Identity Finder User Guide

CAL POLY CORPORATION
SAN LUIS OBISPO *Information Technology*

Introduction

Identity Finder refers to a suite of software programs developed by Identity Finder, LLC. This suite of programs is designed to help ensure the security of vital information in order to help prevent data leaks within a company. The suite offers five essential utilities: discovery of sensitive data, classification of information, remediation of confidential information, monitoring, and remote reporting.

In short, it allows you to search, identify, and manage sensitive data stored on your local computer.

For more information on Identity Finder, see the Cal Poly Information Security page on Identity Finder.

The California State University (CSU) has identified three classification levels that are referred to as Level 1, Level 2, and Level 3. For more information on the data classification and handling standards, click here:

Why are we doing this

Per the CSU Sensitive Data Security and Protection Audit, we are required to audit and identify where sensitive data is stored. Identity Finder will search your email and local computer (not the network drives) and locate possible sensitive data. It is the responsibility of each person to review the results and take the appropriate action for each identified item. You need to assess what the data is and what is the risk to the University if the data is stolen.

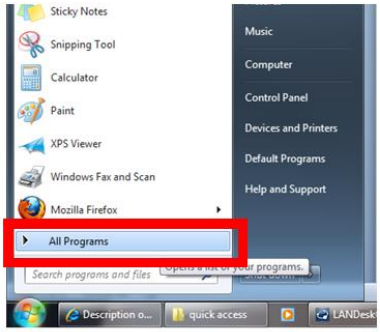
If there is sensitive data stored on your local computer the University could be at risk. This risk could be from someone stealing your physical computer or accessing it electronically if your computer is compromised.

Opening Identity Finder for the First Time

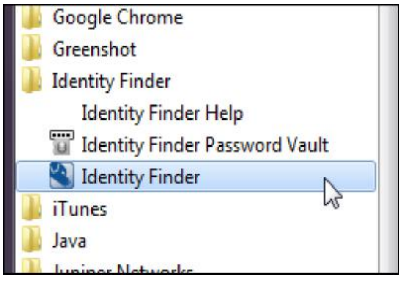
Identity Finder is easy to use. To get started:

1. Click on the Windows Start icon found at lower left corner of the Task Bar.

2. Click on All programs



3. Click on Identity finder



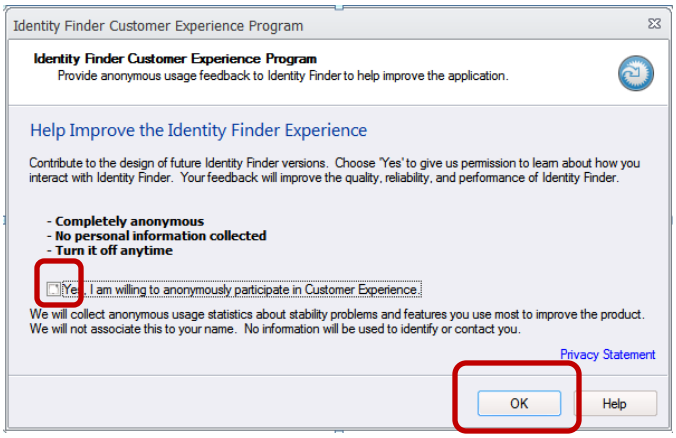
4. This will open Identity Finder

   The <u>first time you start Identity Finder,</u> it will ask a few questions.

   a. "Help Improve User Experience"

      i. **Do Not** check the box for "Yes, I am willing to anonymously participate in Customer Experience"

      ii. Select OK on bottom right



   b. New Identity Finder Profile

      i. Create a profile by entering a user name and password

      ii. Create a **New Unique Password** for Identity Finder; then click OK

   c. From now on, when you open Identity Finder, it will just ask for your password.

