# Identity Finder Faculty & Staff Guide

Helping You Mitigate the Risks of Confidential Data

Please note:  Clicking on any underlined text will take you to the corresponding location in the guide.

## CONTENTS

# I. About Identity Finder

## What is Identity Finder?

In response to the risks of recent security breaches in academic institutions with large amounts of highly-sensitive information, the L&S IT Office (LSITO) is introducing Identity Finder, a tool which allows L&S employees to easily locate and mitigate the risks of confidential data.

The deployment of Identity Finder consists of two parts. The first part, the Identity Finder service, allows LSITO to locate and generate comprehensive reports on the locations of confidential data (SSNs, Credit Card Numbers, etc.) on L&S-owned computers. The second part, the Identity Finder client, will allow College employees to search their own computers for confidential data and also to use the reports from the Identity Finder service to mitigate the risks associated with this sensitive information.

## Why do I need Identity Finder?

The L&S IT Office has made significant efforts to further secure L&S-owned computers and data, most recently through the introduction of our proactive Web Browser plugin patches. However, due to the nature of the College's open computing environment, L&S computers are still being compromised.

As these threats have evolved, data harvesting and password-stealing applications are now routinely found on compromised L&S computers. At the same time, existing compliance requirements have increased the consequences of inappropriately disclosing confidential information.

Roughly 70% of the College's compromised computers have featured such data, especially in the form of old student records. Compounding the problem, many people are unaware that this data is present within their collection of old documents and files.

## How will Identity Finder mitigate these risks?

Utilizing the reporting functionality of the Identity Finder service, LSITO will be able to identify and locate confidential data and provide comprehensive Identity Finder reports to established departmental contacts or individual staff members. College employees can use these reports along with the Identity Finder client to apply one of the three methods of remediation: "scrubbing" (removing the sensitive information, or redacting) legacy files, "shredding" (permanently deleting) unnecessary files, or by "securing" necessary files on PantherFile.

## How should I proceed if I've received an Identity Finder report?

If you've received an Identity Finder report, walk through the Configuring & Running an Identity Finder Search section on the next page to generate an updated list of sensitive files. When your search is complete, identify your files with the guidelines in the Reviewing your Results section, and finally apply the most appropriate mitigation option from the Safeguarding your Data section.

## Can the L&S IT Office complete this procedure for me?

While LSITO is available to demonstrate the remediation process, the process of classifying each confidential file and applying the appropriate remediation method can only be conducted by the data owners themselves. Moreover, the sensitive nature of the data involved in the procedure may include confidential information that should be kept private even from LSITO technicians.

The remainder of this document explains the search functionality of the Identity Finder client, along with each of the three methods of remediation introduced above.

# II. Using Identity Finder

For your convenience, the process of using Identity Finder to find and safeguard your confidential data is broken into three simple steps. The first step deals with running an Identity Finder search to locate confidential data on your computer. The second step walks you through reviewing your search results to classify each file with confidential data to prepare for the third step of safeguarding your data by applying the most appropriate of the three remediation options explained in the About Identity Finder section.

## Step 1. Configuring & Running an Identity Finder Search

To begin using Identity Finder, click on the Start button, then browse to All Programs > Identity Finder and click on the Identity Finder program as shown to the right.

The first time you run Identity Finder, you'll be presented with the New Identity Finder Profile window shown to the right.

Your password-protected profile securely saves your settings and any information you enter to configure Identity Finder searches.

To continue and create a profile, enter a password in the first text box and enter it again in the second box, then click the Next button to display the Identity Finder Search Wizard window shown below.

LSITO highly recommends setting up a profile the first time you run Identity Finder. You may use your ePanther password or another memorable password, but you will need to provide this password each time you run the program or open any saved results from previous searches.

As shown to the right, there are three ways to use Identity Finder to search your L&S computer for confidential data: the Quick Search, the Search Wizard and the Advanced Interface.

For most users, the Search Wizard will be the quickest and most effective method to begin finding and safeguarding your confidential information.

However, in the following instances it may be easier to use the Advanced Interface:

- If you've received an Identity Finder report and know the folders and files that contain the confidential data you'd like to safeguard.

- If you'd like to search for confidential data in custom file types beyond the Identity Finder defaults of Microsoft Office, PDF, text, web, and other common file formats.

- If you'd like to begin Scheduling a Recurring Identity Finder Search

This guide will only cover the process of using the Search Wizard. If you'd like to schedule a recurring Identity Finder search for sensitive information, please turn to page 10 for complete details.

