

## User Guide: Sensitive Data Clean-up - Employee-initiated Scans

A major objective of the Sensitive Data Protection Initiative (SDPI) is to identify and remove all sensitive data from all desktop computers, laptops and email. The Information Security Office is coordinating the campus wide project to search for and cleanup sensitive data from each workstation. Identity Finder (IDF) is the software to be used to find sensitive data and which provides procedures to securely dispose of or protect the data. It also provides logs for tracking the search and clean-up results.

***The scope of cleaning the entire campus of all sensitive data is very large. Employees are encouraged to begin running scans as soon as possible.***

Identity Finder comes with initial campus settings for scanning your workstation which will look for Level 3 highly sensitive data that includes SSN's, Credit Card numbers and Drivers License numbers. You can do more in depth scans by changing the settings to also scan for Bank Accounts, Passwords and Passport numbers, among other things.

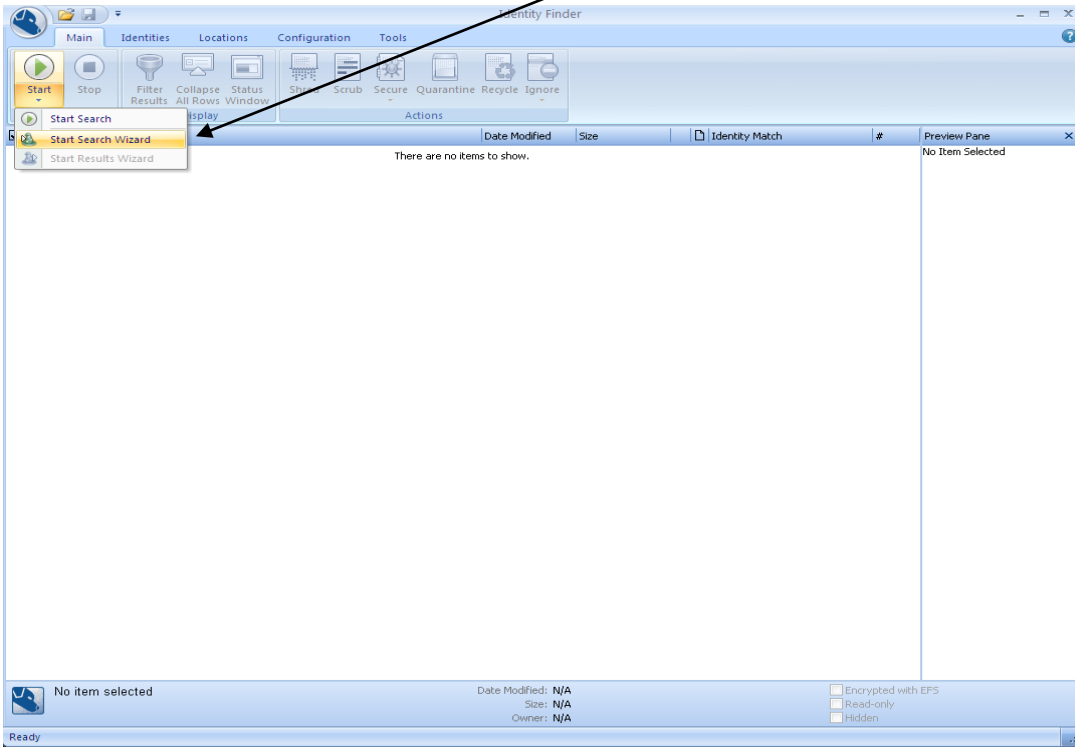
Follow this guide to run the Identity Finder software on your computer and to properly handle any sensitive information it finds. If you run into problems or have questions, contact the Information Technology Help Desk at 715-346-4357 (HELP).

### Scanning Instructions

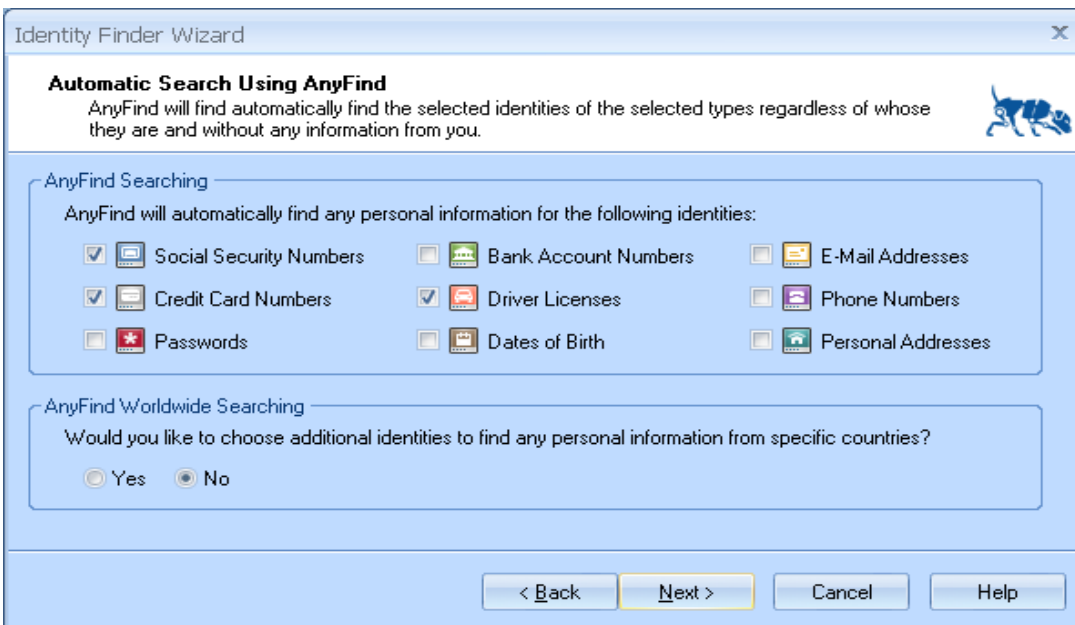
Start Identity Finder by clicking Start, All Programs and click the first choice named Identity Finder.