If you forget your profile password, don't worry! You can delete the profile and start over. For more, visit here: Identity Finder Profile Password

Using Identity Finder

For detailed instructions on how to use Identity Finder, see following links available on the Cal Poly Information Security page:
Identity Finder - Searching for Sensitive Data
IDF - Remediating Discovered Sensitive Data
Identity Finder Profile Password

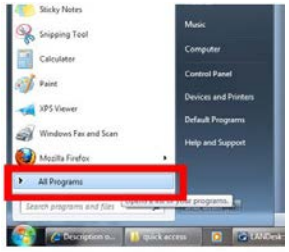
1. Start Identity Finder

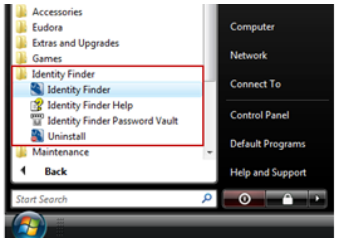
   If this is the first time you have opened Identity Finder, see the "Opening Identity Finder for the First Time" section above.

   a. Click on the Windows Start icon on lower left corner of the Task Bar

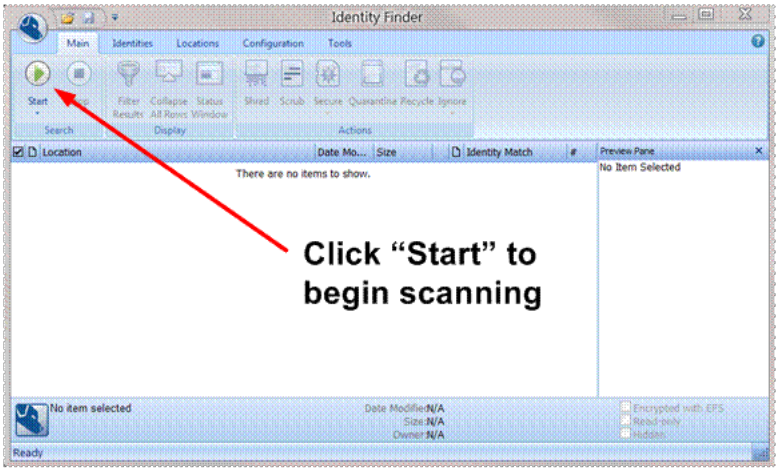
   

   b. Click on All Programs, and then click on Identity Finder

2. Start a search. Identity Finder is pre-configured to search for Level 1 Data. Select the Start Button upper left corner of the window.



Identity Finder will take hours to run!

It can take Identity Finder hours to run. It is configured to run in the background with low priority to minimize the effect on your computer's performance. However, it is recommended to run Identity Finder while you are not at your computer (i.e., overnight, especially the very first time).

1. Start Identity Finder
2. Start a scan

LOCK YOUR COMPUTER.

Lock your computer by holding down Windows Key and pressing the "L" key together.

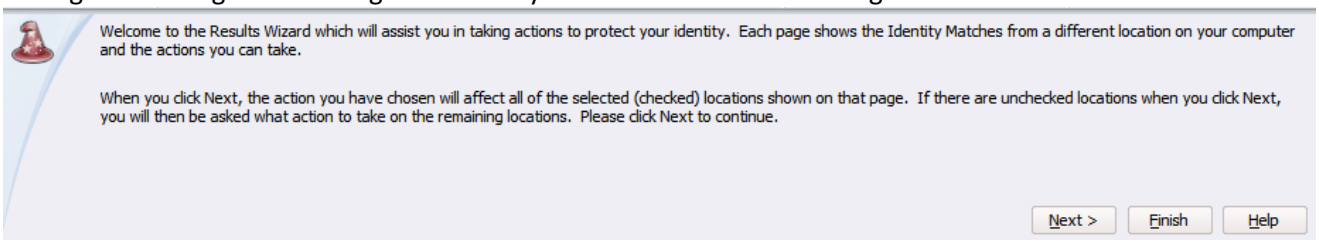
It is very important that you lock your computer before you walk away. Do not leave your computer unlocked and unattended.

Understanding the Results

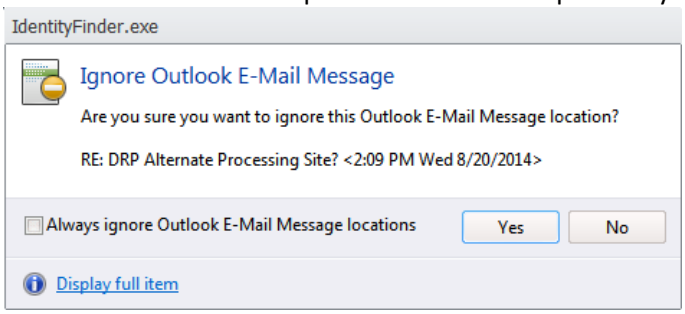
When Identity Finder is done, it will display a detailed report of what it found. You will then be able to select items to Delete, Scrub or Ignore. At first glance, the report can be a little overwhelming; here is an explanation of the different parts.

