEHD partners and customers. It has undergone a Census Bureau review more limited in scope than that given to official Census Bureau publications. [This document is released to encourage discussion of work in progress, and to provide information necessary for an efficient cooperation.] The U.S. Census Bureau's Longitudinal Employer-Household Dynamics Program (LEHD), is partially supported by the National Science Foundation Grant SES-9978093 to Cornell University (Cornell Institute for Social and Economic Research), the National Institute on Aging, and the Alfred P. Sloan Foundation. The views expressed herein and the information provided herein are attributable only to the author(s) and do not represent the views of the U.S. Census Bureau, its program sponsors or data providers. Some or all of the data referenced in this paper are confidential data from the LEHD Program. For further information, please contact U.S. Census Bureau, LEHD Program, Demographic Surveys Division, FOB 3, Room 2138, 4700 Silver Hill Rd., Suitland, MD 20233, USA.

How to use FTP and PGP to send files to LEHD

Lars Vilhuber

DRAFT December 31, 2003

Contents

1 Quick reference

- First time: Install PGP software.
- First time, and once a year: Install LEHD public key
- (Optionally) Generate MD5SUM
- Encrypt data (and MD5SUM) file using PGP right-click menu.
- Transfer encrypted data file to Census FTP server "ftp2.census.gov" using FTP client software

2 Obtaining Software

2.1 PGP

The software needed is the widely used PGP client software, available from PGP Corporation ($$) for Windows and Macintosh clients. The discussion in this document will help in setting up and using that client, for which LEHD LMI partner states can obtain one license from LEHD.

Alternative software for almost all operating systems can be obtained from GNU Privacy Guard (free). A command-line interface fully compatible with the OpenPGP standard, called “Filecrypt”, can also be obtained from Veridis.

2.2 FTP Client

Almost all operating systems (including Windows) contain a command line FTP interface, and graphical client software exists for most graphical interfaces. In Windows, Internet Explorer has FTP capability, though you may have a different favorite client. Any FTP client will work. Others include (incomplete list):

- WS FTP LE, free for government and home users.

2.3 MD5SUM utility

A popular checksum is the MD5SUM. Windows/DOS utilities can be downloaded for free from http://www.md5summer.org/. A GNU version of “md5sum” is generally available for UNIX systems. Copies of both the GUI and the command line utilities were provided on your setup disk. We will assume that you are using the graphical version “MD5 Summer”.

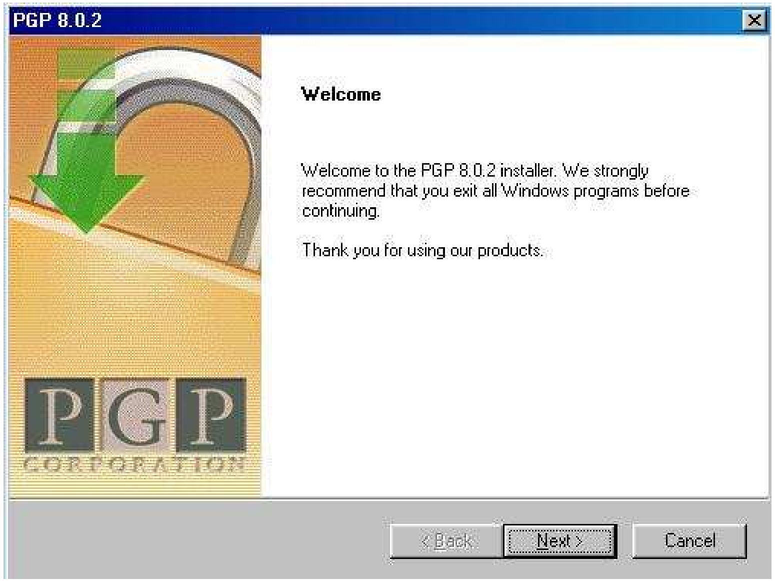
3 Installation of software

3.1 Installing PGP (Windows)

Unless otherwise stated, and in particular if no screenshot is provided, simply choose the default option provided by the installer. Note that the installation requires you to reboot your PC.

You can either download the installer from the PGP website, or obtain it on CDROM. In either case, locate the installer file (`PGP8.exe`, `PGPDesktop.exe`, or similar). If this is a ZIP archive, it will contain the actual installer file and its PGP signature. Use the actuall installer file, and double-click on it. You will see Figure 1.

