SACRAMENTO STATE
INFORMATION RESOURCES & TECHNOLOGY

identityfinder

What is Identity Finder?

Identity Finder is a program that locates Protected Level 1 data in files. Identify Finder is installed on most University-owned/managed computers, and can be installed if it is not present.

To protect Protected Level 1 data, and comply with CSU Policy 8065.0, the IRT Information Security Office encourages the use of Identity Finder (also known as Spirion) to remove and reduce the files or documents that contain confidential information, and/or ensure they are stored in proper location. Please see csus.edu/filesecurity for storage and sharing information.

Identity Finder can perform actions on locations that contain Protected Level 1 data, including the ability to delete (Shred), redact (Quarantine).

What Does Identity Finder Search?

The types of files that Identity Finder searches for are Microsoft (Word, Excel, Access, PowerPoint, etc.) Adobe (PDF), text files, web files and other common file types.

The Confidential Level 1 Data it looks for includes:

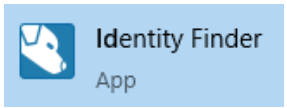
- Social Security Numbers
- Credit Card Numbers
- Passwords
- Bank Account Numbers
- Driver License Numbers
- Dates of Birth

Running a Scan in Identity Finder

Identify Finder is supported on both Windows PC and Mac.

Windows PC

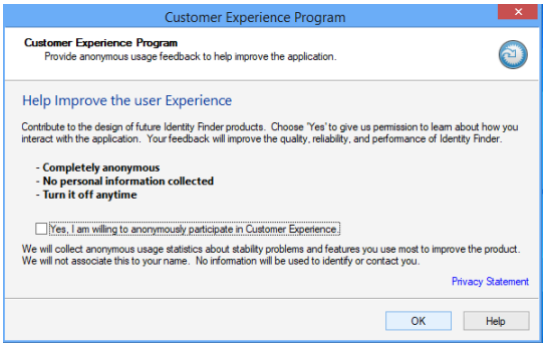
1. In the Windows search bar, type **Identity Finder**.
2. The Identity Finder App should appear.
3. Click the **Identify Finder** icon.



Mac

1. Click the **Application Folder.**
2. Click the **Identity Finder** icon.

When you run Identity Finder for the first time, you will be prompted to participate in an Identity Finder Customer Experience Program. Feel free to decline this and uncheck the box *"Yes, I am willing to anonymously participate in Customer Experience."* Click the **OK** button to continue.



Creating your Identity Finder Profile

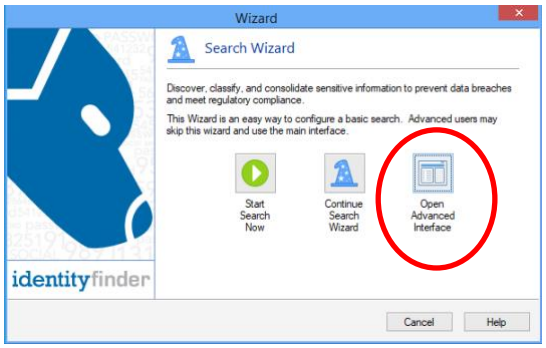
When you first launch the Identity Finder application, you will be prompted to create a profile password. You will need to remember this password in order to access your saved searches in the future (including results marked as false-positives).

Note: Profile passwords cannot be recovered. In the event that a profile password is lost, the existing profile must be replaced with a new profile; meaning that previous scan results will be lost.

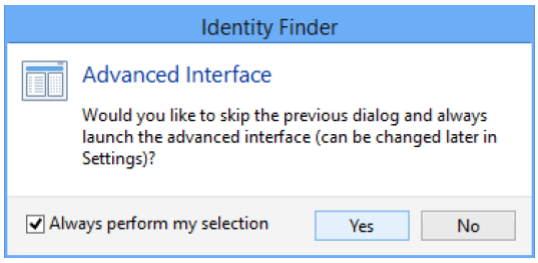
Starting a Search

If this is your first time running Identity Finder, it will start the Wizard. The Wizard is **not** recommended because it can take much longer to run a scan. Choose **Open Advanced Interface**.

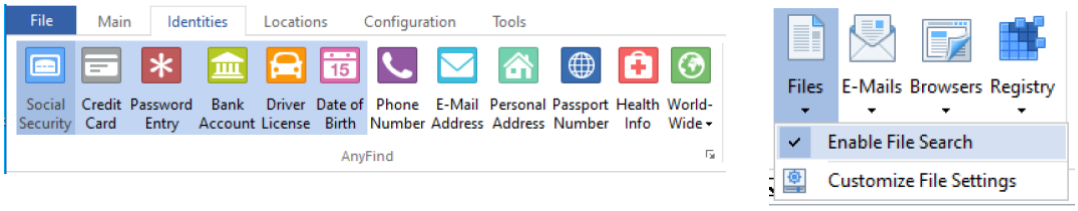
1. If the Wizard was displayed and you chose **Open Advanced Interface,** choose the **Always perform my selection** option and click **Yes** to skip the previous dialog so that it always runs the **Advanced Interface** instead of the Wizard.



