

# Identity Finder

## Managing Personally Identifiable Information (PII)

The documentation contains the following sections:

- [Step 1: About Identity Finder](#)
- [Step 2: Download & Install Identity Finder](#)
- [Step 3: Review the Worksheet \(Faculty & Staff Only\)](#)
- [Step 4: Configure & Run Identity Finder](#)
  - o [4a: Windows Configuration](#)
  - o [4b: Mac Configuration - available November 2009](#)
- [Step 5: Manage Your Results](#)
  - o [5a: Determine the Origin](#)
  - o [5b: Actions & Password Vault](#)
  - o [5c: Acting on Your Search Results](#)
  - o [5d: Other PII](#)
- [Step 6: Schedule Re-runs](#)
- [Step 7: Submit the Worksheet to ISO \(Faculty & Staff Only\)](#)
- [Identity Finder FAQ](#)

---

For information related to this topic refer to:

- [Training & Awareness: Identity Theft](#)  
(<http://www.cmu.edu/iso/aware/idtheft/index.html>)
- [Securing Your Computer](#) (<http://www.cmu.edu/computing/security/index.html>)
- [ISO Web Site](#) (<http://www.cmu.edu/iso/>)

*Last Updated: 10/7/09*

## Step 1: About Identity Finder

Identity Finder assists you in preventing identity theft by finding Personally Identifiable Information stored on your computer, file shares or external media and providing you with the ability to easily and quickly protect or securely dispose of it.

### What is Personally Identifiable Information?

Personally identifiable information (PII) is any piece of information which can potentially be used to uniquely identify, contact or locate a single person. PII is generally kept private and often used for financial, medical or research identification. Examples of PII include Social Security Numbers, Credit Card Numbers, Bank Account Numbers, Driver's License Numbers and account passwords.

### Why Clean Up PII?

If your computer or external media is lost, stolen or broken into over the network, sensitive PII may be harvested from your compromised equipment. A surprising amount of sensitive PII (e.g. your passwords, credit card numbers, and maybe even Social Security Number) may be retained on your computer just from daily use along with sensitive PII stored in personal and work files. This information can be used to steal not only your money and identity, but also the money and identities of anyone else who either shares your computer or whose sensitive PII you store for Carnegie Mellon work. And if you do store sensitive PII for Carnegie Mellon work, the University would be obligated under PA state law to notify everyone affected by the breach and could potentially be legally liable.

You might think this could never happen to you, but consider these facts:

- Laptop losses totaled \$6.7 million for 2005 -- [2005 Computer Security Institute/FBI Computer Crime and Security Survey](http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf) (<http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf>)
- 1 out of every 8 to 15 laptops were lost or stolen over the last few years
- The Carnegie Mellon network sees over 700,000 cyber attacks per day
- PII breach notifications were sent for two lost Carnegie Mellon laptop incidents within the last year and a half
- Over eight million Americans have their identities stolen annually -- [Federal Trade Commission](http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf) (<http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>)
- 85% of identity theft victims find out about identity theft through an adverse action such as a loan or employment denial and the average identity theft victim will have to spend 600 hours clearing his or her good name -- [Identity Theft Resource Center](http://www.idtheftcenter.org) (<http://www.idtheftcenter.org>)

Invest the time now to clean PII from your machine and help prevent [Identity Theft](http://www.cmu.edu/iso/aware/idtheft/index.html) (<http://www.cmu.edu/iso/aware/idtheft/index.html>) for yourself, for everyone who shares your computer and for everyone whose data you handle.

### Why Can't Computing Services do This for Me?

Although your departmental computing administrator or DSP consultant may install software and help you with the clean up process, you must ultimately decide what

files to securely delete or securely retain given your duties and needs. Additionally, the PII searching software will find sensitive PII such as passwords and financial account numbers that you should keep private even from your computing support personnel.

## How Do I Clean Up PII on Windows Machines?

Follow the steps provided in this document to install and run Identity Finder.

**Faculty and staff members:** Please complete a PII Clean Up Worksheet for **each computer** you clean **while you are in the process** of cleaning it. These worksheets are the only mechanism we have for measuring the effectiveness of the software and improving the PII clean up process. Please take the time to provide us with this much needed feedback.

