Overview: Identity Finder at WCSU

What is purpose of today’s training?

- Overview of Information Security

- Introduction to the Identity Finder software client:
  - Quick overview presentation
  - In-depth explanation of the client

Information Security Overview

- Key points from the Information Security and Data Management Awareness seminar are:
  - Employees are responsible to protect data from unauthorized disclosure, corruption or loss and ensuring they maintain data in compliance with record retention requirements
  - Policies are defined for data stewardship, classification, storage and retention
  - One of the technical safeguards implemented to aid users is to use a program called Identity Finder

What is Identity Finder?

- Identity Finder is a program that locates sensitive data (i.e. SSN, credit card numbers) in files (i.e. Word, Excel, PDF) or email messages.

- In addition to locating sensitive data, Identity Finder can perform actions (shred, quarantine, scrub) on locations that contain sensitive data

- The actions performed on locations that contain sensitive data must be in compliance with Record Retention requirements

Who has to run Identity Finder?

- All employees with potential access to DCL3 data will need to run Identity Finder to ensure DCL3 data is stored only in **approved** locations and on **approved** equipment or storage facilities.

- DCL3 data is defined as *protected confidential data, which comprises identity and financial data that, if improperly disclosed, could be used for identity theft or to cause financial harm to an individual or the institution including:*
  - Social Security Numbers
  - Credit Card Numbers
  - Bank Account Information
  - Driver's License Numbers

What does it search?

- When you configure a search, you need to tell it:

1. **What type of data you are looking for:**

   Social Security Numbers, Credit Card Numbers, Bank Accounts and Driver's Licenses

2. **What type of files you are looking in:**

   Files – Searches Microsoft (Word, Excel, Access, Powerpoint, etc), Adobe (PDF), text files, web files and other common file types. Searches compressed files too.

   Email – Exchange mailbox including attachments, Outlook profile, .pst files

What does it search? (continued)

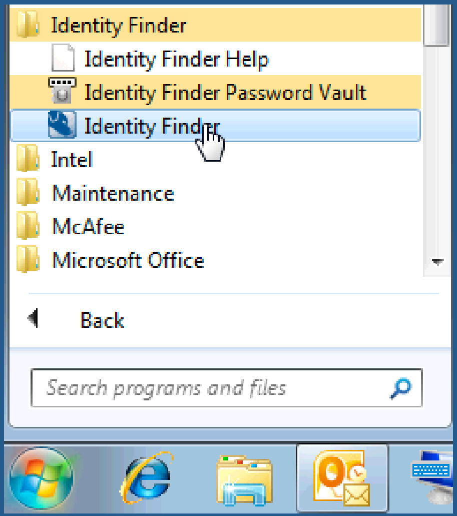
3. **Where you want to look:**
   - Your computer’s hard drive(s) (i.e. C:\)
   - Your remote share(s)
   - Your Exchange e-mail
   - Any Outlook archive file (.pst) that e-mail was saved to
   - CDs and DVDs
   - Thumb drives
   - External hard drives

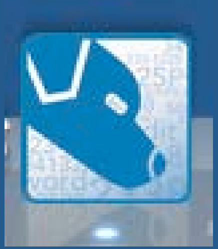
The Identity Finder Software Client

- Identity Finder has been installed on your Windows/Mac computer
- This tutorial will provide information about:
  - Where the software is located
  - How to use the software
  - What features are enabled and can be used to assist you in scanning for personally identifiable information.
  - How and where to save personally identifiable information in the event that it is located

