**Tools**

*These links are for your use only, as sources of images used below if they are not high quality enough in this doc.*

1. Adium tool guide [– Link](https://ssd.eff.org/en/module/how-use-otr-mac)
2. Basic Security Setup for Android - [Link](https://securityinabox.org/android_basic)
3. ChatSecure tool guide - [Link](https://ssd.eff.org/en/module/how-install-and-use-chatsecure)
4. Cobian Backup Guide - [Link](https://securityinabox.org/cobian_main)
5. How to change your Facebook privacy settings - [Link](https://www.eff.org/deeplinks/2013/01/how-protect-your-privacy-facebooks-graph-search)
6. How to opt-out of Facebook's data broker relationships – [Link](https://www.eff.org/deeplinks/2013/02/howto-opt-out-databrokers-showing-your-targeted-advertisements-facebook)
7. How to opt-out of Twitter's data broker relationships – [Link](https://www.eff.org/deeplinks/2013/07/how-opt-out-twitters-tailored-advertisements-and-more)
8. Jitsi Tool guide – [Link](https://securityinabox.org/jitsi)
9. K9 & APG tool guide – [Link](https://securityinabox.org/k9_apg_main)
10. KeePassX tool guide – [Link](https://www.keepassx.org/screenshots/)
11. ObscuraCam Tool guide – [Link](https://securityinabox.org/obscuracam_main)
12. Orbot & Orweb tool guide – [Link](https://securityinabox.org/Orbot_main), [Link](https://securityinabox.org/orweb_main)
13. PGP for Linux tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-linux)
14. PGP for Mac O SX tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-mac-os-x)
15. PGP for Windows tool guide – [Link](https://ssd.eff.org/en/module/how-use-pgp-windows-pc)
16. Pidgin tool guide – [Link](https://ssd.eff.org/en/module/how-use-otr-windows)
17. Psiphon3 tool guide – [Link](https://www.level-up.cc/leading-trainings/training-curriculum/deepening/psiphon3)
18. Recuva – File Recovery Guide – [Link](https://securityinabox.org/recuva_main)
19. Redphone Tool guide – [Link](https://ssd.eff.org/en/module/how-use-redphone-android)
20. Signal Tool guide – [Link](https://ssd.eff.org/en/module/how-use-signal-%E2%80%93-private-messenger)
21. TextSecure tool guide – [Link](https://ssd.eff.org/en/module/how-use-textsecure-android)
22. Tor for Mac tool guide – [Link](https://www.torproject.org/projects/torbrowser.html.en#macosx)
23. Tor for Windows tool guide – [Link](https://ssd.eff.org/en/module/how-use-tor-windows#overlay=en/node/57/)
24. TrueCrypt Tool Guide – [Link](https://securityinabox.org/truecrypt_main)

**RECUVA TOOL GUIDE**

# ****Recuva**** Tool Guide

# Data recovery and secure deletion

**Lesson to read:**

* **Backing Up**

**Download Location:** <http://www.piriform.com/recuva/builds>

**Computer requirements:** Any version of Windows

**Version used in this guide:** Recuva 1.3

**License:** Freeware

**Level:**Intermediate

**Time required:** 20 minutes

**Using Recuva will give you**:

* The ability to perform different scanning techniques
* The ability to recover previously deleted files on your computer, including emails, images and videos
* The ability to securely delete private or sensitive information

**Mac OS** users could use [**TestDisk** and **PhotoRec**](http://www.cgsecurity.org/), as an alternative, which are also compatible with **Microsoft Windows**and **GNU Linux**.

### 1.1 Before you start

In situations where private or sensitive files may have been mistakenly deleted, Recuva can help you to scan for and restore some of them. As discussed in the **Deleting lesson**, a file deleted using the standard Windows operating system Delete function, even after the Recycle Bin has been emptied, might still exist on the computer.

However, there are circumstances under which Recuva cannot retrieve information. If you have permanently deleted or wiped any temporary files by running CCleaner with the Secure file deletion (Slower) option enabled, those files are virtually unrecoverable. Recuva cannot recover files after programs like CCleaner or Eraser have been used to wipe free disk space or if Windows itself has already overwritten any previously occupied space. Recuva also cannot recover damaged documents and files.

Recuva can also be used to securely overwrite your private or sensitive data.

# How to Install Recuva

### 2.0 How to Install Recuva

**Step 1**. **Double click**“rcsetup138.exe”; the Open File - Security Warning dialog box may appear. If it does, **click**“Run” to activate the language box.

**Step 2**. **Click**“OK”to activate the Welcome to the Recuva Setup Wizard screen.

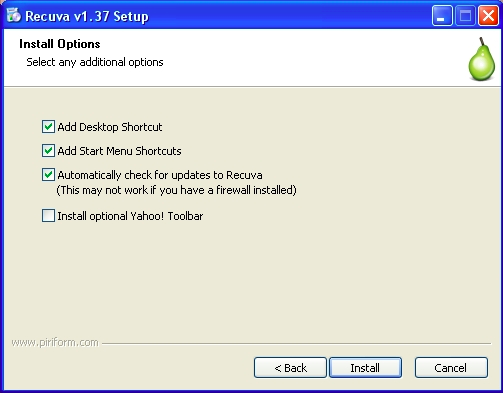
**Step 3**. **Click “**Next**”** to activate the License Agreement screen. Please read the License Agreement before proceeding with the rest of the installation process.