Figure 1: Initial installation screen



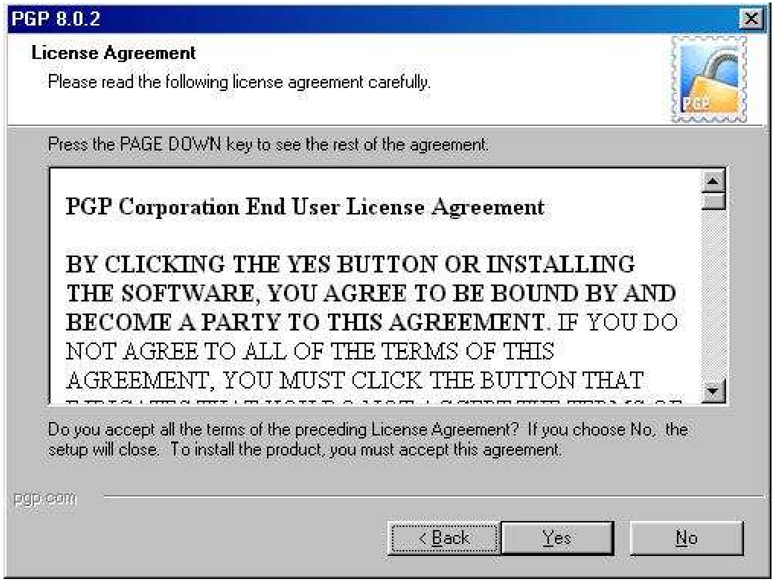
Welcome

Welcome to the PGP 8.0.2 installer. We strongly recommend that you exit all Windows programs before continuing.

Thank you for using our products.

In order to proceed, accept the license agreement by clicking on YES:

Figure 2: Accept license agreement



License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

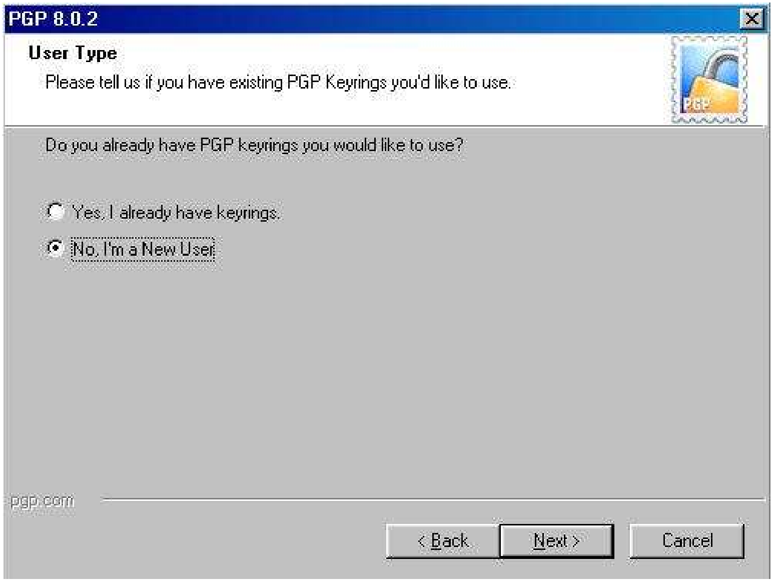
PGP Corporation End User License Agreement

BY CLICKING THE YES BUTTON OR INSTALLING THE SOFTWARE, YOU AGREE TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, YOU MUST CLICK THE BUTTON THAT

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install the product, you must accept this agreement.

If not pre-selected, choose "I'm a New User" in Figure 3.

Figure 3: Installation screen 3



Please tell us if you have existing PGP Keyrings you'd like to use.

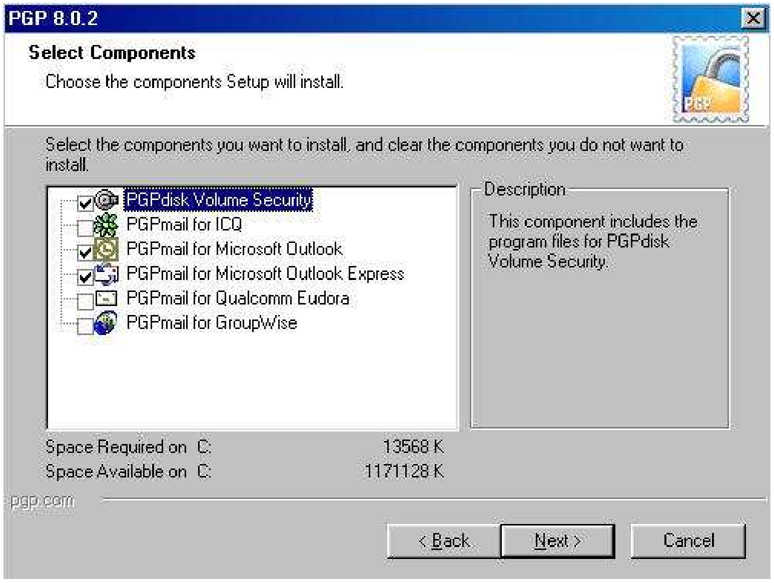
Do you already have PGP keyrings you would like to use?

○ Yes, I already have keyrings.

● No, I'm a New User

The installer will always install the basic Key Management tools. On Figure 4, you have the choice of installing a number of additional options. Not all of these will be covered by your license, but can be installed without problem. You need none of these for encrypting files on your harddrive.

Figure 4: Installation options



PGP 8.0.2

Select Components

Choose the components Setup will install.

Select the components you want to install, and clear the components you do not want to install.