## Using the Search Wizard

To use the Search Wizard, run Identity Finder using the procedure on the previous page and enter your profile password to bring up the *Identity Finder Search Wizard* options shown on the previous page.

Note: If the Identity Finder advanced interface appears instead of the *Identity Finder Search Wizard* window after you enter your password, you can access the Search Wizard by clicking the arrow beneath the Start button at the upper left of the window and then clicking on Start Search Wizard as shown to the right.



To continue, click the Continue Search Wizard image to bring up the *AnyFind* options shown below.

The *AnyFind* search options on this screen allow you to specify which types of sensitive personal information you'd like to find, in addition to the default values shown to the right.
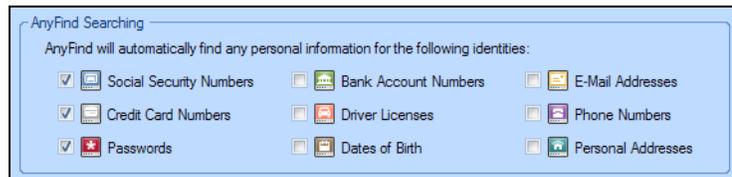


LSITO recommends keeping the default *AnyFind* search options of SSNs, Credit Card Numbers, and passwords. Aside from being the most commonly-found sensitive information, these options will reduce your search time and help eliminate the possibility of false positives.

After you've chosen the types of information you'd like to find by clicking the appropriate check boxes, click the Next button at the bottom of the window to bring up the *OnlyFind* options shown below.

The *OnlyFind* options on this screen prompt you to enter specific details which allow Identity Finder to accurately locate certain types of information.
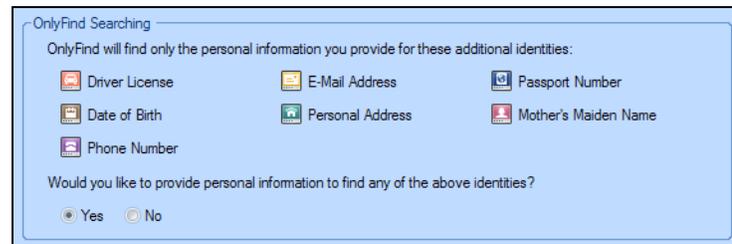
If you're only searching for the default types of personal information, you can click the No radio button at the bottom



of the window to select it and then click the Next button. If you'd like to search for any of the listed types of personal information, click the Next button to begin entering your details on the window shown below.

For each type of information you'd like to locate, enter the appropriate details and then click the Add button to add it to the column on the right. To remove an item from the right column, click once to select it, then click the Remove button.
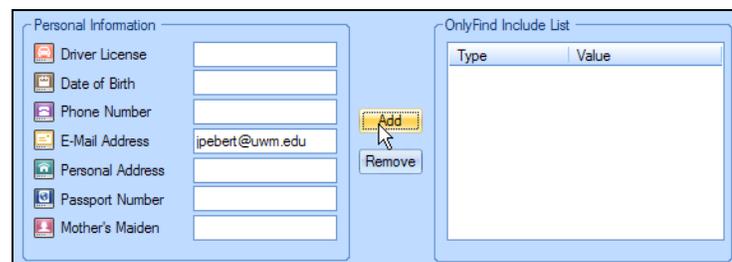
If you're unsure about formatting for any of the types of information, simply hold



your mouse cursor over the text field in question to display a popup window with entry guidelines as shown to the right.
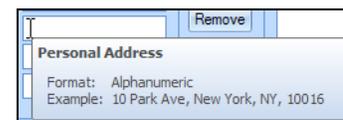
When you've finished entering the details for the personal information you'd like to locate, click the Next button to begin choosing which locations you'd like Identity Finder to search on the *Locations* window shown on the next page.

The Locations options on this screen allow you to specify the locations you'd like Identity Finder to search to find the personal information you selected earlier.

To search an additional location, simply click the appropriate check box to select it.
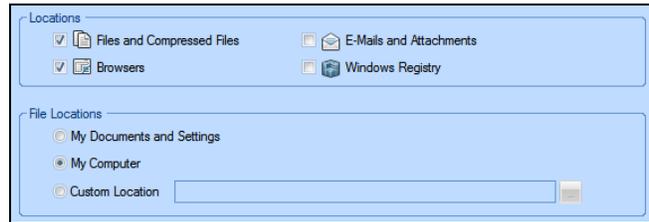
> ℹ️ LSITO recommends keeping the default search and file location options unless you want to search specific locations for files that may contain sensitive information.