**Step 4**. **Click**“I Agree” to activate the Choose Install Location screen.

**Step 5**. **Click**“Next” to activate the Install Options screen.

**Note**: The Install Options screen appears with the Install optional Yahoo! toolbar option enabled. Do not install the **Yahoo!** toolbar, which may compromise your Internet privacy and security.

**Step 6**. **Check**the Install optional Yahoo! toolbar check box to disable it as shown below:



**Step 7**. **Click “**Install**”** to begin installing **Recuva**. This will activate the installation progress bar that will disappear after the installation has completed itself in a few minutes.

**Step 8**. **Click “**Finish**”** to complete installing **Recuva**.

Now that you have successfully installed **Recuva**, you are ready to begin recovering and/or overwriting private and sensitive information.

# How to Perform Different Scans Using Recuva

### 3.0 Before You Begin

In this section, you will learn how to perform different types of scans, and be introduced to the General and Actions tabs in the Options screen. **Note**: A scan will simply retrieve and display the files which are potentially recoverable. The actual recovery procedures are discussed in the next section.

### 3.1 How to Perform a Scan Using the Recuva Wizard

The **Recuva**Wizard is recommended in situations where neither the full nor partial name of the file you would like to recover is known. It is also recommended if this is the first time you are using **Recuva**. The **Recuva**Wizard lets you set the scan parameters by letting you specify the file type and/or from where the file was deleted.

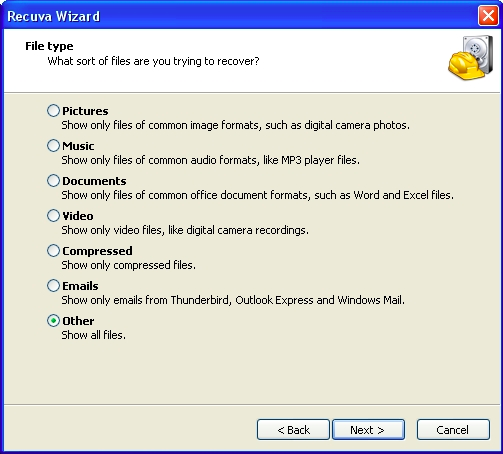
To begin scanning for deleted files, perform the following steps:

**Step 1**. **Click**the Recuva icon or **select Start > Programs > Recuva > Recuva**to launch the program, and activate the following screen:



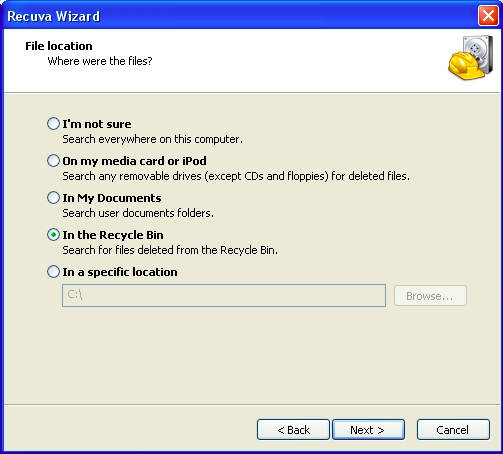
**Tip**: If you know the exact or even partial name of a file you would like to recover, **click**“Cancel” to go to the Piriform Recuva main user interface, and then follow the steps in section **3.2 How to Perform a Scan without Using the Recuva Wizard.**

**Step 2**. **Click**“Next” to activate the following screen:



The Recuva Wizard File type displays a list of different file types, and describes what files might be recovered when each option is enabled.

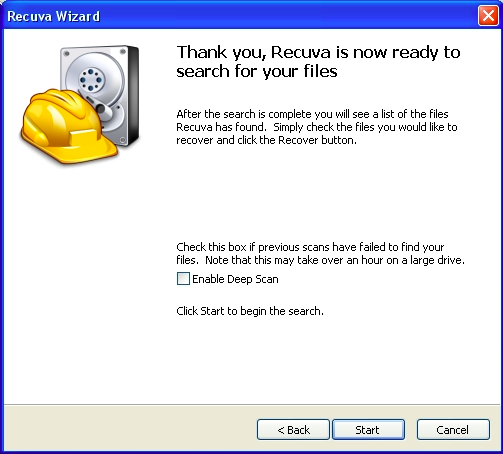
**Step 3**. **Check**the Other option, and then **click**“Next” to activate the following screen:



**Note**: The default setting for the Recuva Wizard File Location screen is the I'm not sure option. This option will extend the scan to all drives as well as removable media, except CDs, DVDs and optical media. It may, therefore, require a longer time to generate results.

Files are most frequently deleted from Recycle Bin in the **Windows**operating systems, to minimize the chance of your accidentally deleting private or sensitive information.