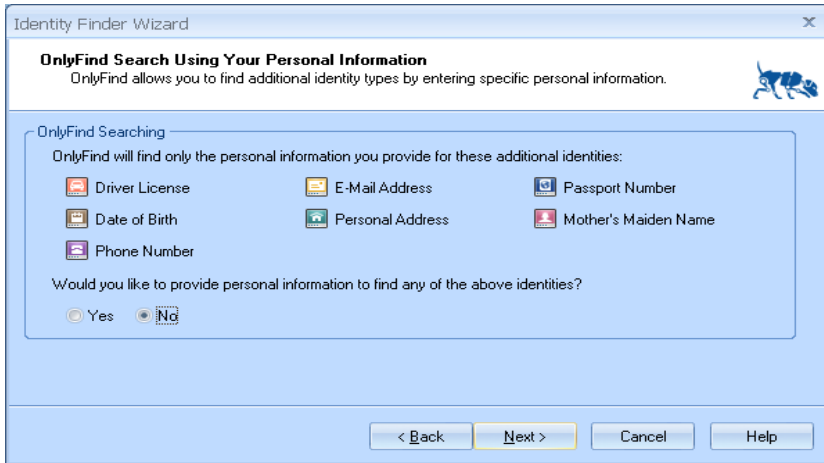
The Identity Finder Main screen will appear. To begin a search, click on the down arrow below Start, then click Start Search Wizard to begin the scan in wizard mode. We suggest always using the Wizard to start your scans because it gives you an opportunity to review your scan selections.



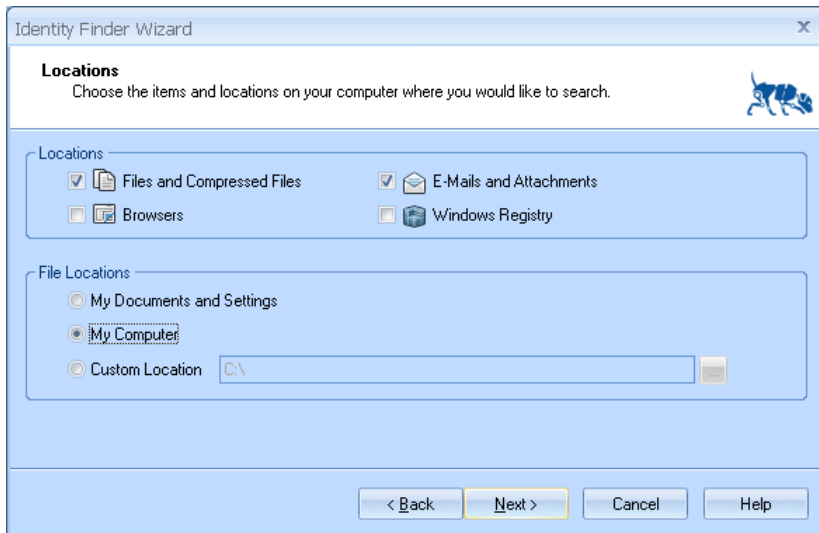
Confirm that the search is only for Social Security Numbers, Credit Card Numbers and Drivers License Number. Then click Next



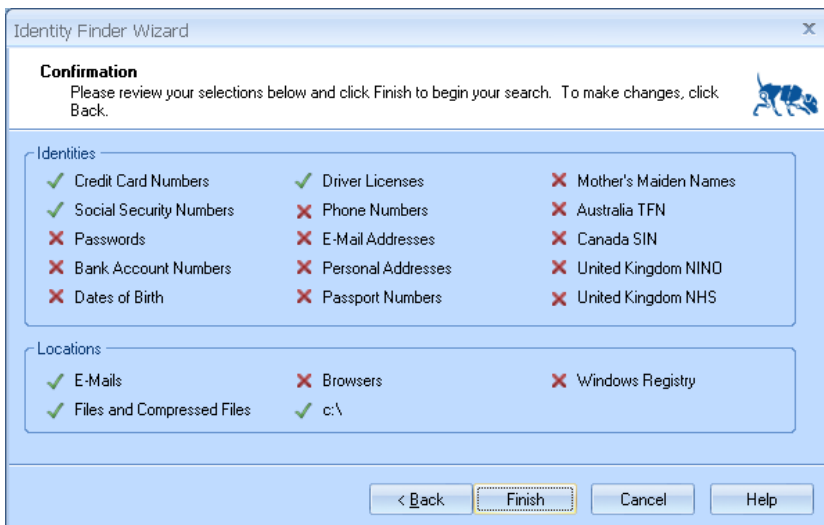
Click the No button regarding the personal information search. Then click Next.



Confirm that Files and E-mail are checked and the Custom Location is c:\. Then click Next.