- ☑ PGPdisk Volume Security
- □ PGPmail for ICQ
- ☑ PGPmail for Microsoft Outlook
- ☑ PGPmail for Microsoft Outlook Express
- □ PGPmail for Qualcomm Eudora
- □ PGPmail for GroupWise

Description

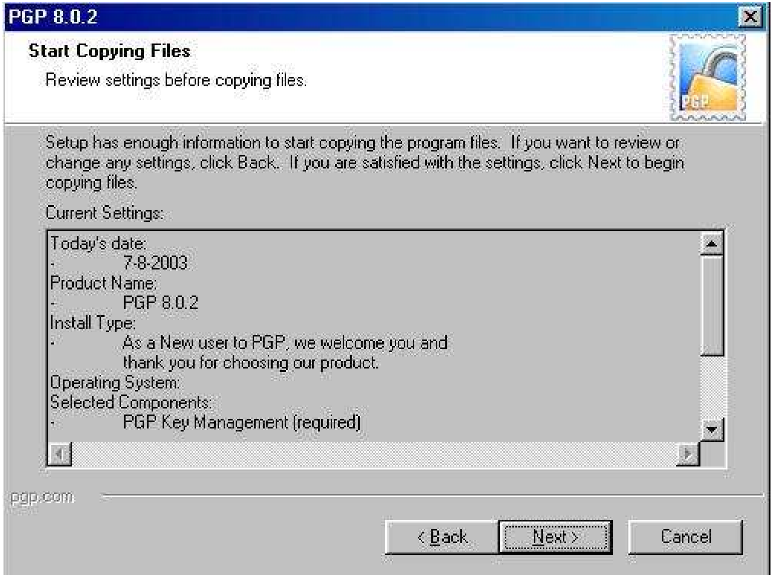
This component includes the program files for PGPdisk Volume Security.

Space Required on C: 13568 K

Space Available on C: 1171128 K

Before finalizing the installation, you get the chance to review your choices in Figure 5. If anything does not look right, simply go "Back".

Figure 5: Review options



Start Copying Files

Review settings before copying files.

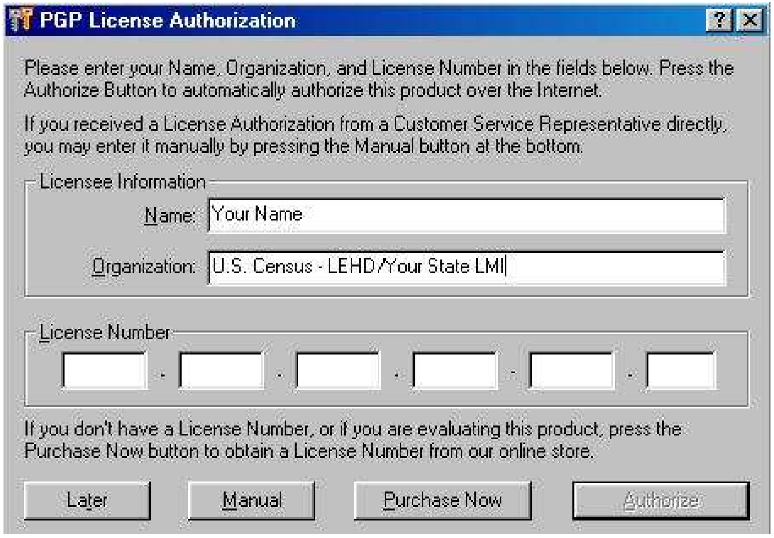
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
Today's date:
-           7-8-2003
Product Name:
-           PGP 8.0.2
Install Type:
-           As a New user to PGP, we welcome you and
            thank you for choosing our product.
Operating System:
Selected Components:
-           PGP Key Management (required)
```

Finally, you have the chance of entering your license code. If you do not have the license information handy, you will get the chance of doing so later, from within the installed program.

Figure 6: License information screen



PGP License Authorization

Please enter your Name, Organization, and License Number in the fields below. Press the Authorize Button to automatically authorize this product over the Internet.

If you received a License Authorization from a Customer Service Representative directly, you may enter it manually by pressing the Manual button at the bottom.

Licensee Information

Name: Your Name

Organization: U.S. Census - LEHD/Your State LMI

License Number

If you don't have a License Number, or if you are evaluating this product, press the Purchase Now button to obtain a License Number from our online store.

Finish the installation by rebooting your PC. After the reboot, or during the installation, you may be asked to generate your own set of keys. This is optional, but encouraged.

3.2 Installing MD5Summer (Windows)

Installing the MD5 Summer application is easy. In fact, you don't actually need to install it. You can simply run "md5summer.exe" straight from the CDROM. However, 'installing' it by copying it to a place on your hard drive will make it available without needing the CDROM.

Installation is a simple drag-and-drop of that file onto your hard drive. A good choice is your desktop.

3.3 Installation of software (Unix)

If necessary, consult your system administrator about installing "gpg", "md5sum", and any necessary FTP client.

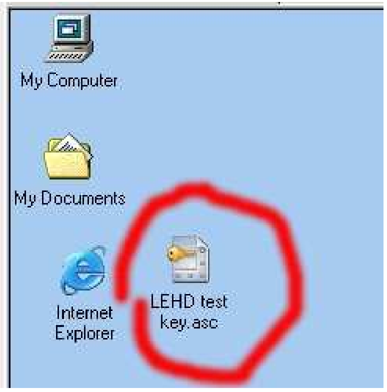
4 Importing keys

4.1 PGP (Windows)

To start using PGP, you need a key. For sending files to Census, all you will need is LEHD's public key, which you will initially receive on floppy or CDROM. After the initial key transmittal, future key exchanges can occur electronically. LEHD will generate a new public key for QWI-related transfers once a year, on June 30th.

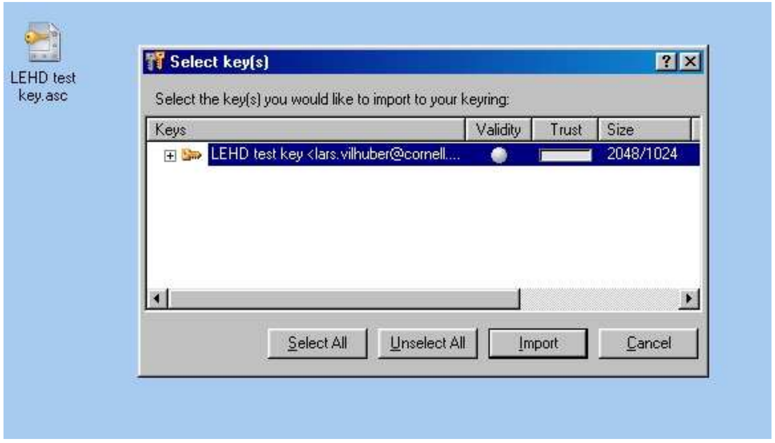
Importing keys into PGP is very easy. Find the key that you received (on floppy, CDROM, or possibly in later stages via email). In the example below, the file containing the key "LEHD Test Key" was saved to the Desktop (see Figure 7).

Figure 7: Importing a key



Double-click the file. You will see PGP Keys provide a window where you can select the keys to import (Figure 8). In this case, with only one key provided in the file, the key is already selected. Click on “Import”. The key is now available for encryption.

Figure 8: Finishing key import



Select the key(s) you would like to import to your keyring:

Keys	Validity	Trust	Size
LEHD test key <lars.vilhuber@cornell....	●		2048/1024

4.2 GPG (Unix)

Under Unix, use the syntax