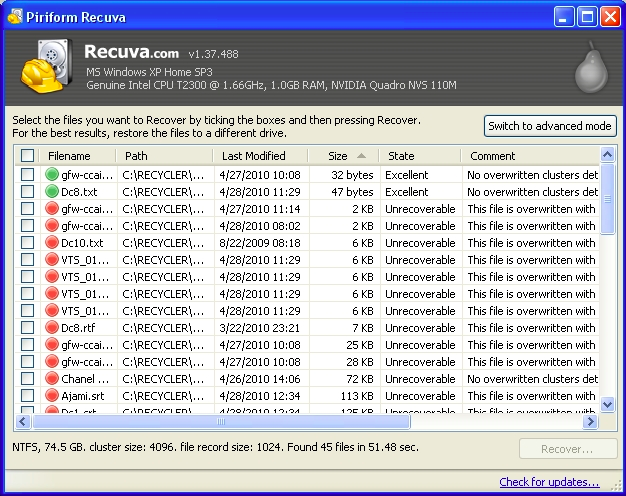
**Step 4**. **Check**the In the Recycle Bin option as shown above, and then **click**“Next” to activate the following screen:



**Note**: For this exercise, do not enable the Deep Scan option. This scanning technique will be discussed in section **3.3 How to Perform a Deep Scan**.

**Step 5**. **Click “**Start**”** to begin recovering your deleted files.

During the file recovery process, two progress status bars appear in quick succession. The Scanning the drive for deleted files progress bar lists the deleted files. The Analyzing the file contents progress bar groups and sorts the deleted files into file types and degree of recoverability. They also display the duration of the scanning and analysis processes. Your Piriform Recuva main user interface may then resemble the following screen:



The Piriform Recuva main user interface lists information about each deleted file, arranged in six columns. Each column is described as follows:

**Filename**: This displays the name and file extension of the deleted file. **Click**the Filename title to arrange the deleted files in alphabetical order.

**Path**: This displays where the deleted file was found. Given that the In the Recycle Bin option was enabled in this example, the file path is C:RECYCLER for all the deleted files. **Click**the Path title to view all the files listed under a particular directory or file path.

**Last modified**: This displays the last time the file was modified before it was deleted, and can be useful in helping to identify the file you would like to recover. **Click**Last modified to list the deleted files according to the oldest or most recent.

**Size**: This displays the size of the file. **Click**Size to list the deleted files beginning with the largest or smallest deleted file.

**Status**: This displays the extent to which the file is recoverable, and corresponds to the file status icons discussed below. **Click**Status to sort the deleted files into the three basic categories, and list them from Excellent to Unrecoverable.

**Comment**: This displays why a given file may or may not be recoverable, and the extent to which a deleted file has been overwritten in the **Windows Master File Table. Click** Comment to view the extent to which a file or group of files have been overwritten.

Each file is associated with a coloured status icon which indicates the extent to which each file can be successfully recovered:

The following list describes each status icon:

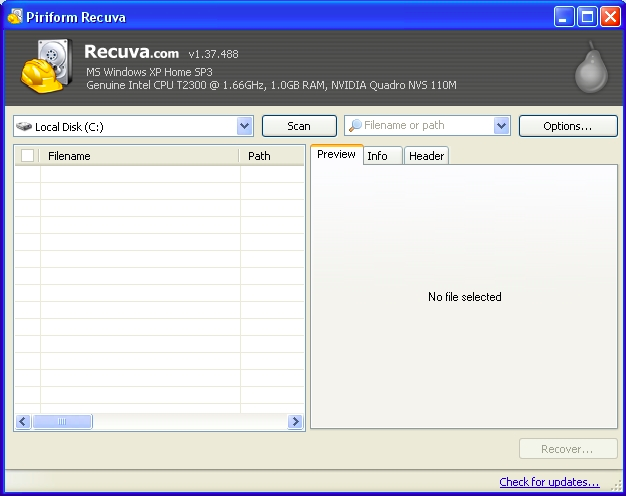
* **Green**: The chances for a full recovery are excellent.
* **Orange**: The chances for recovery are acceptable.
* **Red**: The chances for recovery are unlikely.

### 3.2 How to Perform a Scan without Using the Recuva Wizard

To access the **Recuva**main user interface directly, (that is, not use the Recuva Wizard), perform the following steps:

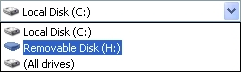
**Step 1**. **Click**the Recuva icon or **select Start > Programs > Recuva > Recuva**.

**Step 2**. **Check**the Do not show this Wizard on startup option, then **click**“Cancel” to activate the following screen:

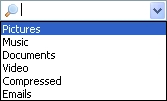


The Piriform Recuva main user interface is divided into the results pane on the left and the Preview, Info and Header tabs in which to sort and view information about a specific deleted file. It lets you set certain scan options, similar to those in the Recuva Wizard.

**Step 3**. **Click**to activate the drop-down list and **select**the drive to be scanned; the Local Disk (C:) is the default and used in this example as follows:



The Filename or path drop-down list lets you specify the kind of file you are looking for, and loosely corresponds to the Recuva Wizard File type screen.



The Filename or path feature is a combination of a text box and drop-down list. It has two main uses: To let you directly search for a specific file, and/or to sort through a list of deleted files, according to file type.

Alternatively, the Filename or path feature can be used to search for files of a specific type, or to sort through a general list of deleted files in the results pane.