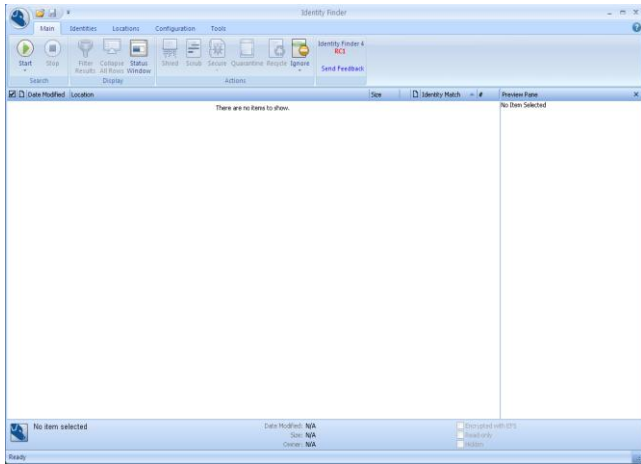


Confirm the following choices are set and click Finish to begin the search.

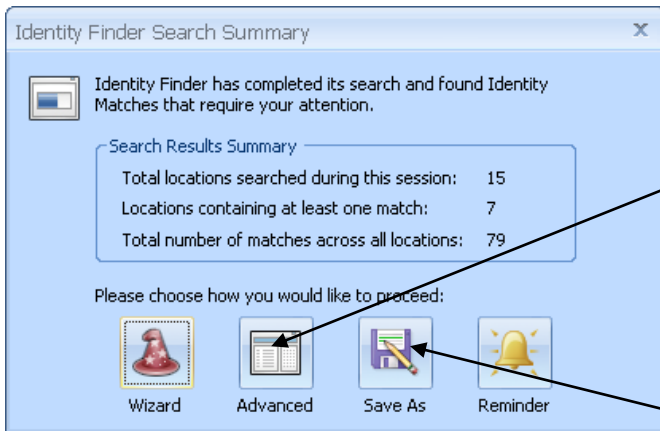


Identify Finder will search and return the results which will then be ready for your cleanup.

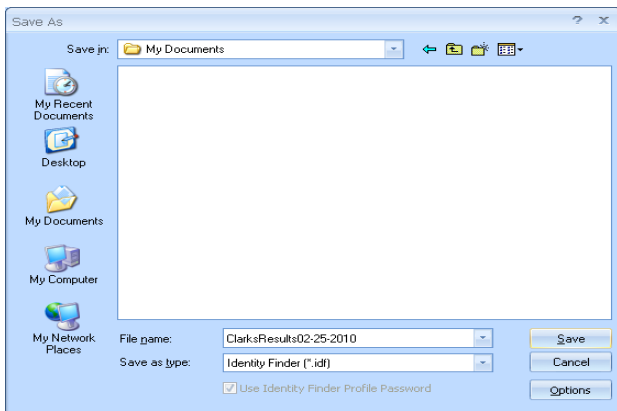
If your results window does not have any entries, ***congratulations*** your workstation does not contain any sensitive data.



If your results window does have entries, you can begin your cleanup immediately by clicking on the Advanced button or you can save your results and complete the cleanup later.