```
> gpg --import lehd_2003.public.asc
```

You may have to set a trust level before you can use the key for encryption. Under Unix, issue

```
> gpg --edit-key [KEY ID] trust
```

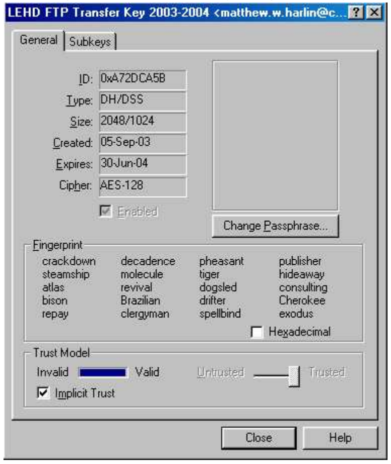
where [KEY ID] is taken from the previous listing of available keys. Follow the prompts to set the appropriate trust level.

5 Verifying keys

5.1 PGP (Windows)

To verify the properties of a key, including its Key ID and expiration date, locate the ”padlock” icon in your Windows taskbar tray, right-click, choose *PGPkeys*. In the resulting listing, right-click on the key you want information on (the standard LEHD key would be ’LEHD FTP Transfer Key 2003-2004’), choose *Key Properties* from the menu. You should see information similar to Figure 9.

Figure 9: Verifying a key



LEHD FTP Transfer Key 2003-2004 <matthew.w.harlin@c...

ID: 0xA72DCA5B
Type: DH/DSS
Size: 2048/1024
Created: 05-Sep-03
Expires: 30-Jun-04
Cipher: AES-128
☑ Enabled

Fingerprint
crackdown decadence pheasant publisher
steamship molecule tiger hideaway
atlas revival dogsled consulting
bison Brazilian drifter Cherokee
repay clergyman spellbind exodus
☐ Hexadecimal

Trust Model
Invalid Valid
☑ Implicit Trust

5.2 GPG (Unix)

You can verify which keys you have installed by issuing

```
> gpg --list-keys
```

This will also list characteristics of the keys:

```
> gpg --list-keys
/home/user/.gnupg/pubring.gpg
---------------------------------
pub  1024D/A72DCA5B 2003-09-05 LEHD FTP Transfer Key 2003-2004
sub  2048g/02DA92EC 2003-09-05 [expires: 2004-06-30]
```

6 Preparing Certification for FTP transfer by LEHD

Before actually sending production-type data to LEHD using these procedures, LEHD strongly suggests going through “certification.” Certification is initiated by transferring a small encrypted test file, rather than a file containing real data. The test file is contained on your startup CDROM which you should have received from LEHD when you signed up for FTP transfers. It is called ’testfile.txt’. The following steps outline the certification procedure:

- Follow instructions in Section 7 on the following page to generate a MD5SUM for the test file. This should give you ’testfile.md5’.
- Follow instructions in Section 8 on page 19 to encrypt the test file and its MD5SUM file. This should give you ’testfile.txt.pgp’ and ’testfile.md5.pgp’.
- Follow instructions in Section 9 on page 23 to transfer *both* files to the LEHD FTP server.
- Notify LEHD that you have initiated the Certification procedure

LEHD will verify the two files sent, and if everything worked fine, sends a ’certification’ email acknowledging that fact.

It is suggested that certification be renewed if the state uses a different source computer for the transfer (transfer of license, change of OS, etc.).

The average time spent on this procedure in the past has been about 2 hours spread across a day. We have successfully and rapidly debugged any problems on both sides related to the transfer, without needing to transfer large files.

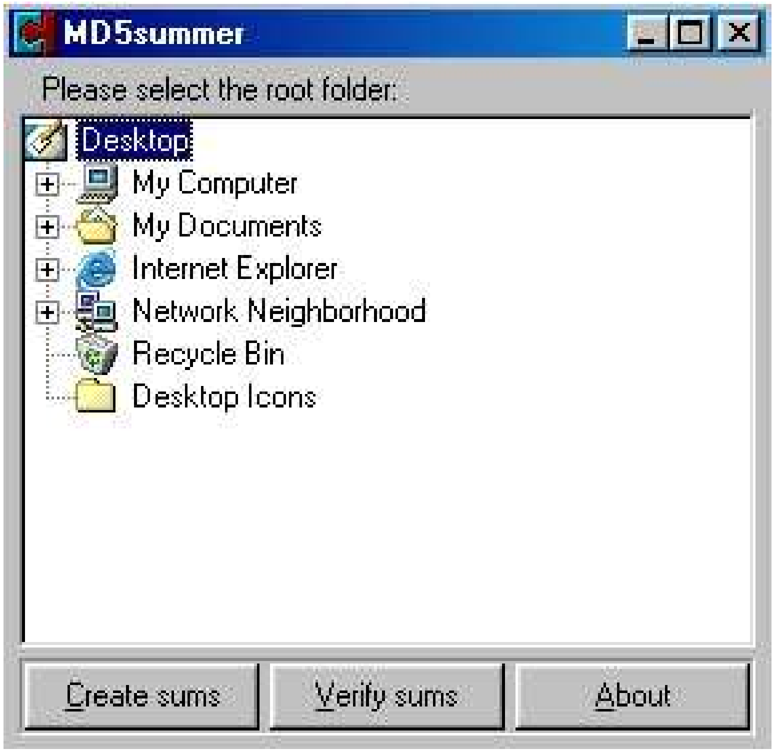
7 Generating a MD5 checksum

Errors can and do occur in both transmission and the encryption/decryption process. One way to detect such errors is to generate a checksum before encryption and transmission, to transmit that checksum to the recipient, who then uses the same procedure to compute a checksum on the received file. If the two checksums are identical, then the file was transmitted without error.

7.1 MD5Summer (Windows)

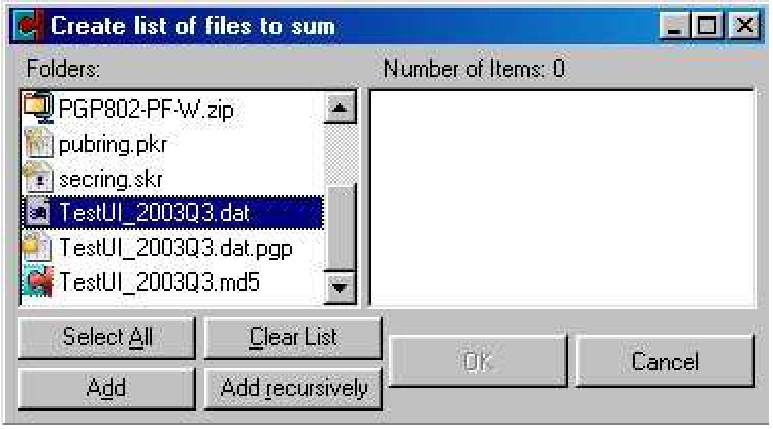
Generating a MD5 checksum is easy with “MD5 Summer”. First, find the program (see Section 3.2). Double-click it. You will see a dialog box as in Figure 10. Choose the directory containing your data file (in our case, the Desktop). Click “Create sums”.

Figure 10: Choosing directory for MD5SUM creation



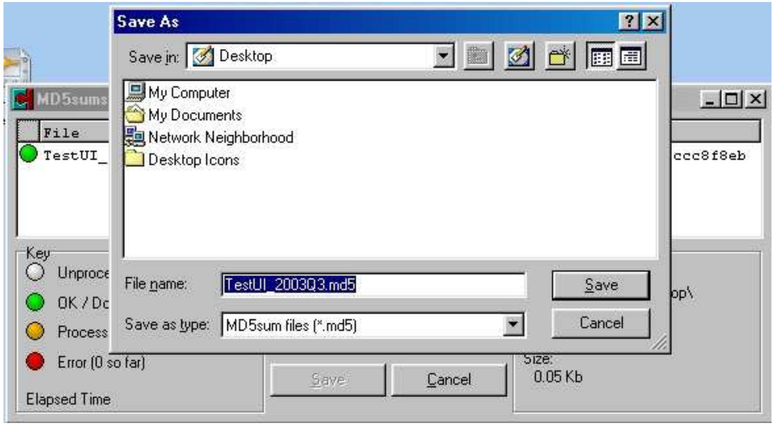
Now select in the left pane all the files for which you want to generate MD5SUMs. You can individually select files, and click on "Add", or collect files in a directory, and choose "Add recursively" after choosing that directory to add all files in that directory.

Figure 11: Selecting files for MD5SUM creation



Once you are satisfied with your selection, click OK. The program will ask you to choose a name for the file that the MD5SUMs will be saved in (Figure 12). The usual convention is to save with the same root name as the file you are checking (if a single file), followed by ".md5". The default proposal by the program is fine. Click "save".

Figure 12: Naming result file from MD5SUM creation


File name: TestUI_2003Q3.md5

Save as type: MD5sum files (*.md5)

The window that is now open shows the status of the MD5SUM generation. Click “Close”. You are finished.

7.2 MD5SUM (Unix)

Under Unix, use the syntax