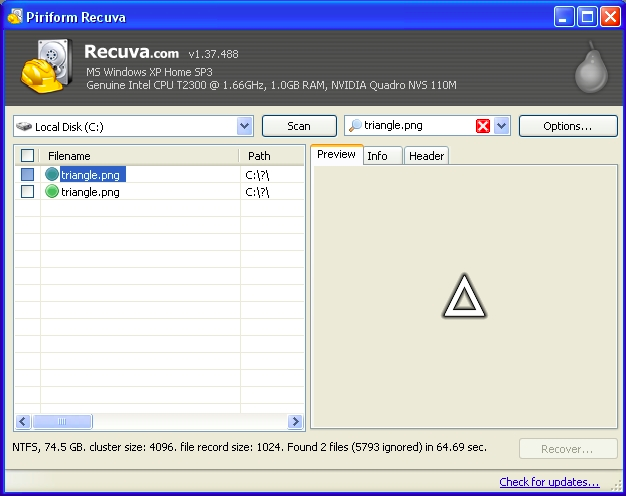
To begin scanning for a file of which all or part of the name is known, perform the following steps:

**Step 1**. **Type**in the name or partial name of a file you would like to recover as follows (in this example, the file triangle.png is being scanned):



**Tip**: **Click**X to reset the File name and path (which appear greyed out).

**Step 2**. **Click “**Scan**”** to begin scanning for your deleted file(s); shortly thereafter, a screen will appear resembling the following:

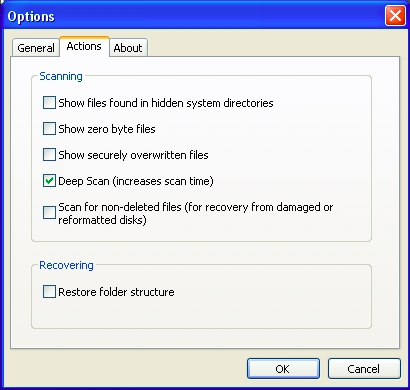


#### 3.3 How to Perform a Deep Scan Using Recuva

The Enable Deep Scan option lets you conduct a more thorough scan; naturally, a deep scan takes a longer time, depending on your computer speed and the number of files you have. This option might prove useful if your initial scan does not display the files you would have liked to recover. Although a deep scan may even take hours depending on the amount of data stored on your computer, it may improve your chances of recovering the files you require.

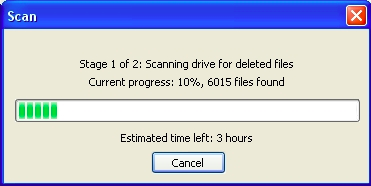
The **Recuva**Deep Scan option can be enabled either through **checking**the Enable Deep Scan option in the Recuva Wizard.

**Step 1**. **Click**“Options” to activate the Options screen, then **click**the Actions tab as follows:



**Step 2**. **Check**the Deep Scan (increases scan time) option, then **click “**OK**”**.

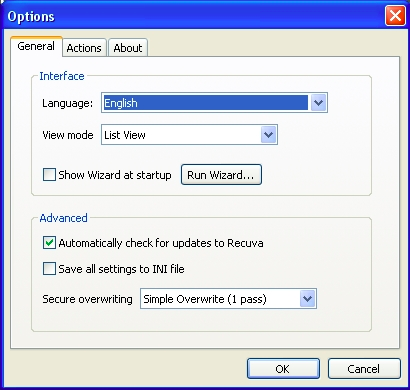
**Step 3**. **Click**“Scan” to begin scanning for deleted files using the Deep Scan option. As mentioned earlier, a deep scan can potentially take a few hours, depending on the size of your hard disk and computer speed:



### 3.4 An Introduction to the Options Screen

In this section, you will learn how to use the different settings to successfully recover and overwrite your private or sensitive information in the Options screen. To configure these settings, perform the following steps:

**Step 1**: **Click**“Options” to activate the following screen:



The Options screen is divided into the General, Actions and About tabs.

The General tab lets you define a number of important settings, including Language (**Recuva**supports 37 languages), View mode and disabling or enabling the Recuva Wizard.



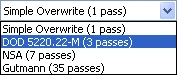
The **View Mode**lets you select how you would like to view the deleted files, and can also be enabled whenever you **right click**a file in the Piriform Recuva.

* **List**: This option lets you view the deleted files in a list
* **Tree**: This option lets you view the directory path of deleted files in the form of an expandable tree.
* **Thumbnails**: This option lets you view the deleted files as graphics or images where possible.

Most importantly perhaps, the Advanced section of the General tab lets you set the number of times your data can be overwritten by random data to protect it from recovery by hostile or malicious parties.

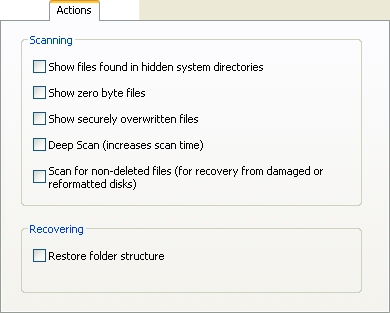
The Secure overwriting drop-down list displays four options for overwriting your private information. Its default mode is Simple Overwrite (1 pass). A pass refers to the number of times your document, file or folder will be overwritten with random data to render it completely unreadable.