Note: If the Files and Compressed Files check box is not selected on the top portion of this window, the file locations portion at the bottom of this window will be grayed out and unavailable.

When you've finished selecting the locations you'd like to search, click the Next button to continue.

The next window, shown to the right, confirms the types of information and search locations you've chosen before the search begins.

To change any of the options, simply click the Back button until you reach the screen with your desired option.
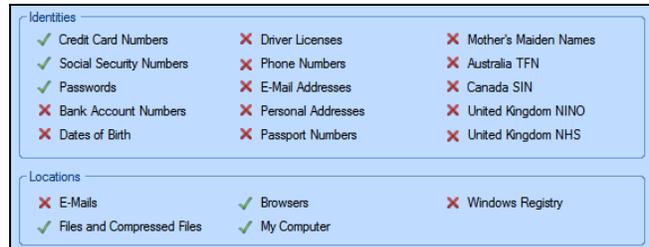
If you're satisfied with the options, click the Finish button to begin your search, which brings up the Identity Finder Status window, shown below, with the Identity Finder application window behind it:
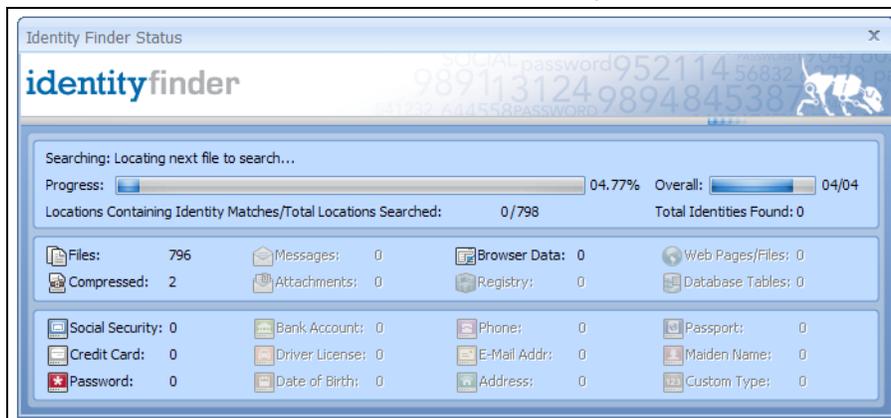
The blue progress bar near the middle of the window updates as the search progresses, while the numbers beneath indicate the number of files searched and the amount of personal information found, sorted by type.

When the search is complete, the Identity Finder Search Summary window shown to the right will appear with the total number of files searched, the number of locations which match your search criteria, and the total number of matches.

For instructions on Reviewing your Results, please turn to the next page of the guide.
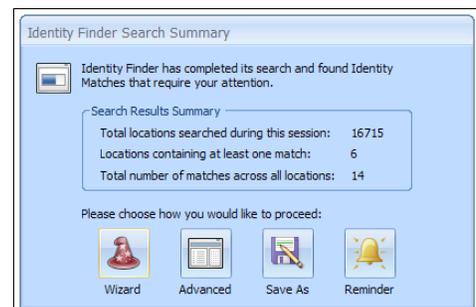
# Step 2. Reviewing your Results

As shown at the end of the previous section, the Identity Finder Search Summary window shown to the right will appear at the end of your Identity Finder search, prompting you to select how you'd like to address the results of your search.