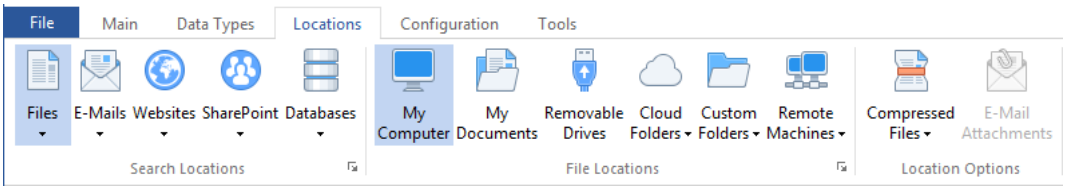
2. After the Identity Finder client launches and before starting a new search, choose **Identities** from the ribbon and select **Social Security**, **Credit Card**, **Password Entry**, **Bank Account**, **Driver License**, and **Date of Birth**.



3. Choose **Locations** from the top ribbon, then choose **Files** and **Enable File Search.**

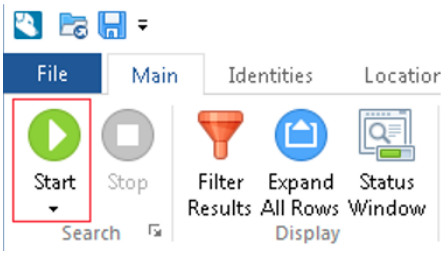


4. Next select **My Computer**.



5. Initiate the scan by clicking on the Main tab and choosing **Start** then **Start Search Now** button. By default, this search will scan the contents of your local computer.

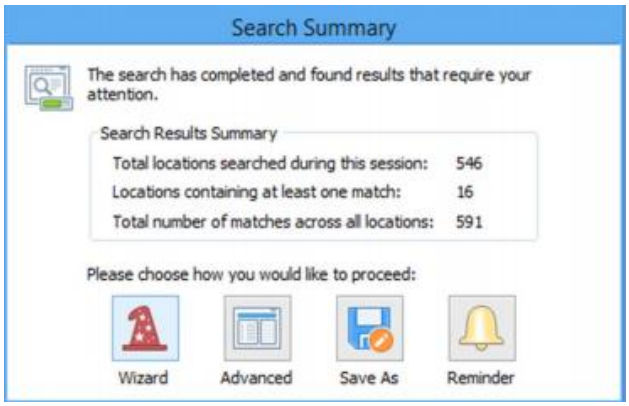
> **Note:** *Running a search on any system for the first time can take several hours. You can continue to work while Identity Finder searches your computer, but it may slow your computer's performance. You may prefer to begin the scan at the end of the day and allow it run overnight. Lock your screen (Windows Key + L) while the scan is running, and while you are away from your computer.*



6. A **Status** window will display to show the current progress of the scan.

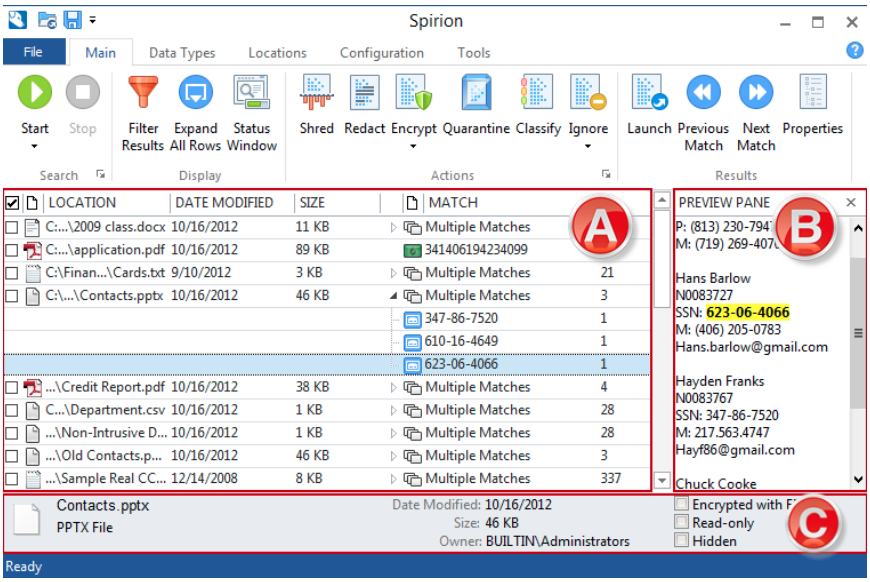
Viewing Search Results

1. Once Identity Finder has completed searching your computer for protected data, it will display a **Search Summary** screen, where you can view the number of matches found. Choose **Advanced:**

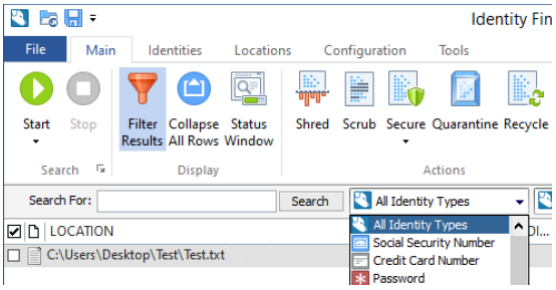


You will see the following:

A. **Results Pane**
Details each item
B. **Preview Pane**
C. **Properties Pane**
Provides all of the relevant information about each item including the location, type and value of the result.