```
md5sum {name of files} > {some name}.md5sum
```

8 Encrypting a file

You are now ready to encrypt a file.

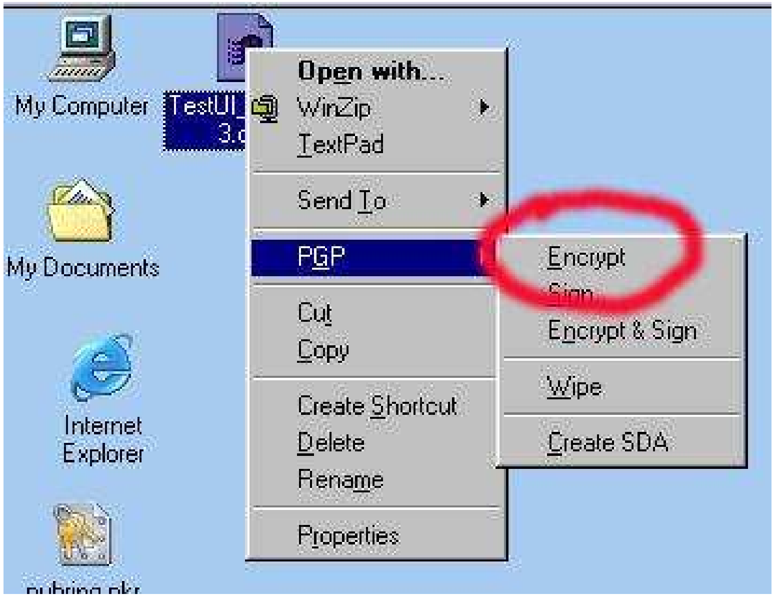
8.1 An important preface to encryption

WARNING: Before starting to encrypt the file, please be advised that ZIP files and PGP are **not** compatible. A encrypted ZIP file can only very rarely be decrypted successfully. Furthermore, zipping files is unnecessary. PGP software automatically compresses files to the same degree that PKZIP-compatible software does.

8.2 PGP (Windows)

Navigate to where you stored the file. This can be on a local drive or a network drive. In the example here, the file is on the desktop. Right-click on the file to access the PGP menu (Figure 13).

Figure 13: Right-click menu with PGP installed



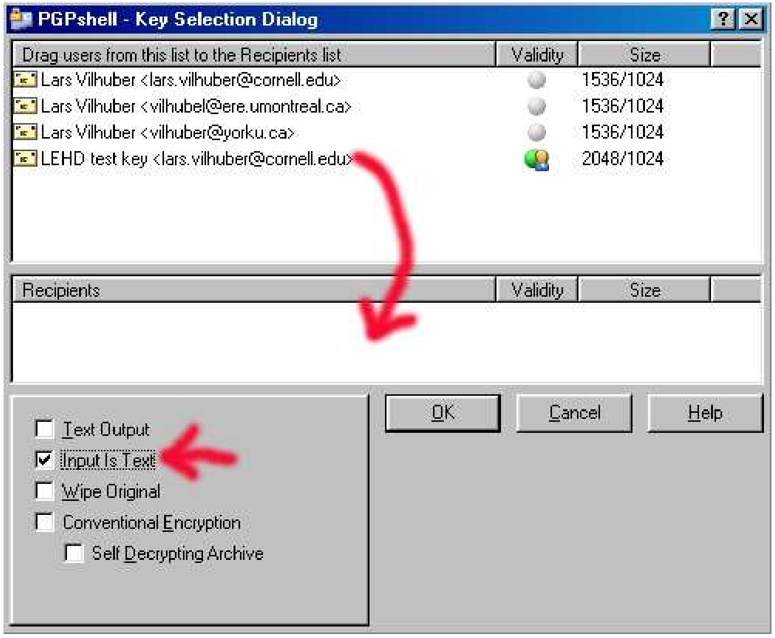
PGP will open a window containing available keys at the top, and a field to accept keys at the bottom. The file will be encrypted to all keys appearing in the bottom fields, and only to those fields. If you generated your own key at installation, it is defined as the default encryption key, and will automatically show up in the bottom field.

Drag the active LEHD key (in this case called “LEHD test key” to the bottom window. Please ensure that the box “Input is text” is checked (see Figure 14).

WARNING: It is **not** sufficient for the default key to appear in the bottom field. You **must** drag the LEHD encryption key to the bottom field.

If you have both your default encryption key and the LEHD encryption key in the lower field, both you and the LEHD can both (independently) decrypt the file. This is the best configuration.

Figure 14: Choosing keys



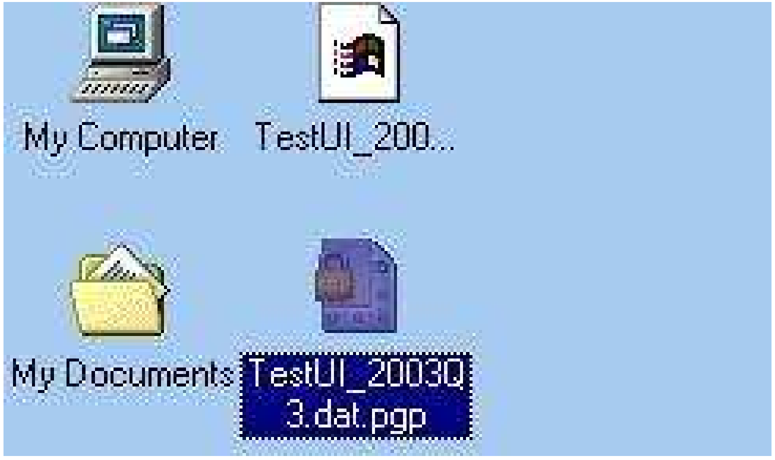
Drag users from this list to the Recipients list	Validity	Size
Lars Vilhuber <lars.vilhuber@cornell.edu>	●	1536/1024
Lars Vilhuber <vilhubel@ere.umontreal.ca>	●	1536/1024
Lars Vilhuber <vilhuber@yorku.ca>	●	1536/1024
LEHD test key <lars.vilhuber@cornell.edu>	●	2048/1024

Recipients	Validity	Size

□ Text Output
☑ Input Is Text
□ Wipe Original
□ Conventional Encryption
□ Self Decrypting Archive

Click OK. Depending on the size of the file and the vintage of your computer, this can take a while. The resulting file is saved in the same location as the original file, with an added “.pgp” extension (Figure 15). You should follow the same process with the MD5SUM file you generated earlier. Remember that all non-encrypted files will be deleted from the FTP server.

Figure 15: Resulting file



8.3 GPG (Unix)

Under Unix, use the syntax