Accessing Identity Finder

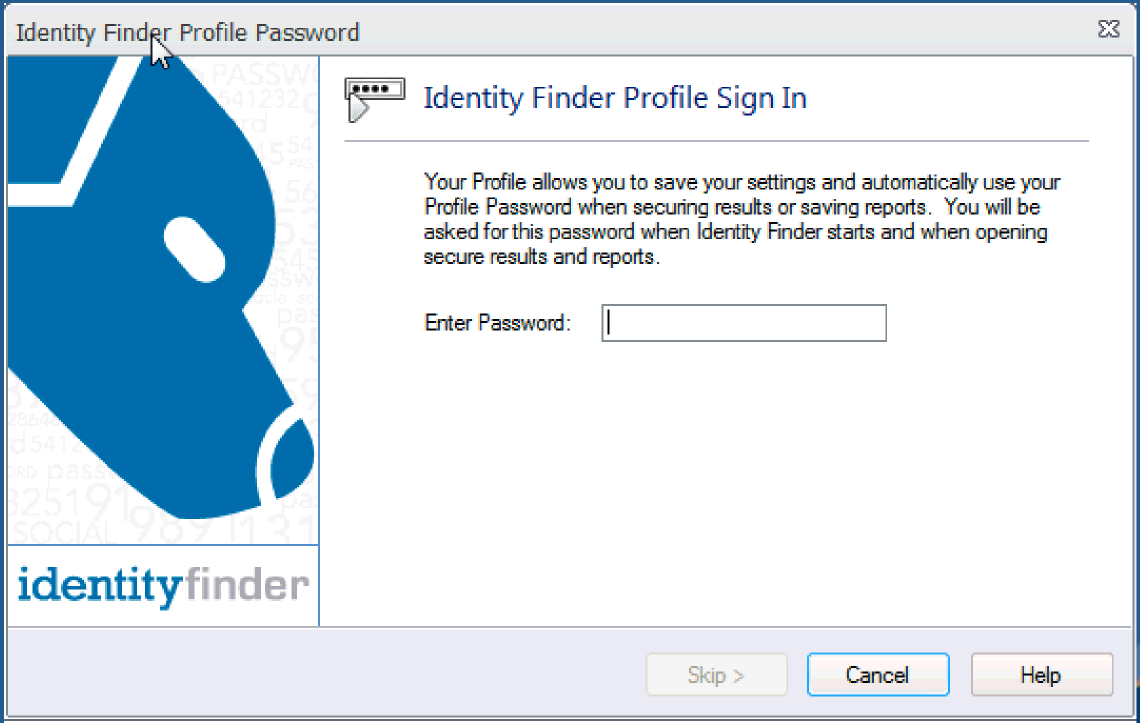
- If you do not see a desktop icon on your Windows computer for Identity Finder, you will need to go to the start menu and select “All Programs”.
- Select “Identity Finder”, then launch the “Identity Finder” application as shown below at left.
- To access Identity Finder on a Mac, select the Identity Finder dock icon as shown below at right.





Launching Identity Finder

- Enter the profile password, then select OK.
- You will be prompted to enter this password every time you launch Identity Finder. You will not be able to choose “Skip”.



Identity Finder Profile Password

Identity Finder Profile Sign In

Your Profile allows you to save your settings and automatically use your Profile Password when securing results or saving reports. You will be asked for this password when Identity Finder starts and when opening secure results and reports.

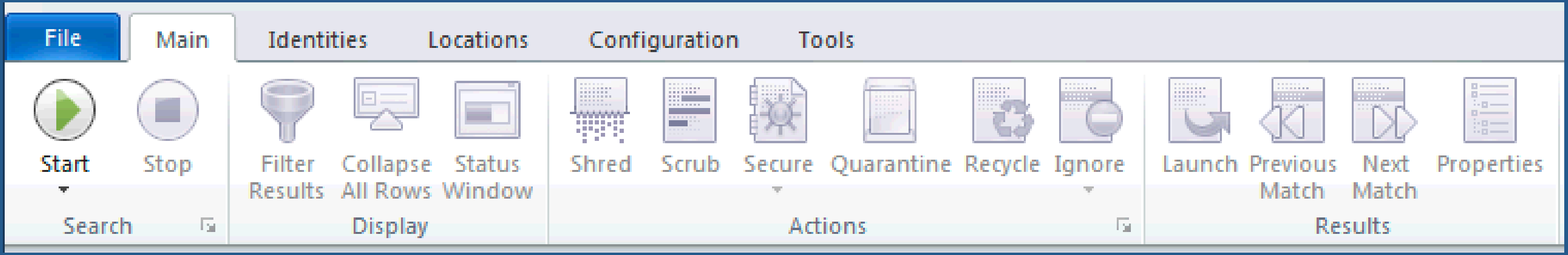
Enter Password:

Launching Identity Finder

- Once the program is launched, you will be prompted to enter a profile password for securing results or saving reports. Please set the password to lowercase ***wcsu***.
- The Identity Finder profile does NOT save personally identifiable information in the reports or in the profile.
- No other users have access to your profile.

Ribbon options

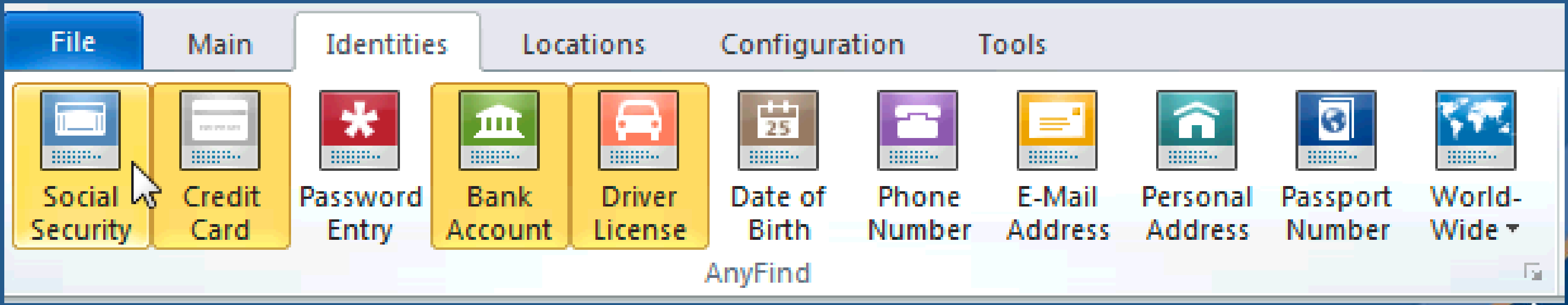
- Just like in Microsoft Office applications, Identity Finder uses what is called a *ribbon* (as shown below) for navigation purposes.



- It is important to familiarize yourself with the **Main**, **Identities**, and **Locations** tabs, features and functions before proceeding with a scan using this software.

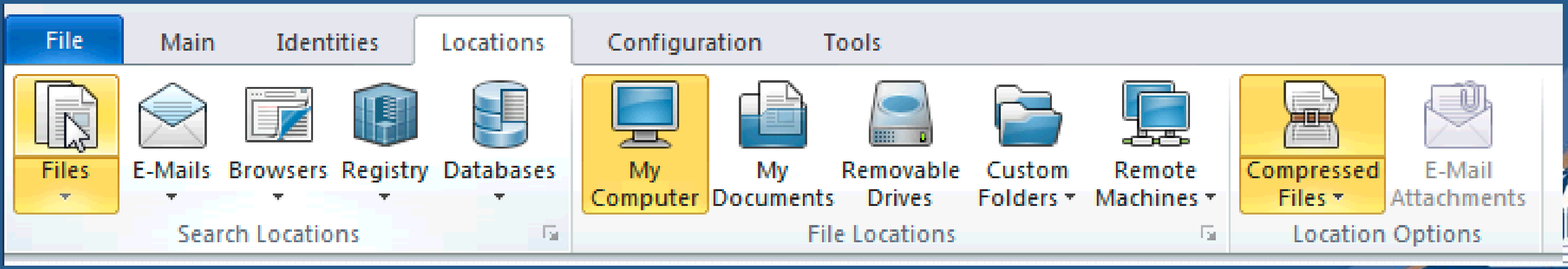
Using the *Identities* Ribbon

- When you select the *Identities* tab, you will see a number of types of data already selected, such as Social Security, Credit Card, Bank Account, and Driver License numbers.
- You can choose to search for additional data, but you cannot deselect the options that are already selected by default.