### Steps for Cleanup

- READ introduction material on this page
- [Download and Install](#) (<http://www.cmu.edu/computing/software/all/identity/download.html>) Identity Finder
- REVIEW the [Worksheet](#) ([http://www.cmu.edu/computing/doc/security/identity/PII\\_Cleanup\\_Worksheet.doc](http://www.cmu.edu/computing/doc/security/identity/PII_Cleanup_Worksheet.doc)) (Faculty and Staff ONLY)
- [Configure and Run](#) an Identity Finder Search
- [Manage Your Search Results](#)
  - o Choose how to clean each search result
  - o Rerun Identity Finder for additional external storage or shared folders
  - o CLEAN files that you KNOW contain PII but Identity Finder missed (Identity Finder may not recognize certain custom file formats)
- [Schedule Re-runs](#) so that you remember to run Identity Finder regularly (e.g., weekly, monthly).
- [SUBMIT the Worksheet](#) to ISO (Faculty and Staff ONLY)



## Step 2: Download & Install Identity Finder

*Last Updated: 4/23/08*

## Step 3: Review the Worksheet (Faculty & Staff Only)

**FACULTY AND STAFF:** Please complete a [PII Cleanup Worksheet](http://www.cmu.edu/computing/doc/security/identity/PII%20Cleanup%20Worksheet.doc) (<http://www.cmu.edu/computing/doc/security/identity/PII Cleanup Worksheet.doc>) for **each computer** you clean **while you are in the process** of cleaning it.

These worksheets are the only mechanism we have for measuring the effectiveness of the software and improving the PII clean up process. Please take the time to provide us with this much needed feedback.



## Step 4: Configure & Run an Identity Finder

### Search

*Last Updated: 10/2/09*

## Step 2: Download & Install Identity Finder

**Note for DSP Clients:** Desktop Support Program (DSP) clients should have Identity Finder pre-installed on their DSP supported computers and thus may skip this step. However, they should download Identity Finder for other personal computers.

### Identity Finder v3.4.8 for Windows

To download Identity Finder, visit the Identity Finder [DOWNLOAD](http://www.cmu.edu/computing/software/all/identity/download.html) (<http://www.cmu.edu/computing/software/all/identity/download.html>) page, and then return to [Step 3](#) to configure and run a search.

### Identity Finder v2.0.1.4 for Mac

Available November 2009.

*Last Updated: 10/07/09*

## Step 4: Configure & Run Identity Finder

Documentation is available for configuring and running Identity Finder on Windows and Mac operating systems. Please select the documentation for your machine.

- [Step 4a: Windows Configuration](#)
- Step 4b: Mac Configuration - Software download will be available November 2009.

*Last Updated: 10/07/09*

## Step 4a: Configure & Run an Identity Finder Search

### Windows Vista or XP

1. Before you begin...
  - Connect or insert any external storage media (external hard drives, USB drives, CDs or DVDs) or file server shares that you want to search in addition to your computer's hard drive.
  - Disconnect from any file server shares that you do NOT want Identity Finder to search.
2. To launch Identity Finder Enterprise Edition, select **Start > All Programs > Identity Finder > Identity Finder Enterprise Edition**.
3. The Identity Finder Welcome window appears. Select the radio button to **Continue in Wizard Mode**, and then click **Next**.



4. The Automatic Searching Using AnyFind window appears. Under AnyFind Searching, be sure that the checkboxes for Credit Card Numbers, Bank Account Numbers, Social Security Numbers and Passwords are checked. Under AnyFind Worldwide Searching, select **Yes** if you are likely to have personal information from specific countries stored on your computer. Click **Next**.  
**Note:** If you choose to search for non-US identification numbers, then the Automatic Searching Using AnyFind Worldwide window appears. Select the additional countries and identity types for which you would like to search.



Identity Finder Wizard

### Automatic Searching Using AnyFind

AnyFind™ will find all Social Security and Credit Card Numbers as well as most Bank Account Numbers and Passwords regardless of whose they are and without any information from you.

AnyFind Searching

AnyFind will automatically find personally identifiable information for the following identity types:

|   |   |
|---|---|
| <input checked="" type="checkbox"/>  Credit Card Numbers (or Debit Card) | <input checked="" type="checkbox"/>  Social Security Numbers |
| <input checked="" type="checkbox"/>  Bank Account Numbers                | <input checked="" type="checkbox"/>  Passwords               |

AnyFind Worldwide Searching

Would you like to choose additional identity types to find personal information from specific countries:

Yes  No

< Back   Next >   Cancel

- The Unique Search window appears. If you wish to provide Identity Finder with your personal information to search for in addition to the Automatic Searching generic rules, select the **Yes** radio button. Otherwise select the **No** radio button to only use the Automatic Searching generic rules. Click **Next**.
- If you select **Yes** in the previous step, the Unique Searching with entry fields window appears (if you selected No, skip to the next step). In the text fields, enter personal information to search for, and then click **Add** to move it to the Unique Identity Include List.