If you'd like to begin reviewing your results at a later time, you can click the Save As button to save a copy of your results for re-opening at a later date. Alternately, clicking the Reminder button configures Identity Finder to remind you to address your search results anywhere from five minutes to a day later.
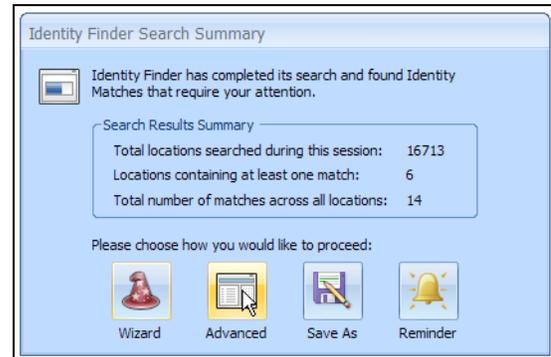
To begin reviewing your results now, click on the Advanced button as shown above to dismiss the search summary window and get your first look at the advanced interface window shown below:
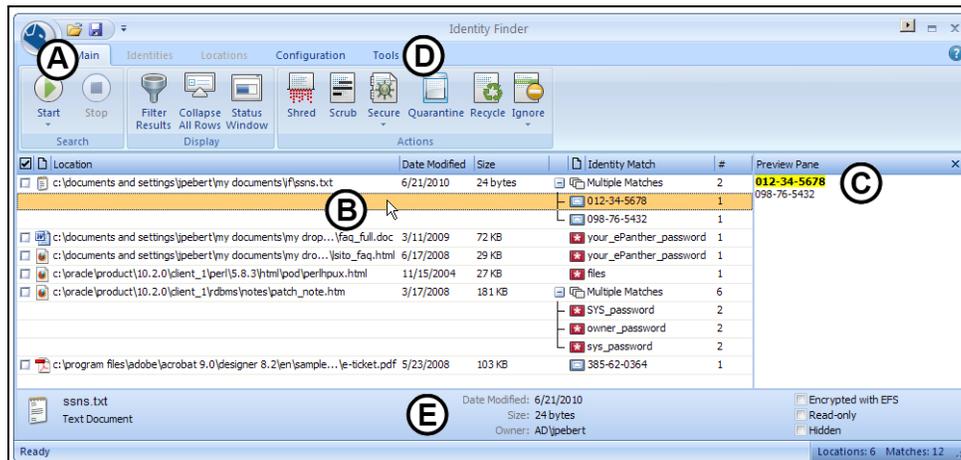
A. The Identity Finder button displays options including saving, opening, and printing results.

B. The Search Pane displays information about files identified as containing confidential data.

C. The Preview Pane shows a preview of the exact location of the confidential data within each file.

D. The interface tabs allow you change display options and select remediation methods.

E. The Properties Pane shows detailed information about files containing confidential data.

In this guide, we'll break up the process of reviewing your search results into two separate activities: identifying files that may contain confidential data using two simple questions, and then classifying these files based on the answers to those questions.

> ℹ Search results identified in the C:\RECYCLER (Windows XP) or C:\$Recycle.Bin (Windows 7) folders will appear to have incorrect filenames. While Identity Finder is not able to accurately determine the original names of these files, they will be located within your Recycle Bin folder.

## Identifying your Files

Moving away from the Results Wizard for a moment, the first step to properly classifying the files in your search results and then taking the appropriate mitigating action is to identify the origin of the file. For many of the files identified by Identity Finder, these two questions may be unnecessary, but for unknown files, ask yourself:

- Where did the file originate?

    o Did you create the file?

    o A previous owner or another user of the computer?

    o Another UWM business or departmental office?

Date Modified: 6/21/2010
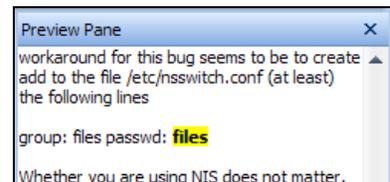Size: 24 bytes
Owner: AD\jpebert
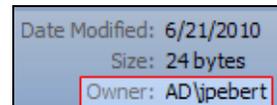
As shown to the right above, if you're unsure of a file's origin, the Properties Pane at the bottom of the Identity Finder window includes an Owner field that will show you who saved the file on your computer. In many cases, however, this field won't accurately reflect the true creator.

If you don't recognize the creator of the file from this field and you don't use this file on a regular basis, ask your supervisor for more information.

- Does the file actually contain confidential personal information?

Though Identity Finder is carefully designed to eliminate false positives, you may find search results which don't actually contain confidential personal information depending on your selected search options.

As shown to the right, the Preview Pane at the right of the Identity Finder window highlights the match within a file and provides a simple method of determining which files contain confidential information.

Preview Pane                               ✕

workaround for this bug seems to be to create
add to the file /etc/nsswitch.conf (at least)
the following lines

group: files passwd: **files**

Whether you are using NIS does not matter.

To use the Preview Pane, single click on the search result in question to display the identified match. For more information, you can consult the Properties Pane at the bottom of the window or double-click on any of the files to open them.

> ℹ  For more information about preventing false positives from showing up in future Identity Finder searches, please consult the Managing your Ignore List section on page 11 of this guide.