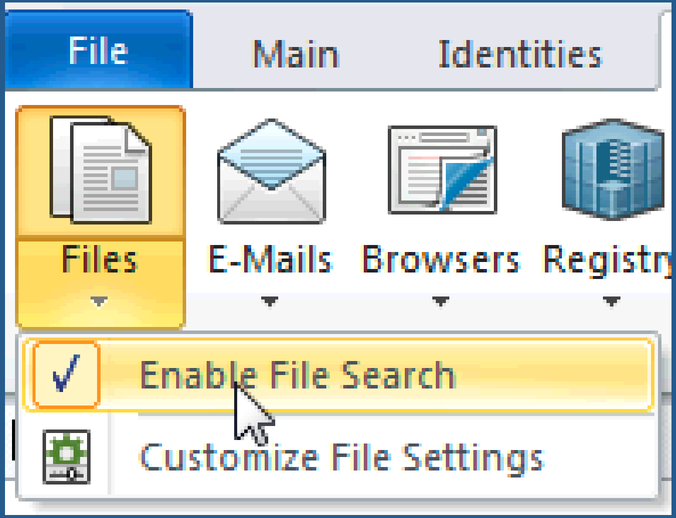
Using the *Locations* Ribbon

- When you select the *Locations* tab, you will have the option to choose to scan files on your computer, scan your email, and other data types.
- You should be primarily concerned with Files and E-mails
- Clicking on the top half of the selected button selects that option, such as Files.
- Clicking on the bottom half of the selected button reveals advanced search options



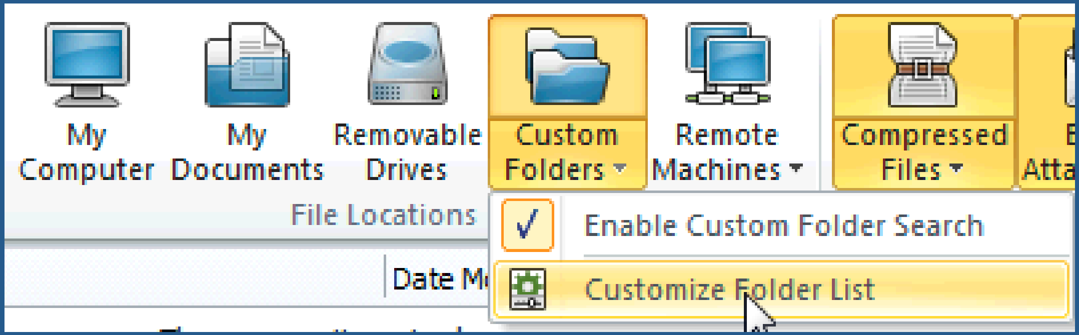
File Searches

- For every search option that is available, you must make sure that the type of search is enabled.
- Clicking on the bottom half of each search icon reveals the ability to enable or disable that particular search. A check next to the option denotes that the option is enabled.
- The search function must be enabled in order to perform the search!



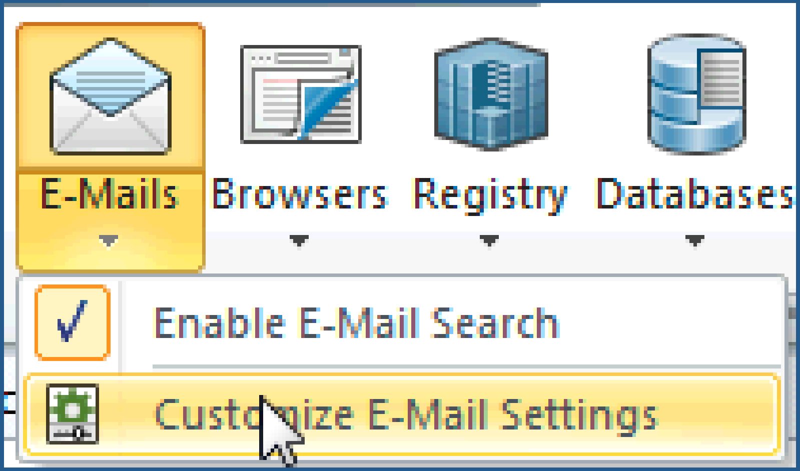
File Searches

- You can refine your search to “My Documents”, “Removable Drives”, as well as specify custom folders by selecting **Custom Folders > Customize Folder List** as shown below.