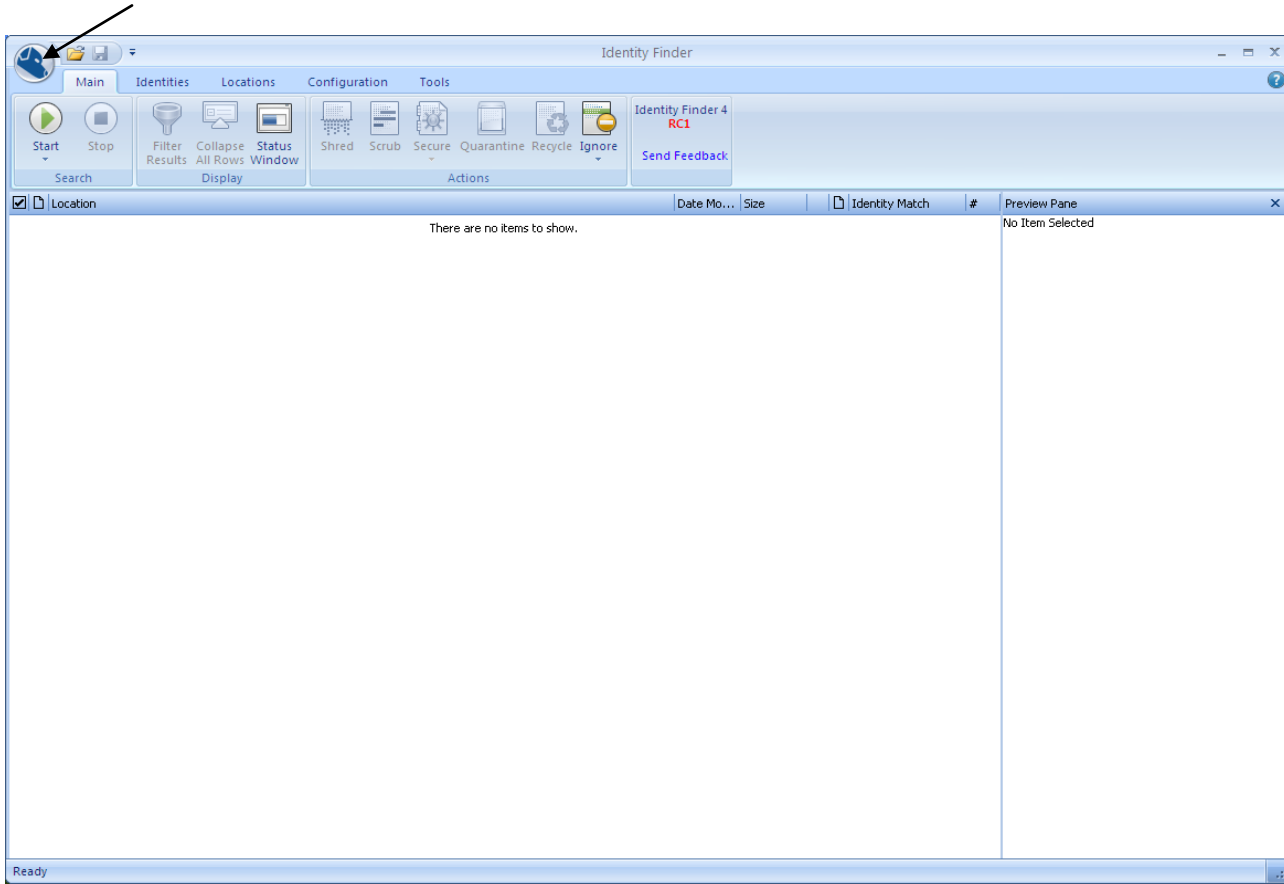


To save your scanned results and cleanup later, click the Save As button. then enter a file name (i.e. ClarksResults02-25-2010) and click the Save button. Identity Finder will save your file in the default folder My Documents, however you can save the file in any directory.

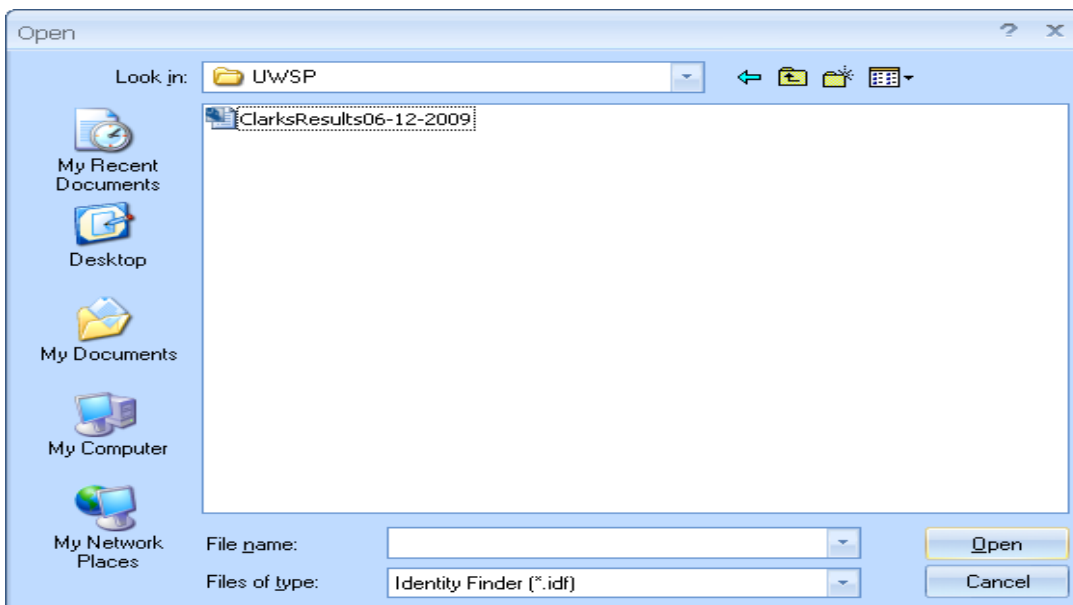


## Clean-up Instructions and Examples:

If you saved your scan results and are returning to cleanup you will need to start Identity Finder and click on the upper left dog button to open your scanning results file.



Click Open and navigate to the folder in which you saved your results file. Select your most recent results from the displayed files list and click Open.



## Remediation Actions

The recommended action is to remove any file containing sensitive data completely by using the **Shred** option. However some files such as Travel Expense Reports (TER's), grade books or others containing sensitive data cannot be removed because of record retention guidelines. For these files you should remove just the sensitive data by using the **Scrub** option. If your scan found results that are not sensitive data (called false positives), you should use the Ignore option.

Based on the Institutional Data Access and Protection Policy, Level 3 sensitive data can only be retained on your workstation if you are authorized by the Data Steward who is responsible for that data. For further clarification of this policy go to the IT Policy website at: <http://www.uwsp.edu/it/about/policies/> and view the Data Security Policies on the Faculty and Staff policies page.

If you have sensitive data you feel you need to retain, you must request permission from the appropriate Data Steward by completing a **Request for Access/Storage of Sensitive Data Form**. If the request to retain the file is approved, the file will be protected by the Information Security Office. If the request is denied, the file must be shredded. The request form is included in the appendix. The procedure to request access is explained at the IT Policy website at: <http://www.uwsp.edu/it/about/policies/>. View the Draft Policies and Procedures on the Faculty and Staff policies page and click on Procedure: Data Access Request.

The following examples show remediating SSN's but the remediation process is the same for all types of sensitive data.

**Shred** - The Shred button is located on the Main ribbon and is enabled for all types of results; 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.

## Example of Shredding a file:

Highlight the file and click the **Shred** button. You will be asked to confirm the removal. Click the Yes button. The file is now removed from your workstation as well as removed from the results list.