Results Wizard

You will see the Results Wizard on the top left portion of the screen. The Results Wizard will walk you through Shredding or Scrubbing data out of your files. Click "Next" to begin.

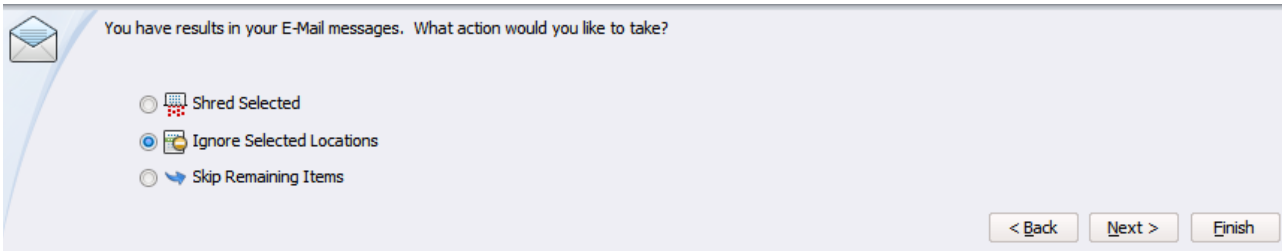


The Results Wizard is simple to use and self-explanatory. Follow along the prompts.



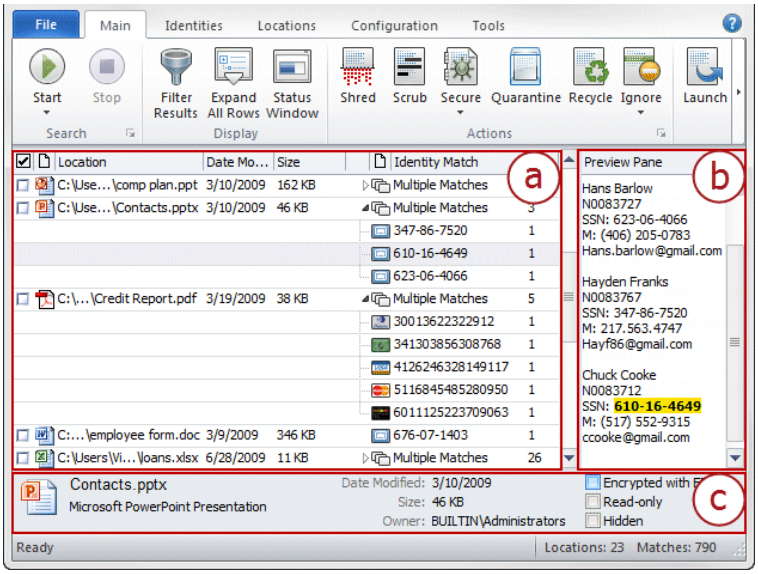
Identify Finder is pre-configured by the University to include Outlook email in its search. It is not possible to exclude your email from the process. You can ignore the search results after the search is complete; however, it is strongly recommended that you remedy the findings the first time.

You may see a dialog box as below. Select the ratio button as appropriate.



Shred the selected results, ignore selected locations, or skip remaining items.

Viewing Search Results



The results of the search are displayed in the **(a) Results View** and, along with the **(b) Preview Pane** and the **(c) Properties Pane**, provide all of the relevant information about the result including the full path to its location, the type, and value of the result, a preview of that result in context, and many other details.

The Results View is a reporting table, similar to a spreadsheet that is on the left side of Identity Finder. It contains all the information about the results of your search and allows you to analyze those results and take action to protect any sensitive information.

Remediating Discovered Sensitive Data

Some features, such as Scrub, Secure, Quarantine, Recycle, and Ignore, are greyed out and may be available to you.