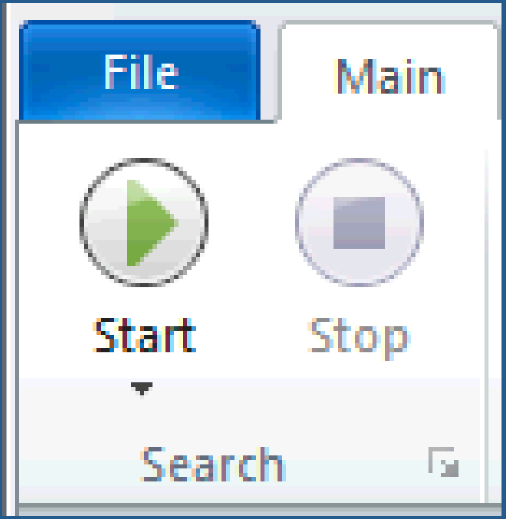
Email Searches

- When performing a search, please note that if you have thousands of emails in your mailbox, it will take a long time to perform the scan. Please allot enough of time to perform the scan.
- In addition to scanning your entire mailbox, you can also scan specific files such as Outlook archive files (.pst)



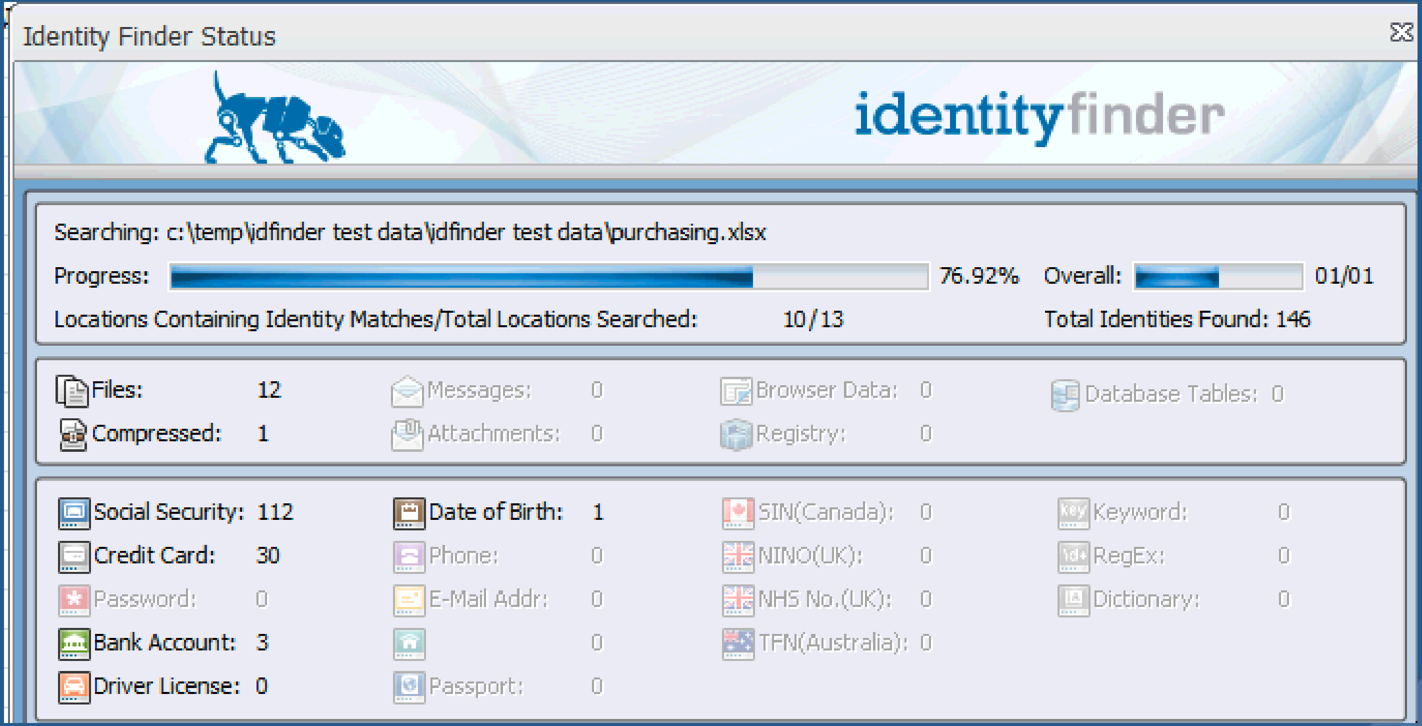
Performing a scan

- Once you have selected the locations that you would like to scan, select the “Main” tab, and select the “Start” button on the ribbon.
- You can stop your search at anytime by selecting the “Stop” button.



Performing a scan

- Once the scan has started, a window like the one shown below will appear:



Identity Finder Status

Searching: c:\temp\idfinder test data\idfinder test data\purchasing.xlsx

Progress: 76.92% Overall: 01/01