Identity Finder Wizard

### Unique Searching Using Your Personal Information

Please enter the unique Identity Matches that you would like to find. Depending on the identity type Identity Finder will enhance your search by converting your information into various formats.

Personal Identity Information Entry Fields

|                  |                        |
|------------------|------------------------|
| Date of Birth    | <input type="text"/>   |
| Driver's License | <input type="text"/>   |
| Personal Address | 100 Pleasant St, Pitts |
| Passport Number  | <input type="text"/>   |
| Telephone Number | <input type="text"/>   |
| Employee ID      | <input type="text"/>   |
| Mother's Maiden  | <input type="text"/>   |

Unique Identity Include List

| Type             | Value      |
|------------------|------------|
| Date of Birth    | 05/20/1985 |
| Driver's License | 87654321   |

Buttons: Add, Remove, < Back, Next >, Cancel

7. The Where to Search window appears. Check to be sure that checkboxes for All Files, Hidden Web Data, E-Mails and Attachments and Windows Registry are selected. Under File Locations, select the radio button for the places you want to search. Choose either **My Documents and Settings**, **My Computer** or **Custom Location**.

Identity Finder Wizard

### Where to Search

Choose the items and locations on your computer where you would like to search.

Where to Search

All Files       E-Mails and Attachments

Hidden Web Data       Windows Registry

File Locations

My Documents and Settings

My Computer

Custom Location

To easily select a Custom Location, use the pull down icon to browse to the drive you want to search.

Buttons: < Back, Next >, Cancel, Help

8. The Finalization window appears. Review your selections, click **Back** to make any changes, or click **Finish** to begin the search as specified.



## Step 5: Manage Your Results

*Last Updated: 9/30/09*

## Step 4a: Configure & Run an Identity Finder Search

### Macintosh Operating System

**Note:** The Identity Finder for Mac software will be made available in November 2009.

#### 1. Before you begin...

- Connect or insert any external storage media (external hard drives, USB drives, CDs or DVDs) or file server shares that you want to search in addition to your computer's hard drive.
- Disconnect from any file server shares that you do NOT want Identity Finder to search.

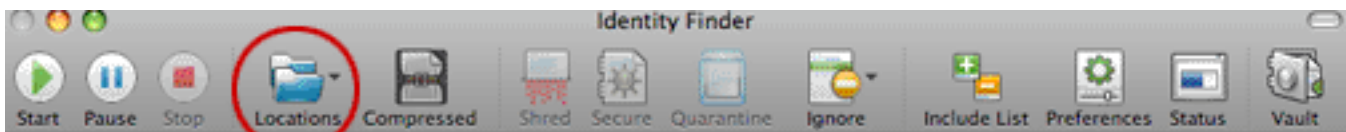
2. To launch Identity Finder, double-click **Applications > Identity Finder.app**.

3. An Internet download warning message will appear. Verify the source and click **Open**.



4. The Identity Finder application will open. Under **Locations**, select the folder that you would like to have searched. For example, you can search Documents, your entire computer, or you can select **Custom** and then click ... to navigate to a specific folder. Once you've identified the folder, click **Open**, then **Add**.