## Classifying your Files

After you've identified the files with confidential information that were found during the Identity Finder search, you'll need to classify each of them into three categories which dictate the appropriate remediation method. The most important factors in classifying each file are the age of the confidential information and the frequency you use the file in your day-to-day activities. For most files containing confidential information, the L&S IT Office highly recommends safeguarding your data by:

- "Securing" essential files by moving them from your computer to a secure PantherFile share
- "Scrubbing" legacy files to redact or remove unneeded confidential data
- "Shredding" unnecessary files to permanently delete confidential data

To complete the final step of the remediation process, we'll return to the advanced interface window shown on the previous page to go through the process of applying the appropriate action for each of the files you've identified as containing confidential information.

# Step 3. Safeguarding your Data

After classifying your files into the appropriate remediation categories, the first step in applying your chosen remediation method is to return to the Identity Finder advanced interface window shown below:
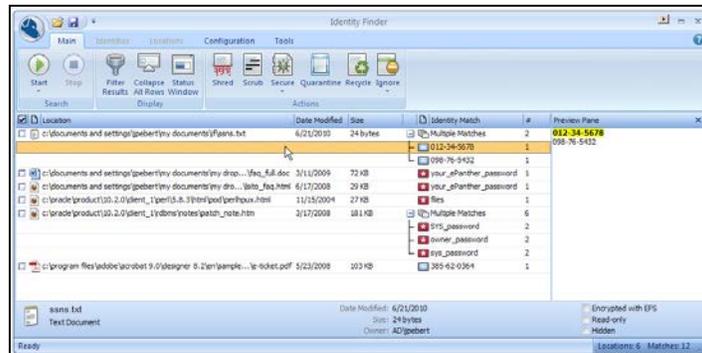


**CAUTION:** If you've chosen to search e-mails and attachments for sensitive information, you must manually delete these e-mails in your e-mail client (Outlook, Thunderbird, etc.).

Because of the way these applications store your e-mail messages, applying the "shred" or "scrub" mitigation methods below could corrupt your locally-stored e-mails.

It's also important to remember that you are only deleting the local copy of the e-mail, which will not remove the message from the server. To delete the e-mail from the UWM mail servers, you can log in to PantherLink to delete the message and then empty your Trash.

## "Securing" Essential Files

The first remediation method we'll cover is the process of "securing" a file by moving it to a PantherFile network share. This procedure assumes you have the Xythos Drive application installed on your L&S PC for ease of PantherFile access. If you're unsure if you currently have this application, check the system tray in the lower right of your screen for the following icon:



If you don't see this icon, please visit the LSITO website at http://lsito.uwm.edu/support or call the UWM Help Desk at (414)229-4040 and request the Xythos Drive application for your L&S computer.

First, right-click on the file you'd like to secure in the list of Identity Finder search results to bring up the options seen to the right. As shown, click the Open file location option to open a window displaying the contents of the folder with the file you've selected.
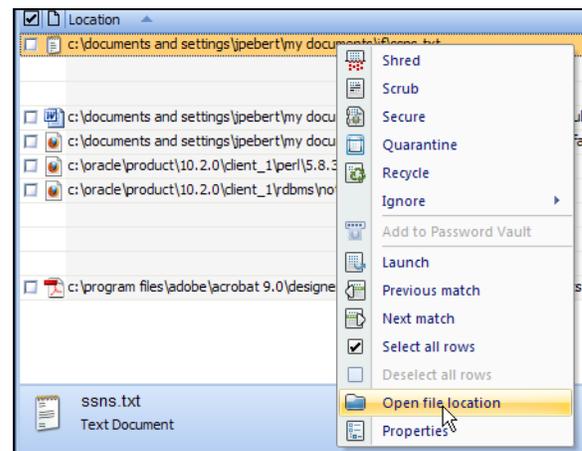
Then, double-click the My Computer icon on your desktop to display a list of drives on your computer.

Under the Network Drives subheading, you'll see the My PantherFile on 'XythosDrive' icon above. If you have the group version of the Xythos Drive application, you'll also see the L&S Group Share icon.

To open your personal PantherFile share, click the My PantherFile on 'XythosDrive' icon. Now, you should have two windows open: one displaying your PantherFile share and one with your unsecured file.

With both of these windows open, we'll be cutting your unsecured file from its current location and pasting it into your secure PantherFile share.

Note: Simply "dragging" the unsecured file to your PantherFile share or selecting the Copy option will only make an additional copy of the file and will not remove the existing file from its current location.

To fully secure your file, you'll need to remove it from your local computer with the following procedure.