**Step 2**: **Select** the DOD 5220.22-M (3 passes) option as follows:



A single pass may prove quite effective in overwriting a given document, file or folder; however, there are parties with the resources and skills to recover a relatively light secure overwrite. Three passes is a solid balance between the time required to perform a secure overwrite, and the ability to recover that document, file or folder.

**Step 3**. **Click**“OK” to save your General tab configuration options.



* **Show files found in hidden system directories**: This option lets you display files in hidden system directories.
* **Show zero-byte files**: This option lets you show you files that have little to no content, and which are basically irrecoverable.
* **Show securely deleted files**: This option lets you display files that have been securely deleted in the results pane.

**Note**: If you have already used **CCleaner** or a similar program, it changes the filename to ZZZZZZZ.ZZZ when it securely deletes a file, for security reasons.

* **Deep Scan**: This option lets you scan the entire drive for the deleted document or file; if previous scans have proven ineffective in locating your file, the Deep Scan may prove useful. However, it does require more time. Please refer to section **3.3 How to Perform a Deep Scan Using Recuva.**
* **Scan for non-deleted files (for recovery from damaged or reformatted disks)**: This option lets you attempt to recover files from disks that may have sustained physical damage or software-related corruption.

The About tab displays version information, as well as links to the Piriform web site.

Now that you are more confident about performing different scans and familiar with the settings in the General and Actions tabs in the Options screen, you are ready to learn how to actually recover and/or securely overwrite your private or sensitive information.

# How to Recover and Securely Overwrite Files Using Recuva

### 4.0 Before You Begin

In this section, you will learn how to recover a previously deleted file, as well as how to securely overwrite any private or sensitive information.

**Recuva**lets you create a new folder for storing your recovered files. Although **Recuva**does let you use existing folders, for reasons of safety and security, we recommend that you copy your recovered files to a removable device like a backup drive or USB memory stick.

**Important**: Although **Recuva**does an excellent job of securely overwriting information, it may leave a file marker indicating the existence of such a file. To protect your privacy and security, it makes sense to save any important, private or sensitive information to a removable device, and not to the original location or path.

### 4.1 How to Recover a Deleted File

To begin recovering a deleted file, perform the following steps:

**Step 1**. **Connect**your removable disk or a USB memory stick to your computer.

**Step 2**. **Check**the check box next to a file you want to recover to enable the Recover... button or **double click**that file to both check and highlight that file.

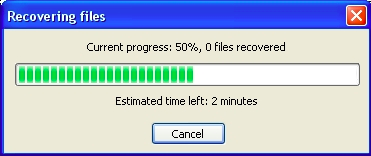
**Step 3**. **Click “**Recover…” to activate the Browse For Folder screen.

**Step 4**. **Select**a destination and then **click**“Make New Folder” to create your recovery folder as shown below.

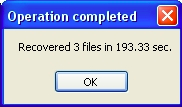


**Note**: In this example, the folder for storing your recovered documents and files has been given an obvious label. However, keeping your digital privacy and security in mind, we encourage you to be more careful in labelling your own folder.

**Step 5**. **Click**“Yes” to begin the file recovery process; a progress status screen appears as follows:



After the files have been recovered, a confirmation will appear resembling the following screen:



**Note**: **Recuva**supports multiple file recovery. Simply check the check boxes of the files you would like to recover and perform **steps 3** to **5**.

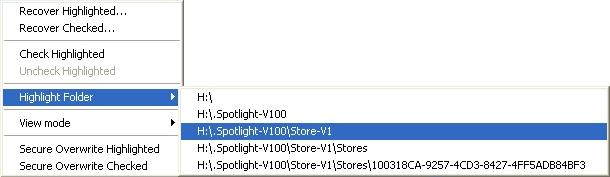
Now that you are comfortable with recovering a previously deleted file, you are ready to learn how to use the pop-up menu to perform multiple file recoveries and secure overwriting of files.

### 4.2 How to Use the Pop-up Menu

**Recuva**offers different options for selecting the documents, files or folders you would like to delete or securely overwrite.

* **Checking** is generally used to quickly select several non-contiguous or separate files for recovery or secure overwriting.
* **Highlighting** is generally used to quickly select contiguous multiple files in a block or group for recovery or secure overwriting.

**Right click**on a deleted file displayed in the **Recuva**main to activate the following pop-up menu:



**Recover Highlighted**: This item lets you recover all or any highlighted deleted file(s).

**Recover Checked**: This item lets you recover a checked deleted file.

**Check Highlighted**: This item lets you check a highlighted deleted file.

**Uncheck Highlighted**: This item lets you uncheck a highlighted deleted file.

As you recall, the **View Mode**can also be set in the General tab in the Options screen. This item lets you select how you would like to view the deleted files.

* **List**: This option lets you view the deleted files in a list as in Figure 5
* **Tree**: This option lets you view the directory path of deleted files in the form of an expandable tree.
* **Thumbnails**: This option lets you view the deleted files as graphics or images where possible.

**Highlight Folder**: This option lets you select multiple deleted files according to their directory path, and lets you perform the actions listed in the pop-up menu on them.