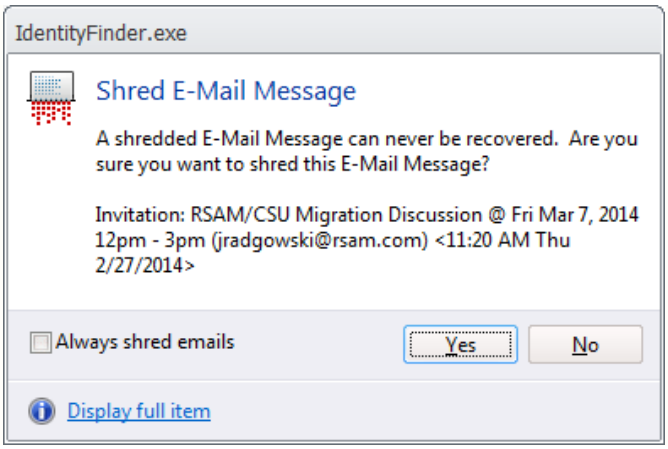
Shredding Sensitive Data

If you wish to permanently remove a file that contains SSN or CCN data, select the Shred option. 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. This option should be used when the file found is no longer needed on the user's computer.

Note: It is not possible to "undo" a Shred. Shredded results cannot be recovered. Once you shred something, it is gone.

There are three ways to Shred:

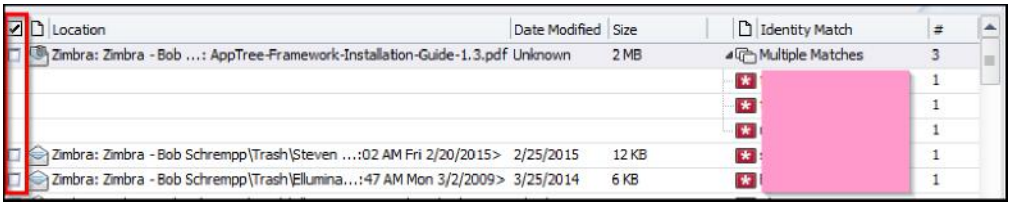
1. Click the result with the left mouse button to highlight it and click the Shred button.
2. Click the result with the right mouse button to highlight it and bring up a context menu, then highlight and left-click Shred.
3. Highlight the result by clicking the left mouse button or by using the arrow keys and then press the Delete key on your keyboard.



Shred is effective at protecting your identity because it is permanent. While this means you can never get your data back, it also means a hacker or malicious intruder also cannot get this data.

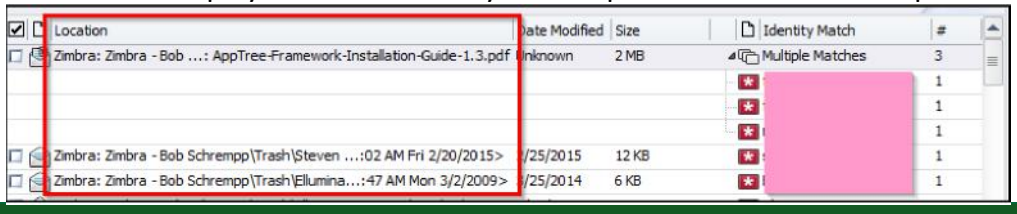
Check Boxes

Down the left side are check boxes so you can select more than one item at a time.



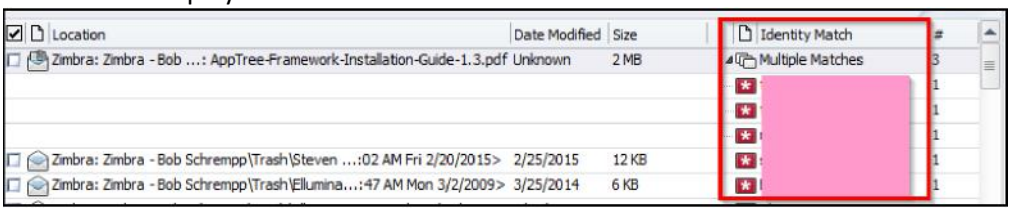
Location

This column displays the location on your computer where the file in question is located.



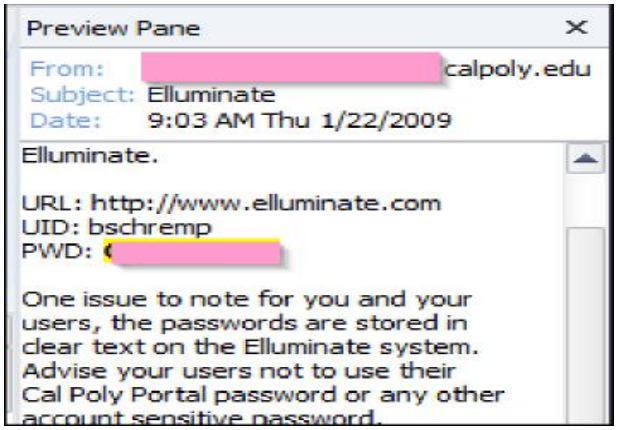
Identity Match

This column displays the data found.