2. Look for the following in your search results:
   - Social Security Numbers
   - Credit Card Numbers
   - Bank Account Numbers
   - Driver License Numbers
   - Dates of Birth



Notes: *Identity Finder may find results that contain data in a pattern similar to Level 1 data but are not. For example, it may flag a nine-digit Campus ID Number. These are called "false positives" and will need to have action taken for these items (once selected) by choosing* ***Ignore. (****See* ***"Taking Action on the Results"*** *section below****)***

When no results are found, this is generally a good sign, but it does not guarantee that your computer does not contain protected data. It simply means that the search patterns used by Identity Finder did not find any results. You are still responsible for protecting Level 1 data.

Filtering Your Results

Once you have the search results, you can filter them by identity type, location type, or both. Click the **Filter Results** button on the ribbon.

1. To filter by identity type, click on the drop-down menu that says **All Identity Types**.
2. From the drop-down menu, you can filter by identity type.
3. To filter by location, click on the drop-down that displays **All Location Types**.
4. From the drop-down menu, you can filter by location type.

Taking Action on Your Results

You'll need to review and take action on each item that Identity Finder finds on your computer. Though this may be time consuming, leaving this data on your computer puts yourself and others at risk. Once you have reviewed the search results, subsequent searches will go quickly and will likely have fewer, if any, results.

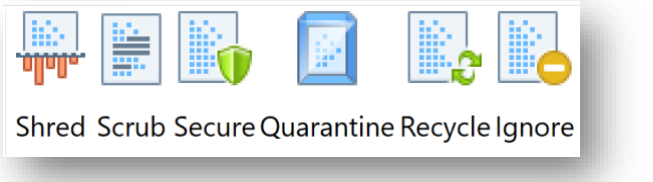
1. Examine an item in Identity Finder, click on the line for the item in the **Results Pane**.
   The **Results Pane** shows the following information:

   - File type icon (Word, Excel, PDF, email, etc.)
   - Location of the file on your computer
   - Date the file was last modified
   - File size (in KB)
   - Identity Type Icon (VISA, Mastercard, SSN, bank account, etc.)
   - Identity Match (the actual protected information found)

2. Once you have selected an item, you can see the protected information in context in the **Preview Pane**. This will give you more information about the protected data. You can also view more information about the file containing the protected data in the **Properties Pane**.

3. Choose a file and then apply one of the following actions for each file:

   - **Shred:** Click the **shred** button on the ribbon to delete the file containing protected information. This action is permanent and cannot be undone.



   - **Scrub:** Use the **scrub** button to remove the protected information from the file and leave the file in place. **Note**: *Scrub is only available for specific file types, including Word, Excel, and text files. Scrub is not available for Email, PDF, or other file types. If the button is grayed out, that means it is not available to use for that file.*

   - **Secure:** Do <u>not</u> use this option for Level 1 Data, instead **Shred** or move the file. You can secure a file with a password with the **Secure** option; however, if the file contains Level 1 Data, it will need to be deleted via the **Shred** option or moved to a secure file storage location.

   - **Recycle:** Do <u>not</u> use this option for Level 1 Data. This option moves the file to your computer's Recycle Bin. Instead use the **Shred** option to properly delete the file.

   - **Ignore:** Click the **Ignore** button and then **This Item Location** to ignore the file in future searches. Choose **This Identity Match** to ignore the particular finding in the file from all file locations in subsequent searches. The file will remain intact for either choice. Remember to use these ignore options for <u>all</u> false positives. **Note:** *You can use the **Manage 'Ignore List'** option to add or remove data to ignore.*

   - **Quarantine:** Use the **Quarantine** button to allow you to move the file to a secure location (e.g., SacFiles Secure). **Note:** Quarantine is not available for all file types, particularly emails. If the Quarantine button is grayed out, it means that the Quarantine action cannot be applied to the file.
     - You will be asked to select a location to move the file to.
       Click on the "..." button in order to choose a location.
     - Make sure to select a secure location, such as a SacFiles Secure folder,
       to ensure that your file is securely stored.

Finishing Up

Once all results found following an Identity Finder search have had action taken, and there are no more results displayed within the **Results** pane (which includes no longer displaying ignored false positive matches), the Identity Finder application may be closed.

If prompted, be sure to choose **Save Results** to ensure search history from this search is saved. Some choices are saved automatically.

Technical Support

- Bookmark csus.edu/filesecurity for recommendations on proper storage and sharing options for files containing sensitive data.

- Need assistance running or managing Identity Finder search results? Contact the IRT Service Desk Team at servicedesk@csus.edu or 916-278-7337.

Thank you for supporting these critical campus information security efforts!