**Secure Overwrite Highlighted**: This option lets you securely overwrite a highlighted deleted file.

**Secure Overwrite Checked**: This option lets you securely overwrite a checked deleted file, changing its status icon to red.

### 4.3 How to Securely Overwrite a Deleted File

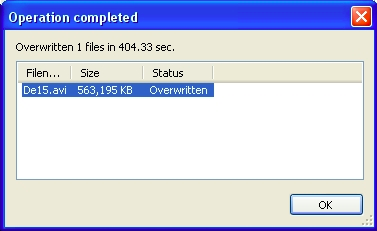
To securely overwrite a deleted file, perform the following steps:

**Step 1**. **Check**the individual file you would like to have securely overwritten, and then right click the check box it to activate the pop-up menu.

**Step 2**. **Select**“Secure Overwrite Checked” to activate the following confirmation dialog box:



**Step 3**. **Click**“Yes” to begin the overwriting process; depending on the size and status of the file as well as the Secure overwriting option you selected in the General tab in the Options screen, this could take some time. After the overwriting process has been completed, a screen resembling the following appears:



You have successfully completed recovering and securely overwriting files using **Recuva**previously deleted files.

# 5 PORTABLE RECUVA



## 5.1 Differences between the Installed and Portable Versions of Recuva

Given that portable tools are not installed on a local computer, their existence and use may remain undetected. However, keep in mind that your external device or USB memory stick, and portable tools are only as safe as the computer you are using, and may risk being exposed to adware, malware, spyware and viruses.

There are no other differences between **Portable Recuva**and the version designed to be installed.

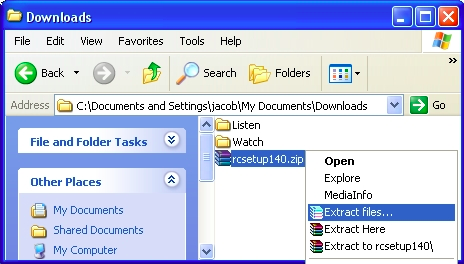
## 5.2 How to Download and Extract Recuva Portable

To begin downloading and extracting **Recuva Portable**, perform the following steps:

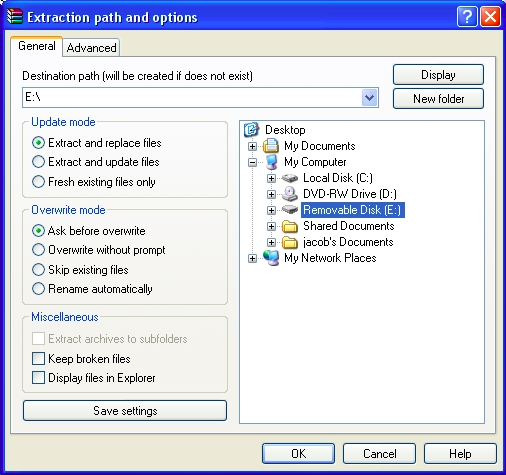
**Step 1**. **Click**[**http://www.piriform.com/recuva/download/portable**](http://www.piriform.com/recuva/download/portable) to be directed to the appropriate download site, and automatically activate the following screen:

**Step 2**. **Click “**OK**”** to save the *rcsetup140.zip*installation file to your computer; and then **navigate**to it.

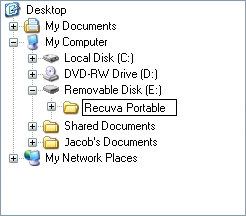
**Step 3**. **Right click**to activate the **Windows**pop-up menu, and then **select**the Extract files... item as shown below:



**Step 4**. **Navigate**to the removable drive or USB memory stick as shown below, and then **click**“New Folder” to create a new folder in which to extract the installation file.



**Step 5**. **Enter**a name for the new folder in the document tree as shown below:



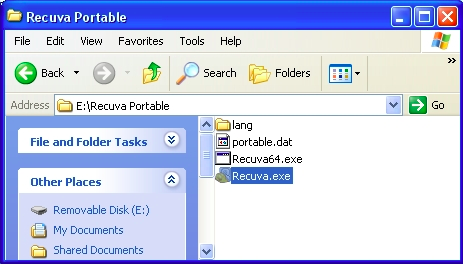
Alternatively, you may type in a folder name in the accompanying drop-down list:



**Note**: Although for the purposes of this example, the new folder is entitled Recuva Portable, users may choose different name.

**Step 6**. **Click**“OK” to begin extracting its contents to newly created folder.

**Step 7**. **Navigate**to your destination external drive or USB memory stick, as shown below, then **open**it to confirm that the **Portable Recuva**program was successfully extracted.



**Step 8**. **Double click***Recuva.exe*to activate the **Portable Recuva**wizard.

Please refer to the rest of the Recuva tool guide above to begin configuring and using it.