The screenshot shows the Identity Finder application window. The main toolbar includes buttons for Start, Stop, Filter Results, Expand All Rows, Status Window, Shred, Scrub, Secure, Quarantine, Recycle, and Ignore. A tooltip for the Shred button is visible, stating: "Shred implements the U.S. Department of Defense deletion standard, which is known as DOD 5220.22-M, for deleting files." The main pane displays a table of search results with columns for Location, Date, Size, Identity Match, and #. The file "c:\documents and settings\cpallen.uwspdom\my documents\testssnarea\addr4.txt" is selected. The status bar at the bottom indicates "Locations: 23 Matches: 1228".

| Location   | Date    | Size    | Identity Match | #  | Preview Pane                                       |
|--|---------|---------|----------------|----|--|
| c:\documents and settings\cpallen.uwspdom\my documents\testssnarea\addr3.txt                           | 6/11... | 820 ... | Multiple Ma... | 10 | Please select one of the matches in this location. |
| c:\documents and settings\cpallen.uwspdom\my documents\testssnarea\addr4.txt                           | 6/11... | 820 ... | Multiple Ma... | 10 |  |
| c:\documents and settings\cpallen.uwspdom\my documents\testssnarea\addr5.txt                           | 6/11... | 820 ... | Multiple Ma... | 10 |  |
| c:\documents and settings\cpallen.uwspdom\my documents\testssnarea\k_r3_appt.xls                       | 2/18... | 63 KB   | Multiple Ma... | 20 |  |
| c:\documents and settings\cpallen.uwspdom\my documents\testssnarea\ssnwithignore.txt                   | 6/11... | 820 ... | Multiple Ma... | 9  |  |
| c:\documents and settings\cpallen.uwspdom\my documents\testssnarea\ssnwithsecure.txt                   | 6/11... | 820 ... | Multiple Ma... | 10 |  |
| c:\documents and settings\cpallen.uwspdom\my documents\testssnarea\uwsp-work.txt                       | 2/18... | 1 KB    | Multiple Ma... | 11 |  |
| c:\documents and settings\cpallen.uwspdom\my documents\uniondues.bqy                                   | 10/6... | 84 KB   | 200309600      | 2  |  |
| c:\documents and settings\cpallen.uwspdom\my documents\apbs-lawson\briquiries\misc deductions.bqy      | 10/6... | 85 KB   | 200309600      | 4  |  |
| c:\documents and settings\cpallen.uwspdom\my documents\budget\ashistory.xls                            | 2/25... | 235 KB  | 226419468      | 1  |  |
| c:\documents and settings\cpallen.uwspdom\my documents\data\fa0828.txt                                 | 8/29... | 20 KB   | 213091845      | 1  |  |
| c:\documents and settings\cpallen.uwspdom\my documents\data\fa1129.txt                                 | 11/2... | 361 ... | 258753854      | 1  |  |
| c:\documents and settings\cpallen.uwspdom\my documents\data\ogfsp\lastsynapsys.txt                     | 11/2... | 31 KB   | 565484092      | 4  |  |
| c:\documents and settings\cpallen.uwspdom\my documents\data\ogfsp\pcard100298.txt                      | 11/2... | 30 KB   | 565484092      | 1  |  |
| c:\documents and settings\cpallen.uwspdom\my documents\data\ogfsp\pcard101698.txt                      | 11/2... | 93 KB   | 565484092      | 2  |  |
| c:\documents and settings\cpallen.uwspdom\my documents\hp maintenance quotes\hpinvent1108201.pdf       | 8/24... | 42 KB   | 264887668      | 1  |  |
| c:\documents and settings\cpallen.uwspdom\my documents\identityfinderadmin...\identityfindermanual.pdf | 8/13... | 13 MB   | 123 12 000 ... | 1  |  |
| c:\documents and settings\cpallen.uwspdom\my documents\ms-databases\msds-revise.mdb [SUBSTANC2]        | 6/9/... | 8 MB    | 647422898      | 1  |  |
| c:\documents and settings\cpallen.uwspdom\my documents\testssnarea\addr3.txt                           | 6/11... | 820 ... | Multiple Ma... | 10 |  |
| c:\documents and settings\cpallen.uwspdom\my documents\testssnarea\addr4.txt                           | 6/11... | 820 ... | Multiple Ma... | 10 |  |
| c:\documents and settings\cpallen.uwspdom\my documents\testssnarea\addr5.txt                           | 6/11... | 820 ... | Multiple Ma... | 10 |  |

The dialog box titled "Shred File" asks for confirmation to delete "addr4.txt". It includes a checkbox for "Always shred files" and "Yes" and "No" buttons. A "Display full item" link is also present.

**Shred File**

A shredded file can never be recovered. Are you sure you want to shred this file?

addr4.txt

Always shred files

[Display full item](#)

