CLARK UNIVERSITY
1887
CHALLENGE CONVENTION
CHANGE OUR WORLD™

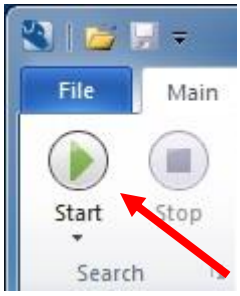
INFORMATION
TECHNOLOGY SERVICES

Help Document Series: Identity Finder Scanning Guide

Instructions on how to use Identity Finder to scan your computer and work with the found files.

Scanning

1. Use the following icon on your Desktop to launch **Identity Finder** (also found under **Start->All Programs->Identity Finder->Identity Finder**)
2. Once the program starts, you will be prompted to enter and confirm a password to save settings from your search; click the **Skip** button, as this step is not needed.
3. A new window, **Identity Finder Guest Profile**, will open and you can click **OK**. The program might check for updates and ask to install them. Let the updates install and click **OK** to continue.
4. Now that Identity Finder is open, you are ready to begin a scan, and should be aware of what will happen:
    a. Scans can take as little as 10 minutes to complete or many hours (typical scans are less than an hour)
    b. If you **Close** the program or **Log off** your computer, your scan results will be lost, forcing you to restart a scan
    c. If you want leave your computer unattended during a scan, **Lock** your computer first to prevent others from seeing your results; any sensitive information found will be seen in the Identity Finder window



5. Click the **Start** button to initiate a scan. The application may ask you to close other applications before it will initiate the scan (e.g., certain web browsers).
6. The scan has been set up to look for the following types of confidential information: passwords, social security numbers, credit card numbers and financial account numbers

Before reviewing the files and content found by Identify Finder, we recommend that you review the Clark's Data Security Policy (http://www.clarku.edu/policies/detailpolicy.cfm?pid=7) along with the Data Classification Policy, within the Data Security Policy.

Data Clean-up

Once the scan is finished, you will be presented with a window containing a list of all files found that could contain the defined confidential information. Not all of these files will have sensitive information, some will contain data that was falsely identified (a false positive).

The easiest way to determine if a file truly contains confidential information, or if it just contains a false positive, is to click on the file name and view the contents of the file in the **Preview Pane** (on the right side of the window). The **Preview Pane** will show you a preview of the file, with the suspected match highlighted. By viewing the file, you should be able to determine if the result is truly a defined confidential data type that needs to be addressed, or if it is a false positive.

(Continued on page 2)

A false positive could be things like ISBN numbers, FedEx account numbers, zip codes; or it could be a random string of numbers that appear in the background code of the file. If you cannot determine the true status of suspected data result, you can double click on the file name to open the file and look through it.

If you determine the file contains any of the following confidential information (passwords, social security numbers, credit card numbers and financial account numbers), please contact your department head/chair to confirm that you need to store the information and then the ITS Help Desk to go about the process of moving the needed files to an ITS managed server. It is against Clark's data security policy to have any these data types on a non-ITS managed server:

Processing the files found by Identity Finder

If your scan finds files that contain the defined confidential data types that should not be on your computer and you no longer need those files, you can proceed with one of the following options:

Option 1: Shred the file

This is the safest option; it will delete the file and ensure that the confidential information is unrecoverable if your computer were to be compromised. If you no longer need the file, please **Shred** it.

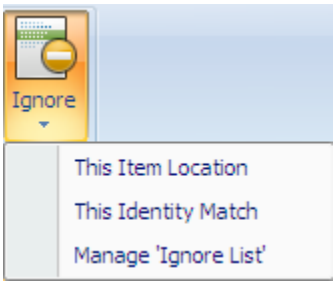
- To **Shred** the files, select only the files you want shredded and click the **Shred** button in the top bar of the window of Identity Finder.
- You will be asked if you still want to shred that file, click the **Yes** button to finish the process, and the **OK** button to acknowledge that the file has been shredded.

Option 2: Clean the file

This is the manual process of removing the sensitive information from an editable file. Only use this option if it is necessary to retain the rest of the data in the document.

- To clean the file, double click it to open it in a program that can edit the document.
- Delete the sensitive data from the file.
- Choose **File->Save As** from the menu and rename the file to indicate that the sensitive data was removed. We recommend that you use a file name such as "OriginalFileName_clean" so that you can easily tell which files have been cleaned.
- Return to Identity Finder and **Shred** the original file.

If the file DOES NOT contain confidential data, you can Ignore or Skip the file.



1. **Ignore** the file. The program will remember this file in the future, so it will not show up the next time you scan your computer.
   - To **Ignore** the file, click on the file name and click the **Ignore** button at the top of the window.
   - In the drop-down list that appears, choose the first option: **This Item Location**
2. Skip the file. If you choose to simply skip over the file, it will still show up in subsequent scans.
   - To skip the file; simply move on to the next file in the list.

When you are finished with all the files in the list, you are done with the clean-up! Simply click the **X** button to close the window.