As shown to the right, right-click on your unsecured file and select the Cut option.
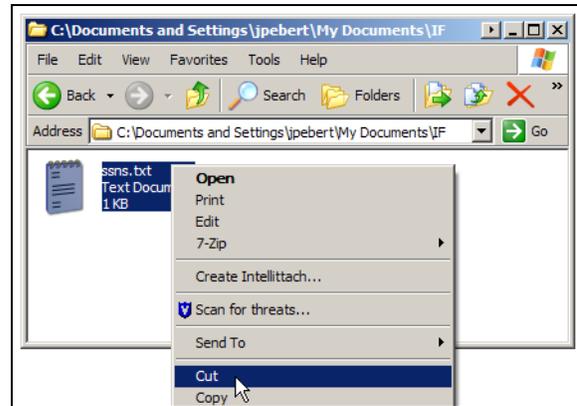


Then, in the window displaying your PantherFile share, navigate to the folder where you'd like to secure your file. In the example to the right, a new folder called 'work' was created.

As shown, right-click on the white space of this PantherFile window, then select the Paste option to secure your file on PantherFile.
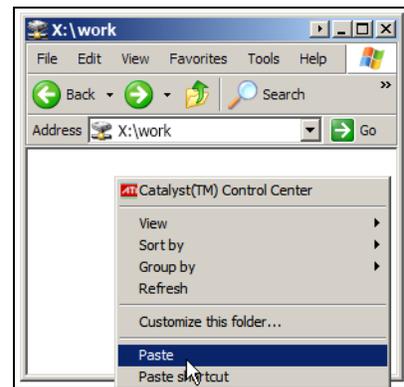


## "Scrubbing" Legacy Files

For older unsecure files, Identity Finder includes a "scrub" feature that can remove or redact unneeded confidential information. The first thing you'll need to decide is whether you'd like to redact the data down to the last four characters or completely remove the confidential information altogether.

Note: If you'd like to completely remove the information, you may skip to the next page to begin the scrubbing process. If you'd like to redact the information instead, follow the short procedure below.

First, return to the Identity Finder window and click the Identity Finder button in the upper left-hand corner, then click the Settings button to display a window with a list of advanced Identity Finder options.

As shown to the right, click to select the Actions category from the list on the left of the Settings window that appears.

Under the Options for Scrub heading, click the Scrub all characters of an identity match except for the last four check box to select it.
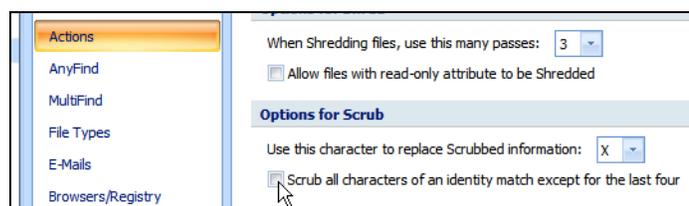


Finally, click the Apply button in the lower right of the window to save this change, and then click the OK button to close the Settings window and return to the Identity Finder main window.

First, right-click on the file you'd like to "scrub" in the list of Identity Finder search results to bring up the options seen to the right. As shown, click the Scrub option from the list of choices.
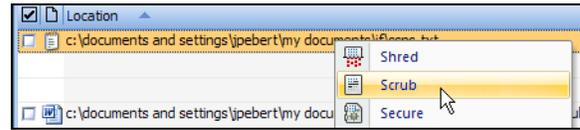
Note: You can also use the "scrub" feature on individual "matches" within each file that Identity Finder locates; make sure that you're selecting the file itself and not one of the matches within the file.
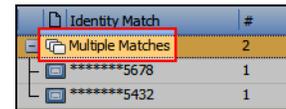
As shown to the right, the Identity Match column will indicate if there are multiple matches within the file you're "scrubbing." As highlighted in the screenshot above, make sure to select the row indicating Multiple Matches to "scrub" each individual match in the selected file.

After you choose the Scrub option, the confirmation window shown to the right will appear to ensure that you'd like to remove the confidential information from the file selected.
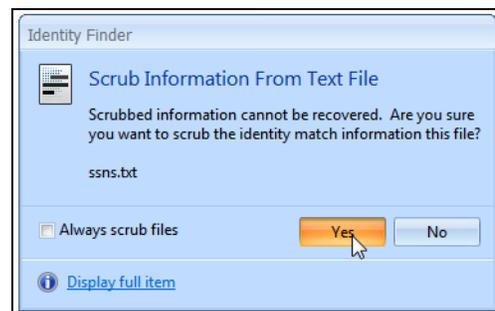
If you're sure you'd like to "scrub" the file of any confidential information, click the Yes button.