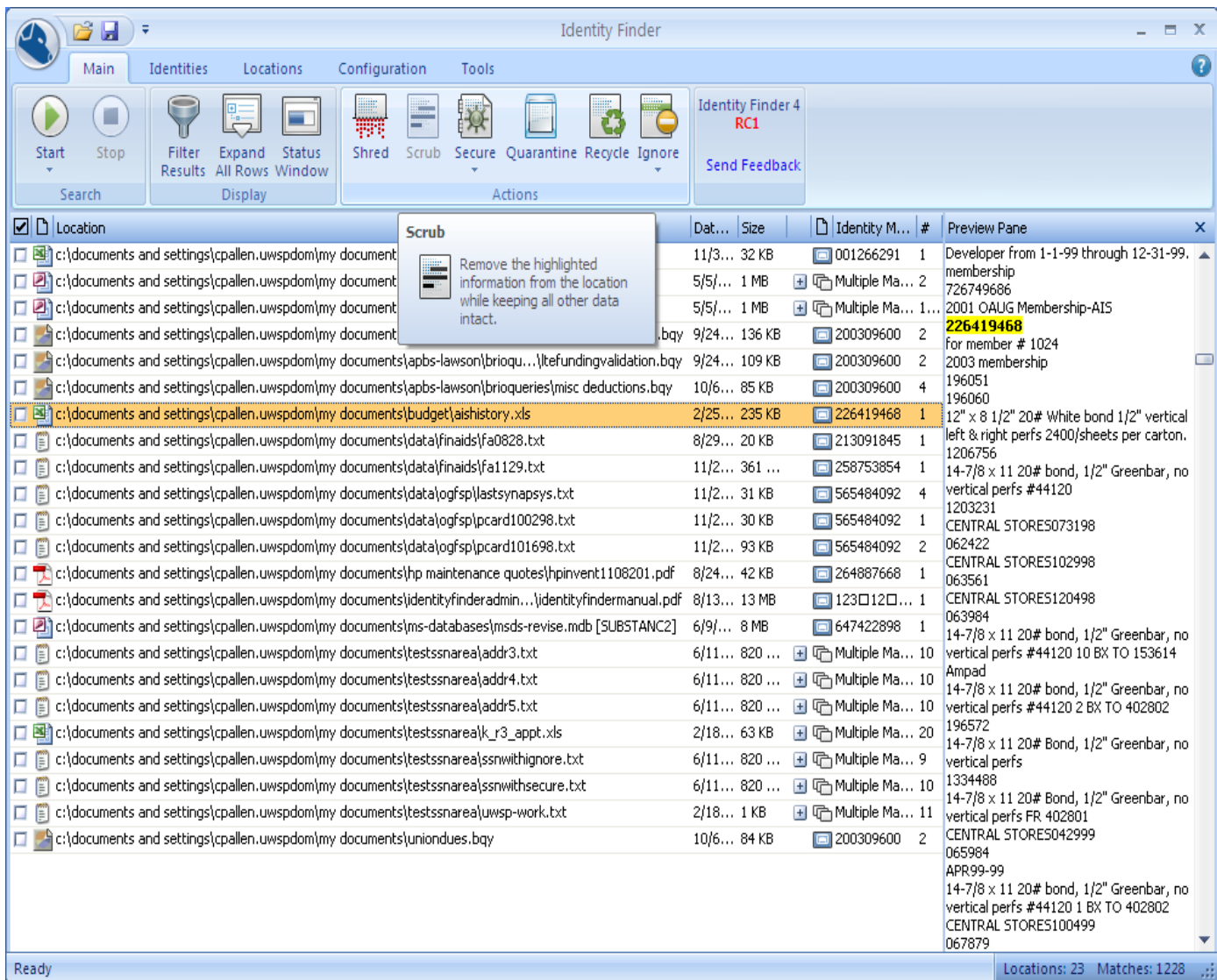
**Scrub** – For files containing sensitive data that cannot be removed you must use the Scrub feature. The scrub feature replaces the sensitive data such as social security number with “Xs” leaving all other content in place. Identity Finder only allows scrubbing sensitive data from text files and 2007 Microsoft Office 2007 files.

### Example of removing sensitive data by scrubbing a file using Identity Finder:

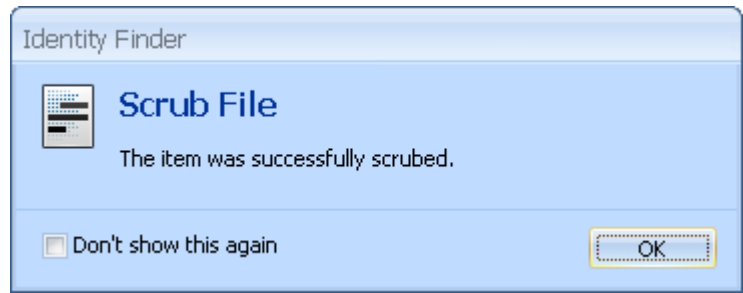
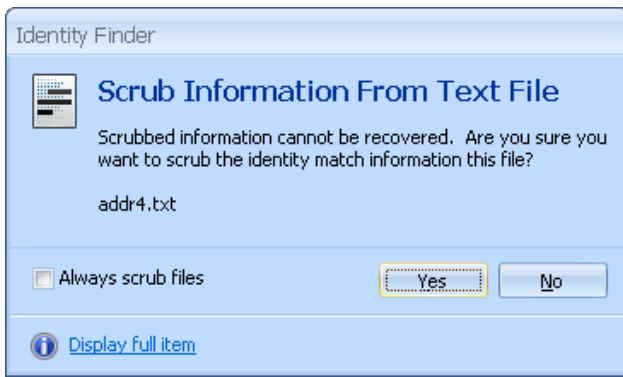
Highlight the file and click the **Scrub** button. You will be asked to confirm the scrub. Click the Yes button. The result will confirm that all SSN’s have been replaced with X’s and the file will be removed from the results list but remains on your workstation.

There are two ways to secure a single text file using the Scrub feature in Identity Finder:

- Single-click the result with the left mouse button to highlight it and click the **Scrub** 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 **Scrub**.







## Example of removing sensitive Data using other editing tools while in Identity Finder.

For other types of files especially Outlook email messages you will have to open the file using the application with which it was created by double clicking on the file while in Identity Finder.