**Note:** Identity Finder for Mac cannot search email files or web browser data at this time.

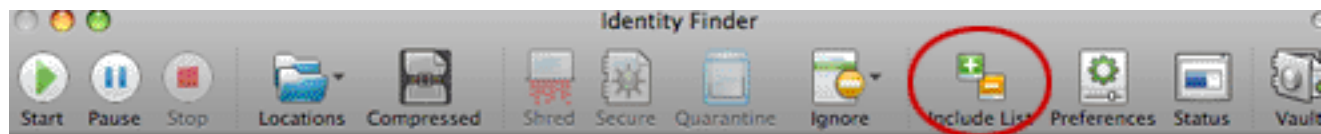


5. Click **OK**.

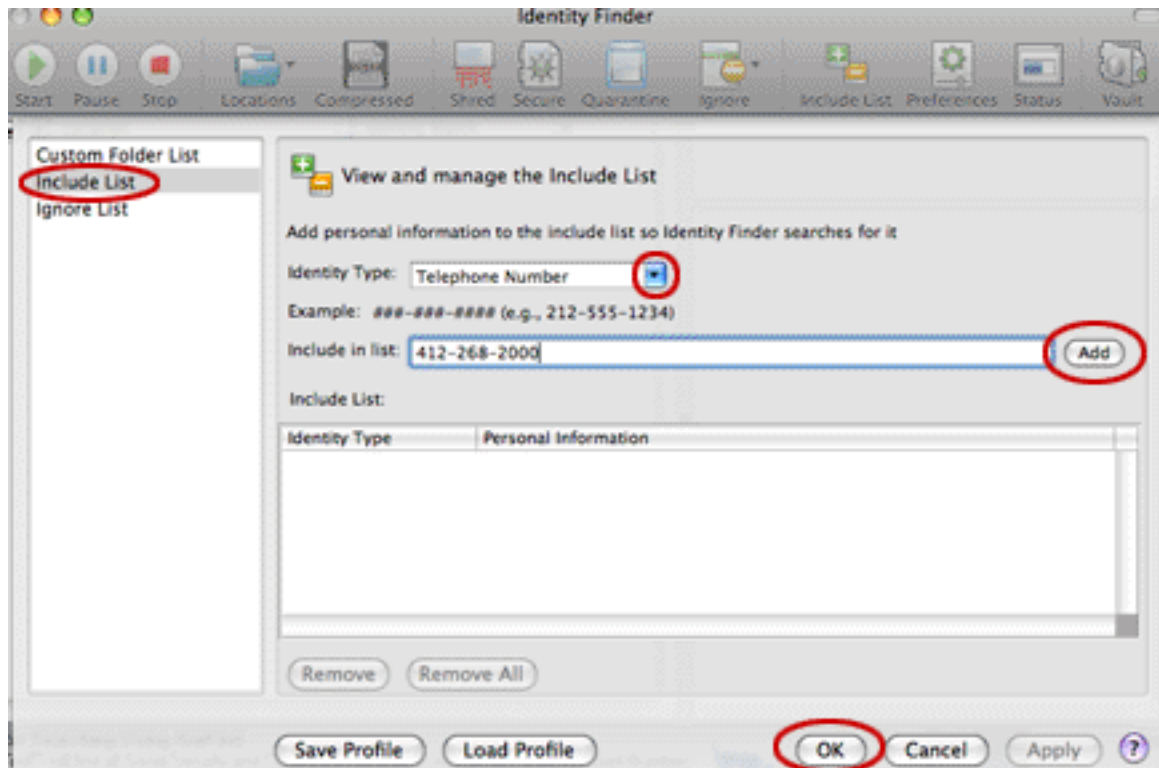
6. Under the **Identities** menu, a list of personal information categories that you can search for will be displayed. Select the specific item to search, such as Date of Birth, and select **Any Find**.



7. To identify specific personal information for the search:
  - a. Select the **Include List** icon.

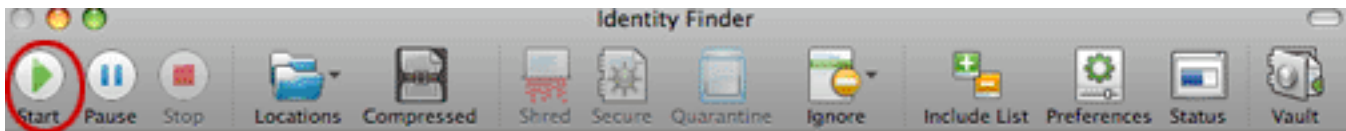


- b. From the drop-down menu, select the identity type (i.e., date of birth, personal address, social security number, credit card number, etc.).
  - c. Type in the relevant information, such as your street address, in the **include in list** text box.
  - d. Click **Add**.
  - e. Click **OK**.



8. Click **Start**.

**Note:** It may take several minutes for your search to be completed, depending on the number of sub-folders and files. The application will run in the background, however, if necessary, you can click Stop to cancel your search.



9. Upon completion, a Search Completed window will appear with the results. If any instances were found, the file location, type of identity match, number of occurrences and a preview of the document will be listed.



## Step 5: Manage Your Results

Last Updated: 10/2/09

## Step 5: Manage Your Results

The most important part of running Identity Finder is determining the most effective and secure way of managing the search results. This section is divided into sub-steps. Be sure to carefully read and proceed through each of the following steps.