## "Shredding" Unnecessary Files

Utilizing a secure US Department of Defense deletion standard, Identity Finder's "shred" option is the most secure method of disposal for unnecessary files with confidential information.

> ⚠️ CAUTION: It is not possible to "undo" a shredding operation.
> Shredded results cannot be recovered. Once a file is shredded, it is gone.

After you've decided to "shred" your confidential information permanently, you'll need to return to the Identity Finder main window.

First, right-click on the file you'd like to "shred" in the list of Identity Finder search results to bring up the options seen to the right.
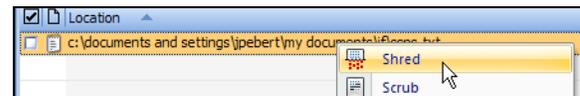
As shown, click the Shred option from the list of choices. As before, the confirmation window shown to the right appears to caution you that shredded files can never be recovered.
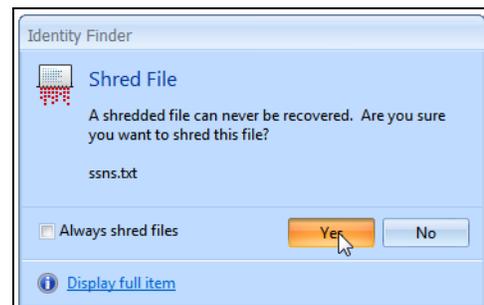
If you're certain you'd like to "shred" the contents of the file you've selected, click the Yes button.

# III. Advanced Features

## Scheduling a Recurring Identity Finder Search

In addition to real-time searches, the Identity Finder client also allows you to set up recurring searches to regularly scan your L&S PC for sensitive information.

To schedule a search, open the Identity Finder client and click the Configuration tab as shown to the right.
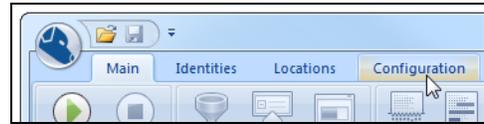
Click the Scheduling icon to bring up the Identity Finder options window, and then click the Schedule Identity Finder checkbox to begin configuring your search:

After you've selected the checkbox, the configuration options below it become accessible. To change the parameters of your scheduled Identity Finder search, click the Configure button as shown to the right.
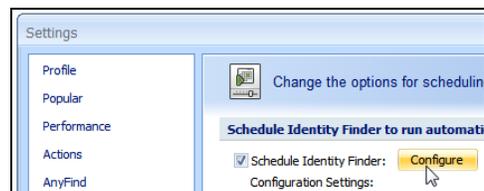
The Task Schedule window shown to the right appears, allowing you to set the time and date of your recurring search.
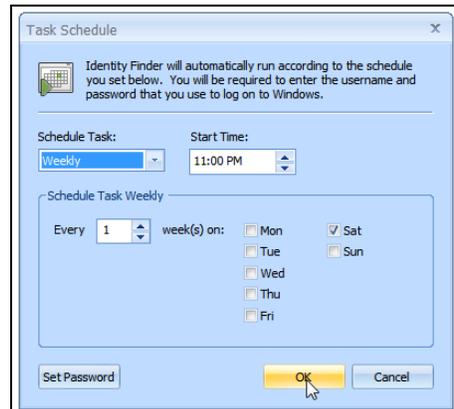
In the Schedule Task dropdown, you can select a scheduled one-time, daily, weekly, or monthly search. In addition, you can allow Identity Finder to search on system startup, login, or when the computer has been idle for a certain length of time.

Depending on your selection in this dropdown, the options may be different than those shown to the right. Select your desired search frequency, then click the OK button at the bottom of the window to close the Task Schedule window and return to the Identity Finder options window.

Under the Advanced Options heading in this window, click the checkboxes if you'd like Identity Finder to close after the search or if you'd like to save the results of the search. Select your desired options and then click the OK button at the bottom of the page to bring up a window asking for your ePantherID and password to schedule the Identity Finder task.
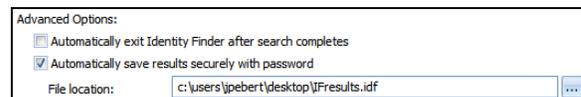
> **i** LSITO recommends that you automatically save your results and exit Indentity Finder unless you intend to schedule the search for a time when you'll be using your computer. This ensures that your results will only be accessible after entering your Identity Finder profile password.