```
gpg --recipient 02DA92EC --encrypt [filename]
```

where `02DA92EC` is the key ID for the active LEHD FTP transfer key.

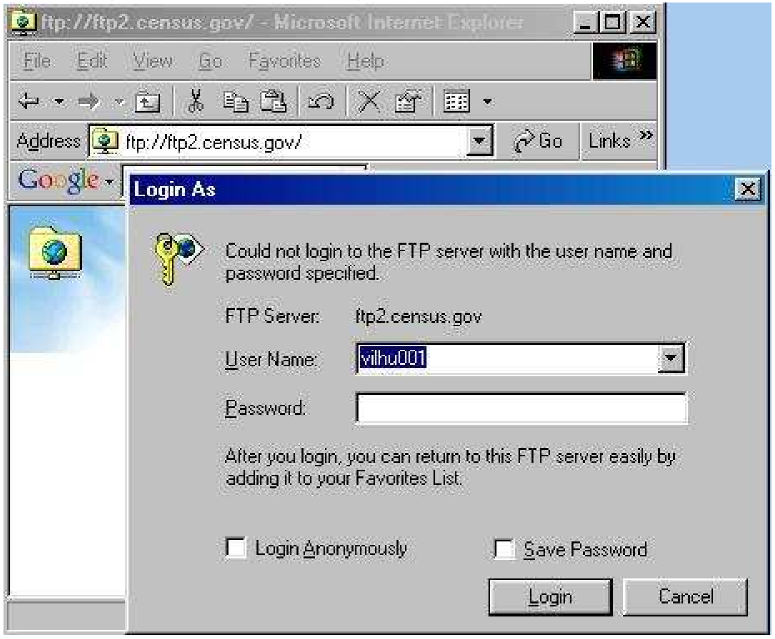
9 Transferring files to Census

9.1 Internet Explorer (Windows)

Start Internet Explorer. In the address line, type "ftp://YOURLOGIN@ftp2.census.gov" and hit Enter. The server will prompt you for a password (see Figure 16). Check that the "User Name" field contains your actual login, and enter the password you were given.

Warning: Some combinations of Windows 2000 and Internet Explorer 6 have been reported to have problems logging in. There is no known fix. Work around by using a different FTP client (see Section 2.2 on page 4).

Figure 16: Connecting to the Census FTP server



ftp://ftp2.census.gov/ - Microsoft Internet Explorer

Address: ftp://ftp2.census.gov/

Login As

Could not login to the FTP server with the user name and password specified.

FTP Server: ftp2.census.gov

User Name: vilhu001

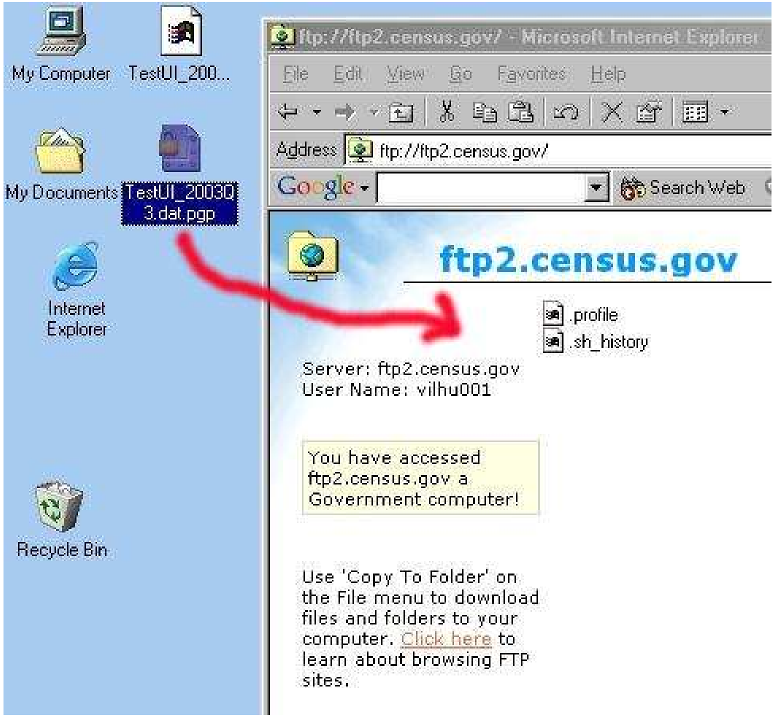
Password:

After you login, you can return to this FTP server easily by adding it to your Favorites List.

□ Login Anonymously □ Save Password

Now drag-and-drop the encrypted file(s) onto the Internet Explorer window . If you generated a MD5SUM file, do not forget to transfer that as well. The file(s) will be copied to the FTP server. This process might take a while, depending on the size of your file and the speed of your connection to the internet.

Figure 17: Ready to transfer



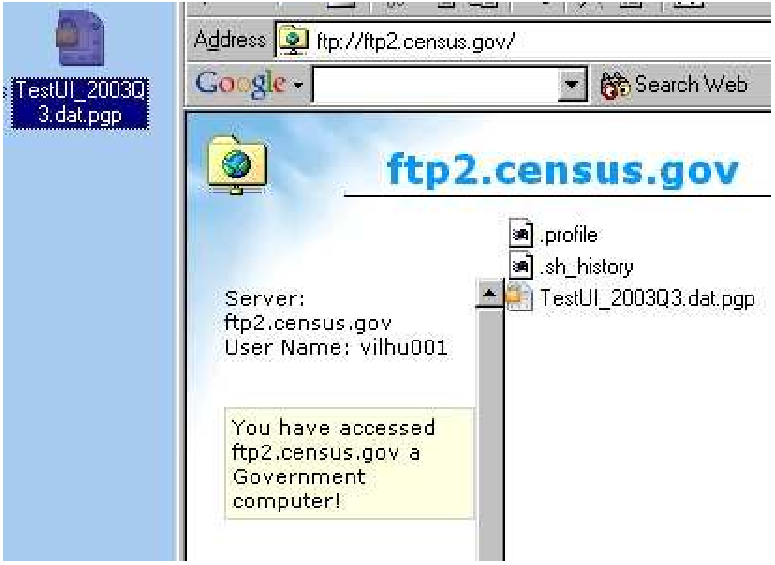