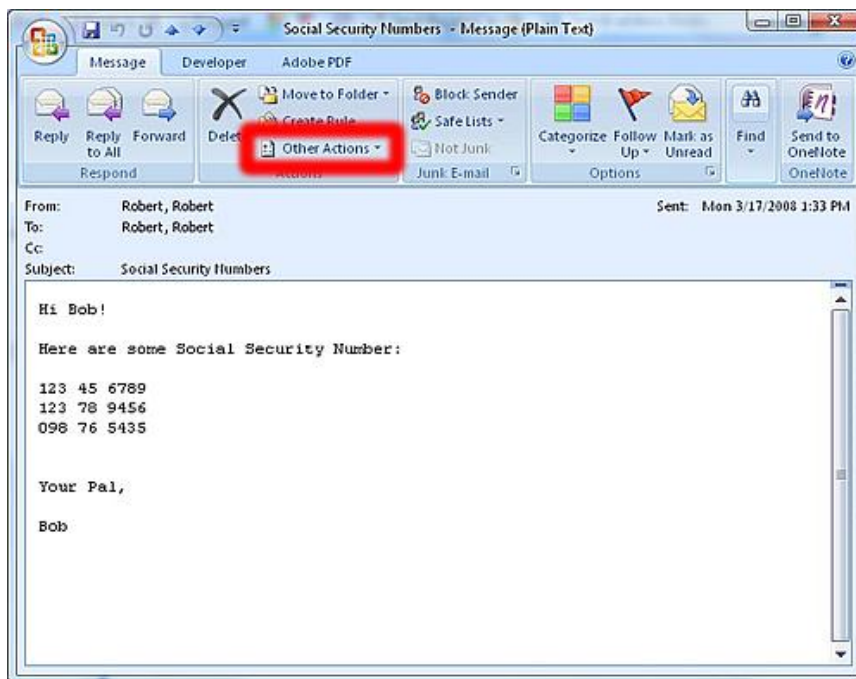
## How to Edit Email Messages to Remove Sensitive Data

You can edit e-mail messages to:

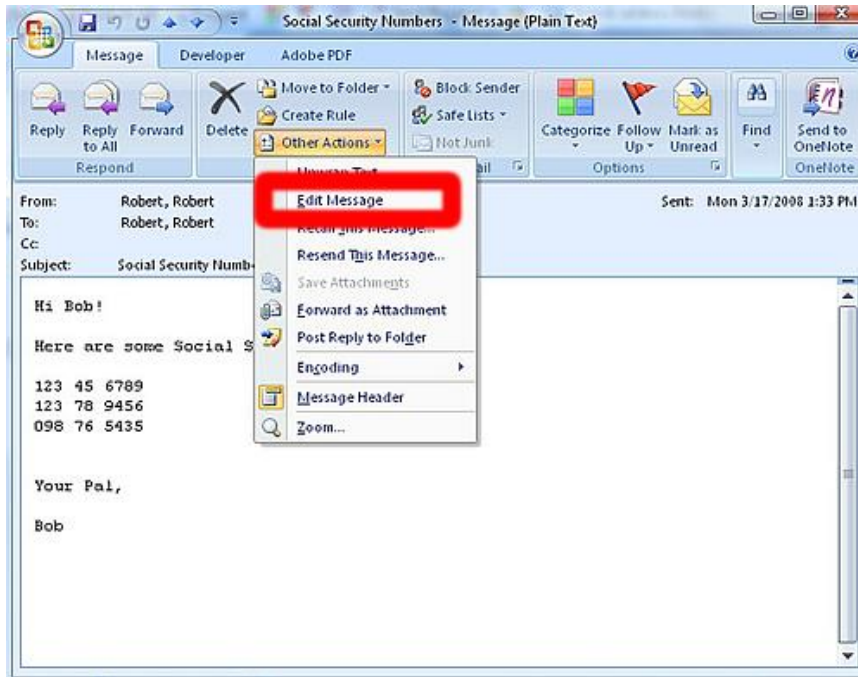
- Delete Social Security Numbers or other sensitive information from messages you have sent or received.
- Delete attachments you have sent or received that contain Social Security Numbers or other sensitive information.

To edit an e-mail message:

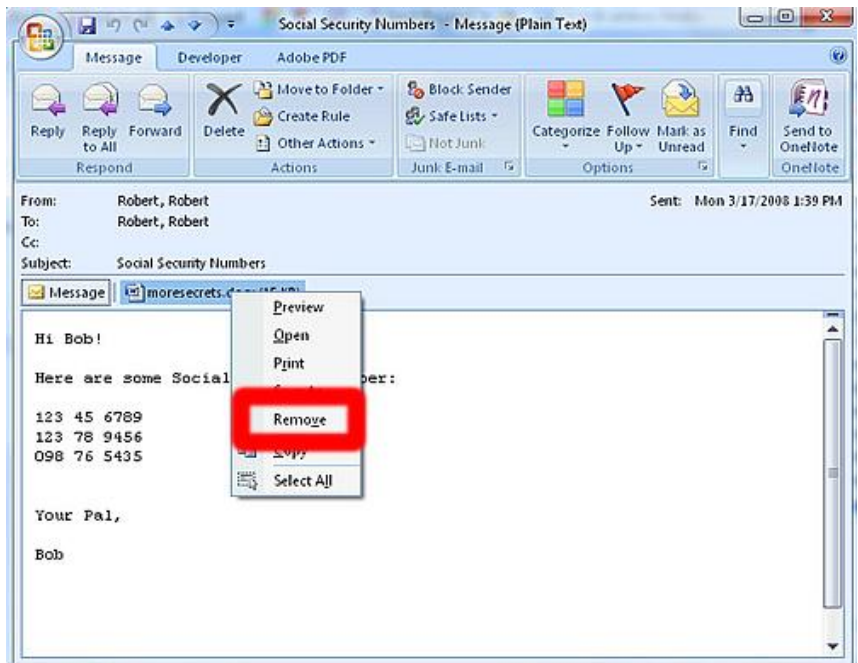
1. Open the message in your Outlook mailbox by double clicking it or open it in Identity Finder.
2. Click on **Other Actions** in the **Actions** group



3. Click on Edit Message. You will be able to edit the message and delete the SSN or other sensitive information. When you close the message, click Yes to save your changes.