- [Step 5a: Determine the File's Origin](#)
- Step 5b: Actions & Tools
- Step 5c: Acting on Your Search Results
- Step 5d: Other PII



### [Step 5a: Determine the File's Origin](#)

*Last Updated: 1/7/08*

## Step 5a: Determine the File's Origin

For each file that contains PII, consider these points:

**IMPORTANT NOTE:** If you are under a litigation hold, contact the Office of General Counsel (412-268-8090 or [jamercol@andrew.cmu.edu](mailto:jamercol@andrew.cmu.edu) ([jamercol@andrew.cmu.edu](mailto:jamercol@andrew.cmu.edu))) before making any changes.

- **Where did the file come from?**
  - o Is it your personal file?
  - o A file from someone who previously used or owned the computer?
  - o A file from Carnegie Mellon business or academic operations?
  - o Do you have no idea where it originated?
- **If the file was left from the previous owner or if you have no idea where it originated:**
  - o If the machine was provided by Carnegie Mellon for business or academic operations consult your supervisor/advisor to learn what to do with the file.
  - o If your supervisor/advisor does not believe the file was part of Carnegie Mellon business or academic operations AND you share your computer with family, friends or co-workers, please consult the people you share your computer with to determine the source of the file and whether it needs to be retained.
  - o If you still do not know where the file originated after consulting your supervisor/advisor and the people who share your computer, [shred](#) the file.
- **Carnegie Mellon Business/Academic Operations Or Personal Data**
  - o If you are unsure whether you need to retain a file containing PII related to Carnegie Mellon business or academic operations, please consult your supervisor/advisor.
  - o If the file does not need to be retained, [shred](#) the file.
  - o If the file does need to be retained, ask yourself if you need the sensitive PII portions.
    - If no, then [redact](#) (i.e., replace sensitive PII numbers with XXX while leaving the rest of the file unchanged).
    - If yes, then ask yourself if you need it on this computer?
      - Yes, then [encrypt](#) the file.
      - No, then [quarantine](#) the file.



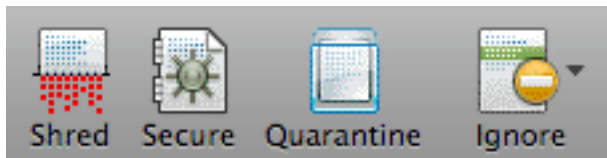
## Step 5b: Actions & The Password Vault

Last updated: 6/23/08

## Step 5b: Actions & The Password Vault

### Actions

After reviewing your search results, you'll need to select the best way to handle this sensitive information. The following actions are available to you:



**Secure (Encrypt or Redact)** - Secures the highlighted item using the associated application's features.

- **Encrypt** - Identity Finder uses application specific encryption where available (e.g., MS Office and Adobe PDF) to password protect the file. When no application specific encryption is available compressed file encryption is used. Depending on the file type, you'll be prompted differently for how to encrypt the file (see Identity Finder Online help topic: **Securing Identity Matches Overview** for details).

#### Important notes on Encryption

- o When you encrypt a file, you should use the option to save the password for that file in your [Password Vault](#) if using a Windows operating system. The Mac operating system will only allow IDF File Vault encryption.
  - o When encrypting Adobe PDF files, be sure to choose RC4 128-bit encryption.
  - o When using compressed file encryption, be sure to choose AES 256-bit encryption.
  - o When AES 256-bit encryption is used, you will NOT be able to open the file by double-clicking on it. You must use Identity Finder's [Open Secure Zip File](#) feature.
- **Redact** - (Text, CSV, and HTML files only as of version 3.4.8) When a text file has sensitive identity match information in it and you wish to keep the file on your computer, but do not need the personal information, you should utilize the **Redact feature** to automate the securing of this file by removing the personal information and leaving all other content in place. You can choose to replace the data with numbers or an "X".

There are two ways to secure a single text based file with redact:

- o Single click the file result with the left mouse button to highlight it and click the **Secure** button on the Main ribbon. Then choose **Redact**.
- o Single click the file result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on **Secure**. Then choose **Redact**.

To redact multiple text files at one time, check the checkbox of each file and then choose one of the methods described above to begin securing the files. You can choose to redact the personal information and replace it with your default choice from your Identity Finder Settings Redact From Text Files option, or you can select any digit from 0 to 9 or an X. Once you click OK, the personal information will be permanently removed.

**Shred** - The Shred button is located on the Main ribbon and is enabled for all types of result; however, depending on the location of the result, Shred behaves differently. For files, shred utilizes a secure United States Department of Defense wiping standard known as DOD 5220.22-M. For other locations, shred removes the information from your computer using other, appropriate methods.