Note: the data has been blanked out with a pink box.

Preview Pane



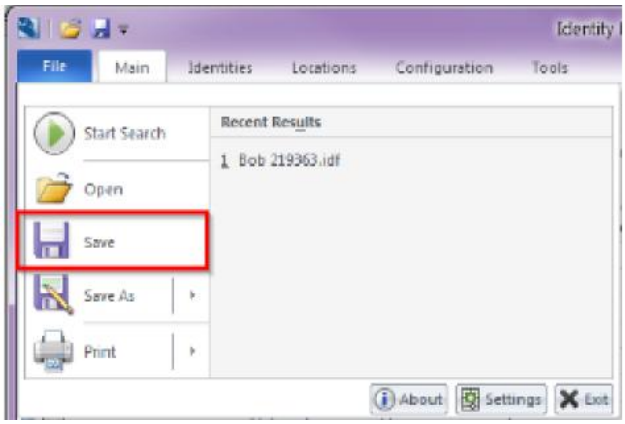
This column displays the selected file and highlights the data found in yellow.

Scrub is only available for specific file types searched via the Files search and it not available for email or some other search locations. You may only scrub Office 2007 and higher files (that is *.docx, *.xlsx, *.pptx) and text files (*.txt, *.log, *ini).

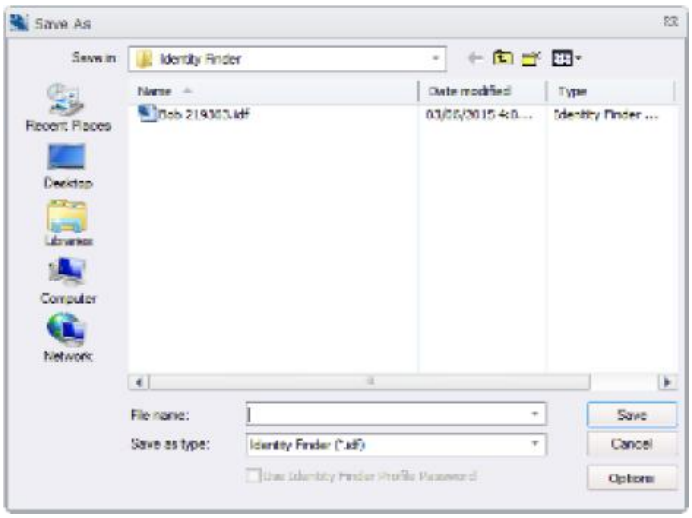
Saving the Results

When you are done processing all your results, save the data.

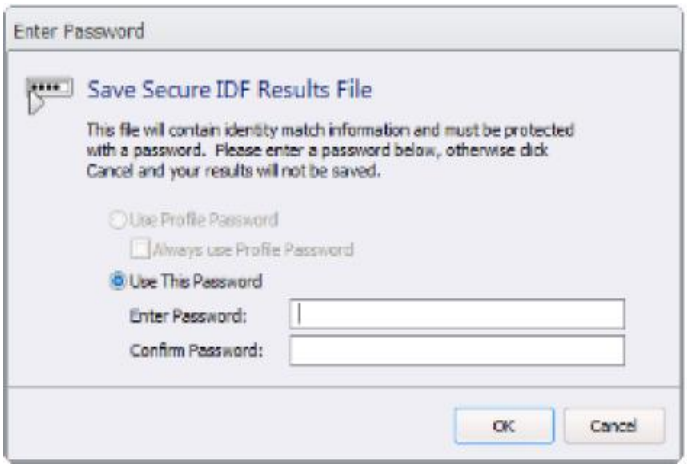
1. From the menu select File Save



2. If you have an existing results file you can replace it or save this set of results as a new file.



3. You will be prompted to enter a password. This is a password on the results file. We recommend you use the same password you use for Identity Finder.



The result contains a list of all the results from Identity Finder. It is important to use a strong password to protect this data.