Enter your ePantherID credentials and click the OK button to schedule your search and close the Identity Finder options window. You can now close the Identity Finder client.

When your search begins, the Identity Finder icon appears in the system tray at the lower right of your screen and the popup to the right appears to inform you that the search has begun.
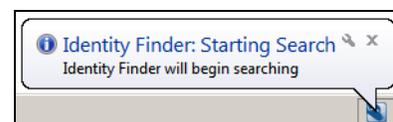
# Managing your Ignore List

If you plan to run regular Identity Finder searches, you should make use of the Ignore List, which contains false positives you have chosen to Ignore from past Identity Finder searches.

If you identify a false positive in your list of search results that doesn't contain sensitive information, simply right-click on the file or individual identity match and move your mouse cursor down to Ignore to bring up the options shown to the right.
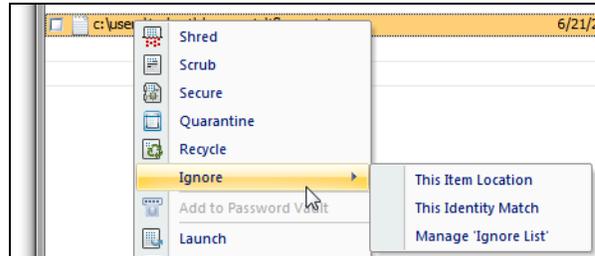
Choosing This Item Location will add the selected file and all identity matches within it to the Ignore List.  Choosing This Identity Match will only add the selected identity match to the Ignore List.   To view the items on your Ignore list, choose Manage 'Ignore List' to bring up the following window:
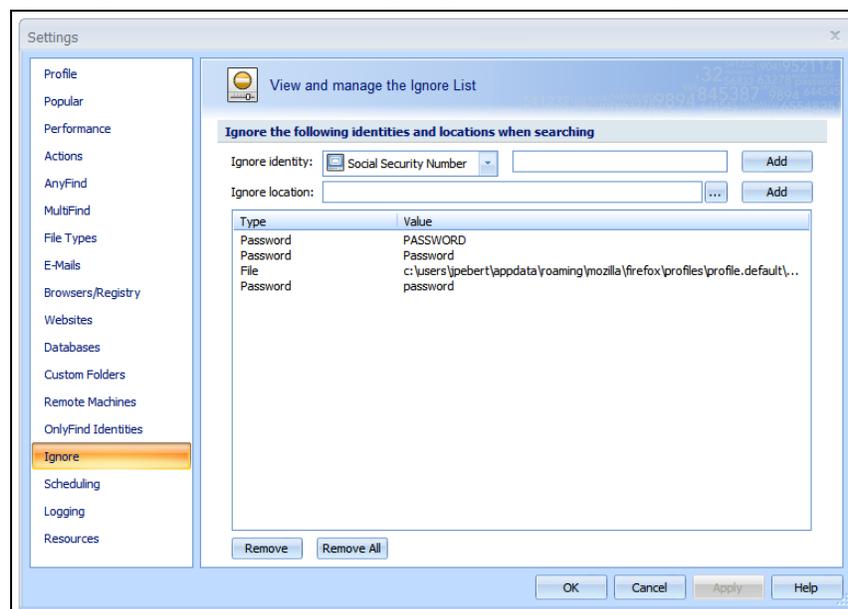
A list of ignored items appears at the right of the window, while the options above it allow you to manually add locations and specific identities to ignore in future Identity Finder searches.
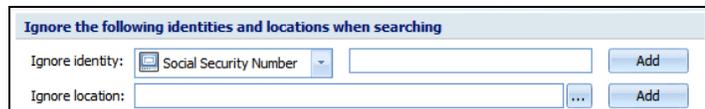
To ignore a specific piece of sensitive information, select the identity type from the dropdown list and enter the text you'd like to ignore in the text field to the right, then click the Add button.  To ignore a specific location, click the … button and browse to your desired location, then click the Add button to add the location to the Ignore List below.

To remove a single item from your Ignore List, click on the item you'd like to remove and click the Remove button at the bottom of the window.  To remove all the items from the Ignore List, click the Remove All button.  When you've finished editing your Ignore List, click the OK button to close the window and return to your search results.