There are three ways to Shred a location:

- Single click the result with the left mouse button to highlight it and click the **Shred** button on the Main ribbon.
- Single click the result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click on **Shred**.
- Highlight the result by single clicking with the left mouse button or by using the arrow keys and then press the **Delete** key on your keyboard.  
Important Note: It is not possible to "undo" a Shred. Shredded results cannot be recovered. Once you shred something, it is gone.

**Recycle** - This feature is disabled on our installer. Moving a file to the Recycle Bin does not actually delete the file. To truly remove a file, use **Shred**.

**Quarantine** - Securely moves the highlighted file to a quarantine location and permanently shreds it from its original location. To Quarantine, highlight the item you want to quarantine; the Quarantine dialog box appears. Select the Quarantine folder to move the file to. This should be a folder that is highly secure, such as an encrypted drive or a storage device to which unauthorized individuals do not have access. Note: You can specify a default Quarantine location in **Settings**. You may also choose to leave behind a warning text document in place of the file.

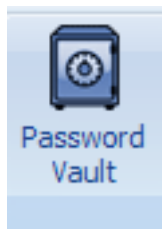
**Open** - Click Open to open and review the contents of the highlighted file in its associated application. **Note for Mac:** selecting the name of the file will display a preview of the document, which can then be opened if desired.

**Ignore** - Allows you to designate certain items to be ignored by Identity Finder. Click **Ignore** and choose from the following:

- **This Item Location:** To ignore this file.
- **This Identity Match:** To ignore this Identity match in ALL locations in which it appears.
- **Manage 'Ignore List':** To create a list of items to ignore, select the **Ignore a File** option and click the **File Selection** button. This button will open a dialog box that allows you to select any file on your computer. After navigating to your desired location, click the **Open** button and the full path to your selected file will be displayed. Once you have selected a file location to ignore, click the **Add** button and it will appear in the Identity and Location Ignore List. To remove a

location or multiple locations, highlight them and click the **Remove** button. The **Remove All** button clears the entire list. If you make changes and want to Save your list for future sessions, click the **Save** button. Otherwise click **OK**. You may be prompted to provide a password if you are saving a new list. If Identity Finder did not automatically load your Ignore Identities and Location list when it started, you can load it now by clicking the **Load** button. You will be prompted for your password. Locations that you add to the Ignore List during a search will be ignored for the remainder of the current search.

## The Password Vault



The Password Vault tool allows you to securely store and manage usernames and passwords for websites, encrypted files, and other locations inside of Identity Finder and protect them with a single Password Vault password. In other words, the Password Vault password is a single master password that allows you to gain access to the Password Vault. Once you've gained access, the Password Vault houses your list of files and their respective passwords.

**Note:** The Password Vault tool is not available for Mac operating systems.

### Important Information for Using the Password Vault

- There is NO WAY to recover a forgotten Password Vault password. Once you've established this password, write it down and lock it in a SECURE location. **If you plan to encrypt files for Carnegie Mellon business or academic operations, be sure to inform your supervisor of the secure location of the Password Vault password to ensure business continuity.**
- **Do NOT** use your **Andrew Account password** as your Password Vault password.

### Accessing the Password Vault Tool

To access the Password Vault tool, click the **Password Vault** button on the Tools and Options ribbon.

1. Once selected, the Password Vault dialog will open. Enter any Location, Comment, Username, and/or Password then click **Add** to add an item and its corresponding password to your vault. Click **OK**.  
**Note:** At no point does Identity Finder attempt to validate that the usernames or passwords that you place in the password vault are correct; therefore, it is necessary for you to ensure that you type them in correctly.
2. The first time you close the Password Vault after adding an item to it, you'll be prompted to set your Password Vault password.  
**Note:** When you re-launch Identity Finder, you'll be prompted for your Password Vault password to access your secure information.