4. If the message contains an attachment that you need to remove, right click on the attachment and select Remove. Save your changes when you close the message. This will delete the attachment.

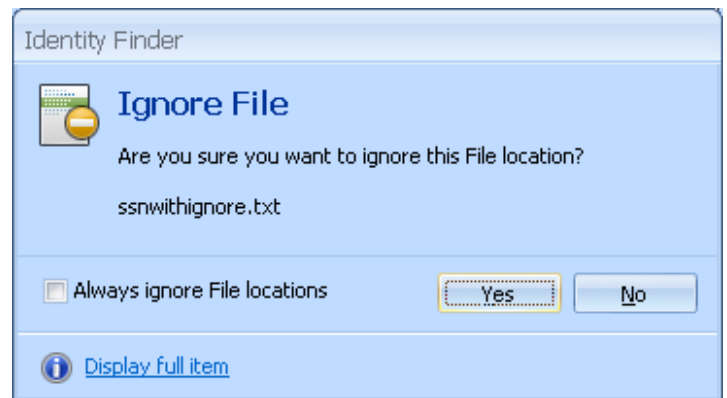
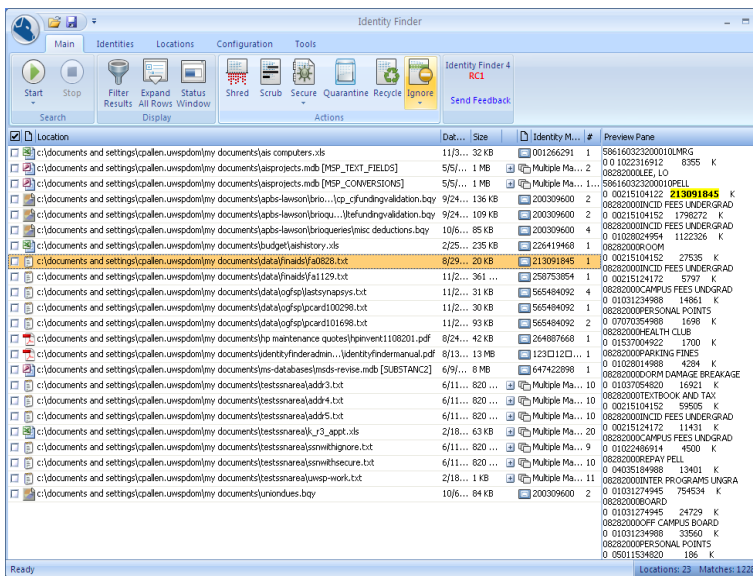


**Ignore** – Allows you to designate certain items to be ignored by Identity Finder. Only files with false positive results may be ignored. False positives are 9-digit numbers that resemble Social Security Numbers, but which are not Social Security Numbers. Identity Finder cannot differentiate a real 9-digit SSN from any other 9-digit number. Select the file to be ignored and click the **Ignore** button on the main ribbon. Choose from the following Ignore options:

- **This Item Location:** To ignore this file.
- **This Identity Match:** To ignore this Identity match(SSN) 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.

**Example of Ignoring a file:**

Highlight the file and click the Ignore button. Click the selection to ignore This Item Location. You will then be asked to confirm your ignore action. Click the Yes button. The file will be removed from the results list.



**Appendix:**



**UNIVERSITY OF WISCONSIN-STEVENS POINT**

**REQUEST FOR ACCESS/STORAGE OF SENSITIVE DATA**

|                                 |                        |
|---------------------------------|------------------------|
| <b>EMPLOYEE / STUDENT NAME:</b> | <b>DATE:</b>           |
| <b>EMPLOYEE / STUDENT ID:</b>   | <b>POSITION TITLE:</b> |
| <b>DEPARTMENT:</b>              | <b>PHONE NUMBER:</b>   |

I request approval to access or store highly sensitive data. I acknowledge my responsibility to treat this data with the utmost care and meet all of the requirements specified in the Institutional Data Access and Protection Policy available at <http://www.uwsp.edu/infosecurity/policies>.

**What type of sensitive data do you wish to access/store?**

Check only one. Complete a separate form for each data type.

- |  |   |   |
|--|---|---|
| <input type="checkbox"/> Student SSN<br>(send to Registrar)                    | <input type="checkbox"/> Employee SSN<br>(send to Personnel Director)             | <input type="checkbox"/> Credit Card Number<br>(send to Controller)           |
| <input type="checkbox"/> Financial account information<br>(send to Controller) | <input type="checkbox"/> Health information<br>(send to Health Services Director) | <input type="checkbox"/> Driver's License/ID<br>(send to InfoSecurity Office) |
| <input type="checkbox"/> Passwords<br>(send to InfoSecurity Office)            |   |   |

**Describe why you wish to retain or access sensitive data (i.e. purpose):**

**Describe where this sensitive data will be located (i.e. laptop, network drive, desktop, file cabinet, etc.):**

**Describe the department or unit that this sensitive data originated from (if known). List any other departments or units with whom you are sharing this information.**

**Department Head Signature:**

I certify that the requestor needs this access to do their job and the information on this request is accurate.

*FOR DATA STEWARD USE ONLY*

|  |  |
|--|--|
| <input type="checkbox"/> <b>APPROVED DATE:</b> | <input type="checkbox"/> <b>NOT APPROVED DATE:</b> |
| <b>ACCESS GRANTED UNTIL:</b>                   | <b>REASON FOR NON-APPROVAL:</b>                    |
| <b>DATA STEWARD SIGNATURE:</b>                 |  |