**REDPHONE TOOL GUIDE**

# ****RedPhone**** Tool Guide

# Encrypted phone calls for Android

**Lesson to read:**

* **Making a Call**

**Download Location:** <https://whispersystems.org/>; can also be downloaded from the [Google Play store](https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone" \t "_blank)

**Computer requirements:** Android 2.2 and up

**Version used in this guide:** RedPhone 0.9.6

**License:** Free Open-Source Software; GPLv3

**Level:**Beginner-Intermediate

**Other reading**: <http://support.whispersystems.org/>

**Time required:** 15 minutes

**Using RedPhone will give you**:

* The ability to make encrypted voice calls over a Wi-Fi or data connection using your normal phone number

NOTE: RedPhone only encrypts calls that are between two RedPhone users, or between users of RedPhone and Signal, the app for iPhones. (See **Signal Tool Guide** for instructions for iPhones)

## 1.0 How to install RedPhone

### Step 1: Download and install RedPhone

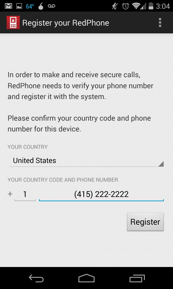
On your Android phone, enter the Google Play store and search for “RedPhone.” Select the app, “RedPhone :: Secure Calls.”

Select “Install” and accept the Terms of Service by selecting “Accept.” The app will download and install automatically.



### Step 2: Register your mobile

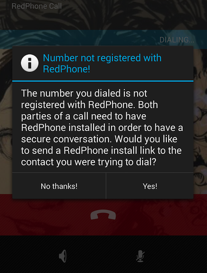
Once you have installed the app, open it; you will automatically be prompted to register your mobile number.



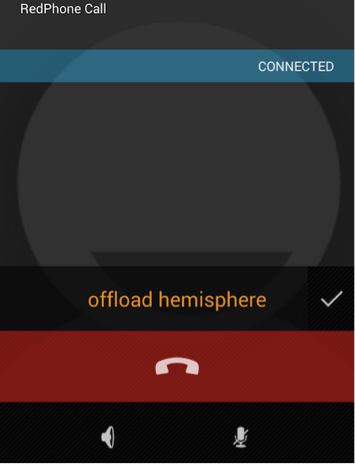
Once you have registered your mobile number, RedPhone will send you an SMS code to verify that the number belongs to you. Type in the code when prompted by the app. You have now successfully installed RedPhone and are ready to make encrypted calls!

## 2.0 Using RedPhone

In order to use RedPhone, the person that you are calling must also have RedPhone (or Signal) installed. If you try to call someone using the RedPhone app and they do not have it installed, the app will ask if you would like to invite them to use RedPhone via SMS, but it will not allow you to complete your call from inside the app.



When you make a call to another RedPhone or Signal user (from either your default system dialer or from inside the app), you will be given a random pair of words. This word pair will allow you to verify your identity and keys with the other user—also known as key verification.



The trustworthiest way to verify the identity of a caller is to use out-of-band authentication to verify the word pair. You can also read the words aloud if you recognize the caller’s voice, although very sophisticated attackers might be able to defeat this if they needed to. The word pair must be identical.

**SIGNAL TOOL GUIDE**

# ****Signal**** Tool Guide

# Encrypted phone calls for iPhones

**Lesson to read:**

* **Making a Call**

**Download Location:** The app can be downloaded from the [Apple App Store](https://itunes.apple.com/us/app/signal-private-messenger/id874139669?mt=8)

**Computer requirements:** Requires iOS 7.0 or later. Compatible with iPhone, iPad, and iPod touch.

**Version used in this guide:** Signal – Private Messenger 1.0.5

**License:** GPLv3

**Level:**Beginner-Intermediate

**Other reading**:

* <https://whispersystems.org/blog/signal/>
* <http://support.whispersystems.org/>

**Time required:** 15-20 minutes

**Using Signal will give you**:

* The ability to make encrypted voice calls over a Wi-Fi or data connection using your normal phone number

NOTE:

* Although it uses telephone numbers as contacts, calls actually use your data connection; therefore both parties to the conversation must have Internet access on their mobile devices.
* Signal only encrypts calls that are between two Signal users, or between users of Signal and RedPhone, the app for Androids. (See **RedPhone Tool Guide** for instructions for Androids)

## 1.0 How to install Signal

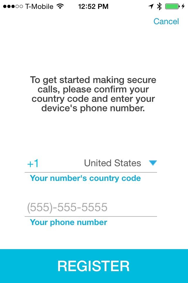
**Step 1**: Download and Install Signal – Private Messenger

On your iOS device, enter the App Store and search for “Signal.” Select the app “Signal – Private Messenger” by Open Whisper Systems.

Click to download the app and accept the iTunes Store Terms & Conditions by selecting “Accept.” The app will download and install automatically. Click “Open” to launch the app.

**Step 2:** Register and Verify your Phone Number

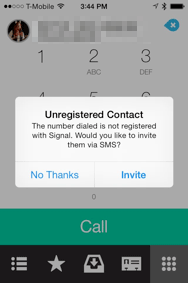
You will see a screen that looks like this:



Enter your mobile phone number and click “Register.” In order to verify your phone number, you will be sent an SMS text with a six-digit code; enter the code in the space provided. If you are unable to receive SMS texts, you have the option of receiving a phone call to verify your phone number. Click “Verify.”