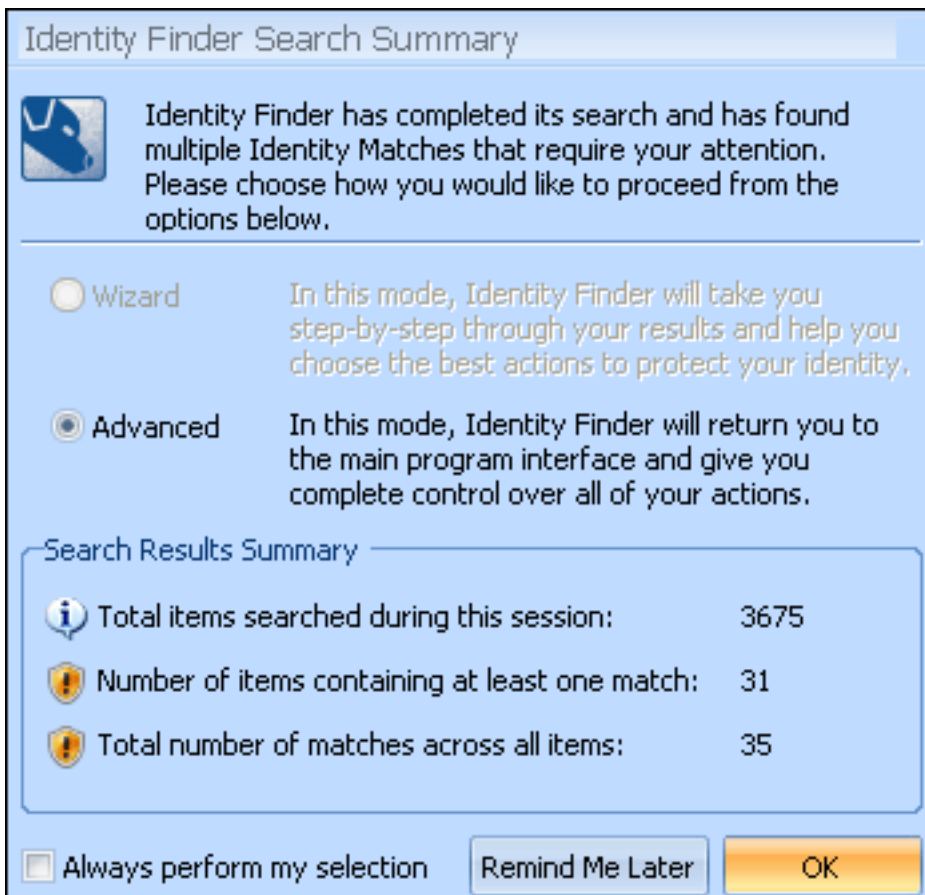
## Step 5c: Acting on Your Search Results

*Last Updated: 10/2/09*

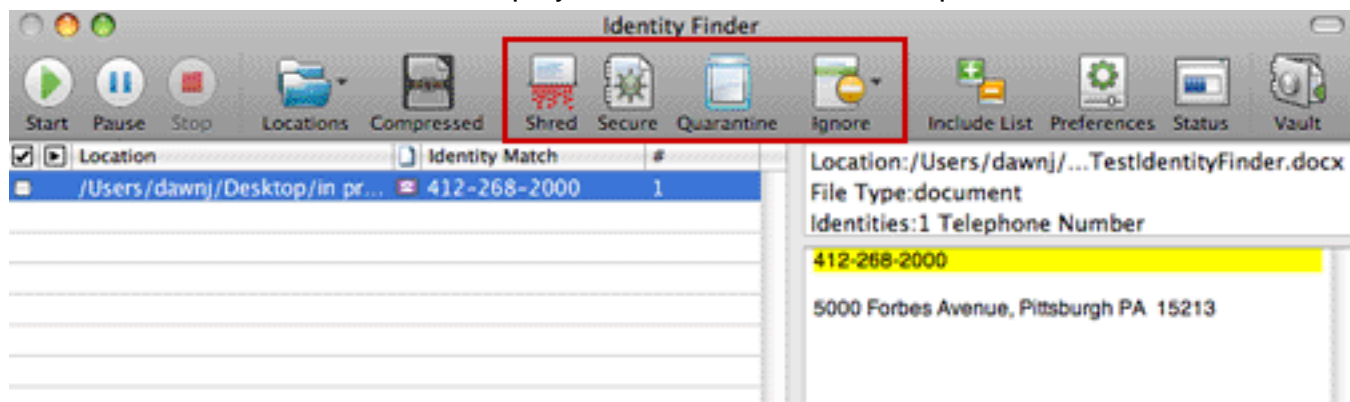
## Step 5c: Acting on Your Search Results

Follow these steps to manage any PII related files through Identity Finder.

1. **Windows:** With the Identity Finder Search Summary box displayed, click **OK**.



**Mac:** The results window will be displayed after the search is complete.



2. For each item, select it and then choose the action you want to apply from the top menu items. For more detailed instruction, refer to [Actions](#).
3. Repeat Step 4 and Step 5a-5c for any other external storage media or folder shares you wish to clean.

