What is DLP?

Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework.

Data Classification Types

Level 1 (PII) Confidential	Data governed by existing law or statute. ♦ Personally Identifiable Information (PII) ♦ Social Security Number ♦ Credit Card Number ♦ Driver License Number ♦ Personal Health Information (ePHI)
Level 2 Internal	Information that must be protected because of ethical or privacy concerns, such as grades, or disciplinary actions. ♦ FERPA Information ♦ Employee Data
Level 3 General	Information such as title, email address, or other directory information that is freely available in the public domain. ♦ FERPA/EE Directory Information

View the Data Classification Policy at: http://policy.csuci.edu/IT/01/it-01-002.htm

California State University | Information Security Channel Islands

identityfinder

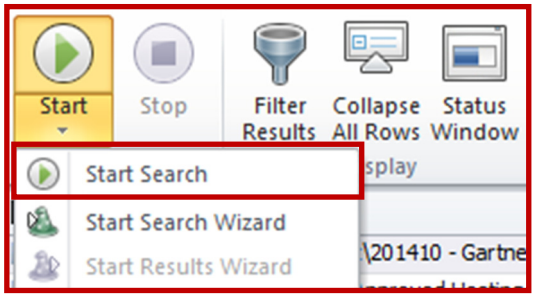
Scanning and Reference Guide

Neal Fisch
Information Security Officer
California State University Channel Islands

One University Drive
Solano Hall 2178
Camarillo, CA 93012
infosec@csuci.edu

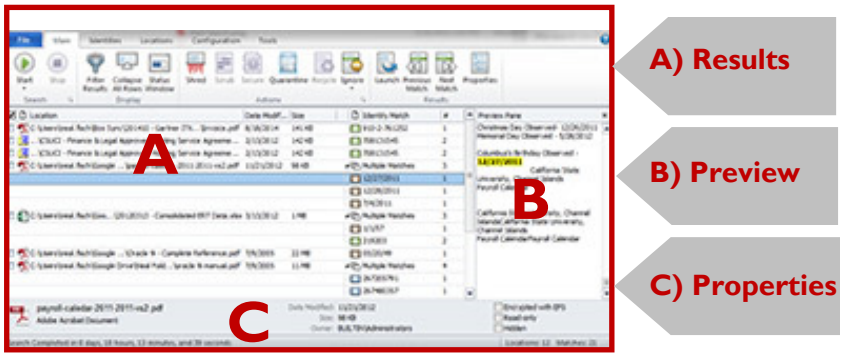
Step 1 **Start** a Search/Scan

To begin a search/scan click the Start button on the Main ribbon (tab) and then click "Start Search".



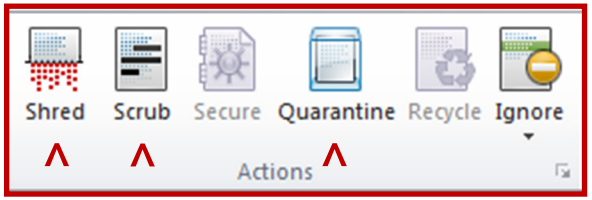
Step 2 **View** Search Results

View provides all of the relevant information about results including the location, type, and value of the search results, a preview of the search results in context, and other details.



Step 3 **Shred, Scrub, Quarantine** - Removing PII

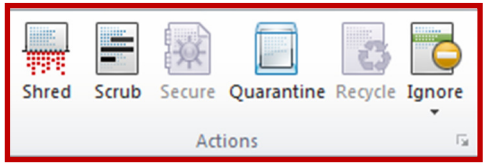
Shred files when they contain personal information that you no longer require. Scrub files when you have a sensitive identity match and want to keep the file but remove the sensitive data. Scrub is also known as Redact. Quarantine will move your file to a new secure location and then Shred the original so it cannot be recovered from the original location.



Additional Information on Actions: *http://www.identityfinder.com/help/client_win/index.htm#ProtectingPersonalInformation.htm*

Step 4 **Ignore** Search Results

Ignore prevents information from being displayed in the future. For example, IDF may discover a sample credit card number inside a temporary internet file or show false positives. If marked, IDF will ignore those matches for current and future searched.



Step 5 **Save** Your Results

Save your IDF search results in a password protected file so you may retrieve and continue to work with your results at any time.