**2.0 Using Signal**

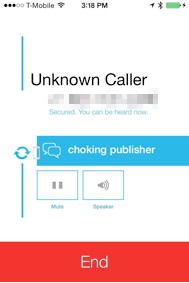
In order to use Signal, the person that you are calling must have either Signal or RedPhone (for Android devices) installed. If you try to call someone using the Signal app and they do not have Signal or RedPhone installed, the app will ask if you would like to invite them via SMS, but it will not allow you to complete your call from inside the app.



**2.1 How to Initiate an encrypted call**

To initiate an encrypted call to a contact, you must use the dialer within the Signal app. (This differs from RedPhone for Android, which also allows you to use the default system dialer.)

Once a call is established, both parties to the call will be shown a random pair of words. This word pair will allow you to verify your identity and keys with the other user—also known as key verification.



The most trustworthy way to verify the identity of a caller is to use out-of-band authentication to verify the word pair. You can also read the words aloud if you recognize the caller’s voice, although very sophisticated attackers might be able to defeat this if they needed to. The word pair must be identical.

**TEXTSECURE TOOL GUIDE**

# ****TextSecure**** Tool Guide

# Secure messaging for Android

**Lesson to read:**

* **Sending a message**

**Download Location:** TextSecure can be downloaded from [Open WhisperSystems](https://whispersystems.org/" \t "_blank); and can also be downloaded from the [Google Play store](https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms)

**Computer requirements:** Android 2.3 and up

**Version used in this guide:**  TextSecure 2.1.7

**License:** GPLv3

**Level:**Beginner - Intermediate

**Other reading**:

* <https://github.com/WhisperSystems/TextSecure/wiki/Using-TextSecure>
* <https://securityinabox.org/en/textsecure_main>
* <http://support.whispersystems.org/>

**Time required:** 15 minutes

**Using TextSecure will give you**:

* The ability to send confidential messages with your mobile phone using end-to-end encryption

**1.0 Before you start**

NOTE: TextSecure works over a Wi-Fi or data connection. While the current version can also be used to send SMS if such a connection is unavailable, **this function will shortly be removed due to security concerns and future versions will work over the internet only**.

Messages in blue are sent over a data connection, while those in green have been sent over SMS.

TextSecure can also currently be used to send SMS to non-TextSecure users, however, those messages will not be encrypted in transit. Encrypted text messages are marked with a small lock.

Both sides have to be using TextSecure for the messages to be secure while they travel over the Internet.

You can set up a passphrase that will encrypt these conversations when they are stored on your local phone. This means that they are better protected against being read if your phone is seized or compromised.

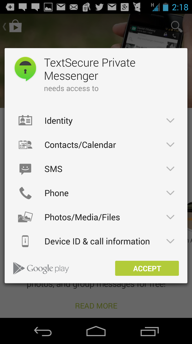
## TextSecure is available in more than 30 languages. You can change the language of the app by selecting “Settings” then “Language.”

## 2.0 How to install TextSecure

### Step 1: Download and install TextSecure

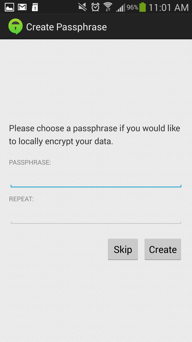
On your Android phone, enter the Google Play store and search for “TextSecure.” Select the app, “TextSecure Private Messenger.”

Select “Install” and accept the Terms of Service by selecting “Accept.” The app will download and install automatically.



### Step 2: Create a passphrase to encrypt data locally

Open the app. You will be prompted to create a passphrase in order to locally encrypt your data. This means that your data will be encrypted in transit, and that your messages will also be encrypted locally on your phone. If you choose to skip this step, your messages will still be encrypted in transit, but will not be protected on your device. For more information on selecting a strong passphrase, see the **Passwords Lesson**.



### Step 3 (optional): Import existing text messages

You will then be asked if you would like to import your existing text messages into TextSecure’s encrypted database. This is up to you: It simply means that old text messages (SMS) will be imported into the TextSecure app and encrypted.

### Step 4 (optional): Register your phone with TextSecure

The next screen will prompt you to “Connect with TextSecure” by registering your mobile phone number with TextSecure. This will allow you to avoid SMS charges in some cases when communicating with other TextSecure users. This is an optional step. Once you have registered your phone, TextSecure will automatically verify your number using a text message.

## 3.0 Verifying Keys

TextSecure uses end-to-end encryption. When you first send a message to another contact that uses the app, the app will initiate a key exchange message with the other user.

You will want to verify keys with the other user (for more information, view the EFF module on [**Key Verification**](https://ssd.eff.org/en/node/37/)**).** To view the keys, click on the padlock icon in the top right of the screen and select “Verify Identity.” You will be shown two sets of keys: one belonging to you and one belonging to the other user.

TextSecure supports manual verification or verification by scanning the other user’s barcode. If you are in the same room as the other person, you can easily scan the barcode on their phone (reachable by clicking on the lock icon on the menu bar at the top of your conversation, selecting “verify identity” and then clicking on the barcode icon) or read your keys aloud to one another.

If you are not in the same room, there are different ways to verify keys with varying degrees of trustworthiness. For example, you can read your keys aloud to one another on the phone if you recognize one another’s voices or send them using another verified method of communication such as PGP or OTR.