Server: ftp2.census.gov
User Name: vilhu001

You have accessed ftp2.census.gov a Government computer!

Use 'Copy To Folder' on the File menu to download files and folders to your computer. Click here to learn about browsing FTP sites.

When the transfer is successful, you should see the file appear in the Internet Explorer window. If you see any error messages, try the transfer again later.

Figure 18: Successful transfer



Server: ftp2.census.gov
User Name: vilhu001

You have accessed ftp2.census.gov a Government computer!

9.2 FTP client (Unix)

There are many Unix clients. A good choice is `ncftpput`, which allows for unmonitored transfers. A sample syntax is

```
ncftpput -f login.cfg . {name of PGP files}
```

(note the dot after `login.cfg`) where the file `login.cfg` should contains

```
host ftp2.census.gov
user myusername
pass mypassword
```

and should be protected from read-access by unauthorized persons.

10 Batch processing (Unix only)

This pulls together all the Unix commands, into one sequence of commands. This could be stored as file that gets executed every time a transfer is to occur

```
files="file1.txt file2.txt"
keyid=A72DCA5B
transferid=STATE.$(date +%Y%m%d)
for arg in $files
do
 gpg --recipient $keyid --encrypt $arg
 gpgfiles="$gpgfiles ${arg}.gpg"
done
md5sum $files > ${transferid}.md5sum
ncftpput -f login.cfg . ${gpgfiles} ${transferid}.md5sum
```

11 Contacts

LEHD Website http://lehd.dsd.census.gov

Technical contact Lars Vilhuber (lars.vilhuber@census.gov)