## Securely Saving Your Results

If your list of PII is extensive, you can securely save your results and manage them at a later time. Follow these steps:

1. Select **Save** and browse to the location where you wish to save the Identity Finder (.idf) file. The Save As dialog box appears.
2. Enter a name for your file and select **Save**. The Enter Password dialog box appears.
3. To protect this information, you must enter and confirm a password that you will use when you next attempt to access this information. Click **OK**.
4. Close the Identity Finder window.

## Accessing Your Saved Information

1. Launch Identity Finder. The Enter Password dialog box appears.
2. Do one of the following:
  - To access your saved file, enter the password from step 3 above.
  - To run a new Identity Finder search, click **Cancel**. The Welcome screen appears. Refer to [Configure & Run Identity Finder](#) for help with performing a new search.



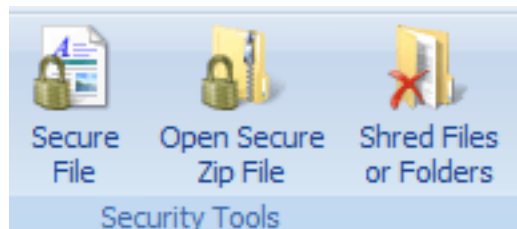
## Step 5d: Other PII

*Last updated: 10/2/09*

## Step 5d: Other PII

Identity Finder may not recognize some custom file formats; however, Identity Finder cleanup features can still be used to handle these files.

Use the following Identity Finder Security Tools to handle files NOT listed in the Identity Finder search results:



**Secure File** - The Secure File tool allows you to secure any file on your computer even if no Identity Match is found in that file. To use the Secure File tool:

1. Click the Secure File button on the Tools and Options ribbon. The Secure File dialog opens.
2. Click the File Selection button to launch a dialog box that allows you to select any file on your computer.
3. After navigating to your desired location, click the **Open** button and the full path to your selected file will be displayed.
4. Then click **Secure** and you will be presented with the specific options to secure that type of file such as encryption strength and password.
5. Choose the appropriate options (refer to [Step 5b Encrypt Action](#)) and click **OK** to secure your file.

**Open Secure Zip File** - The Open Secure Zip File tool allows you to open and extract (unzip) the contents of any secure zip file on your computer. This is a very useful feature if you used Secured a Compressed File or Secured a Text Based or Other File in conjunction with the Strong or Stronger encryption setting.

To open a secure zip file:

Click the Open Secure Zip File button on the Tools and Options ribbon.

Once selected, the Open Secure Zip File dialog will open. Click the Select Zip File button to launch a dialog box that allows you to select any zip file on your computer. After navigating to your desired location, click the "Open" button and the full path to your selected file will be displayed. Then click the Select Target Location button to launch a dialog box that allows you to select any folder on your computer. After navigating to your desired location, click the "OK" button and the full path to your selected folder will be displayed. Finally, type your password in the Password field and click the "Extract" button. Your files will be extracted to the desired location and an Explorer window will open to display the extracted files.

**Shred Files or Folders** - Allows you to shred any file or folder (and all subfolders and files) on your computer, even if no Identity Match is found. Click the **Shred** button. When the Shred Files dialog box opens, browse to the folder or file(s) that you want to shred. **YOU CANNOT UNDO THIS ACTION!**



## Step 6: Schedule Re-runs

*Last updated: 1/7/08*

## **Step 6: Schedule Re-runs**

Mark your calendar or use the Identity Finder scheduling feature as a reminder to run Identity Finder on a regular basis (e.g., weekly, monthly).



## **Step 7: Submit the Worksheet (Faculty & Staff Only)**

*Last updated: 1/7/08*

## **Step 7: Submit the PII Worksheet (Faculty & Staff only)**

Thank you for completing the PII worksheet. This information will help us to improve the effectiveness of the software.

Please email the worksheet to [iso-identityfinder@andrew.cmu.edu](mailto:iso-identityfinder@andrew.cmu.edu) (<mailto:iso-identityfinder@andrew.cmu.edu>).

*Last Updated: 1/7/08*

## Identity Finder FAQ

### How do you find the Identity Finder version number?

To find the Identity Finder version number, follow these steps:

1. Launch Identity Finder
2. If the Identity Finder Wizard appears, click **Cancel**.
3. Click the Identity Finder button (top left) to bring up the Identity Finder menu.
4. Click the **About** button from the Identity Finder menu.
5. The version number is displayed in the middle of the window next to Version.

### What email program does Identity Finder support?

Identity Finder can search emails contained in Outlook, Outlook Express, and Windows Mail. Unfortunately, Identity Finder cannot search Mozilla Thunderbird.