Locations Containing Identity Matches/Total Locations Searched: 10/13 Total Identities Found: 146

Files: 12 Messages: 0 Browser Data: 0 Database Tables: 0

Compressed: 1 Attachments: 0 Registry: 0

Social Security: 112 Date of Birth: 1 SIN(Canada): 0 Keyword: 0

Credit Card: 30 Phone: 0 NINO(UK): 0 RegEx: 0

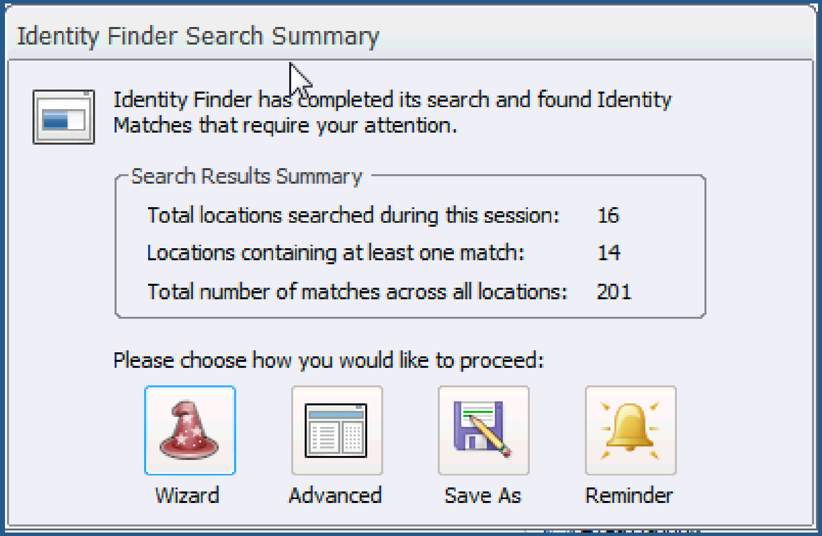
Password: 0 E-Mail Addr: 0 NHS No.(UK): 0 Dictionary: 0

Bank Account: 3 0 TFN(Australia): 0

Driver License: 0 Passport: 0

Performing a scan

- When the scan has completed, the search results window shown at right will appear.
- You can save the report by choosing “Save As”.
- The report will not contain any personally identifiable information
- You can close out of this window by selecting “Advanced”.



Identity Finder Search Summary

Identity Finder has completed its search and found Identity Matches that require your attention.

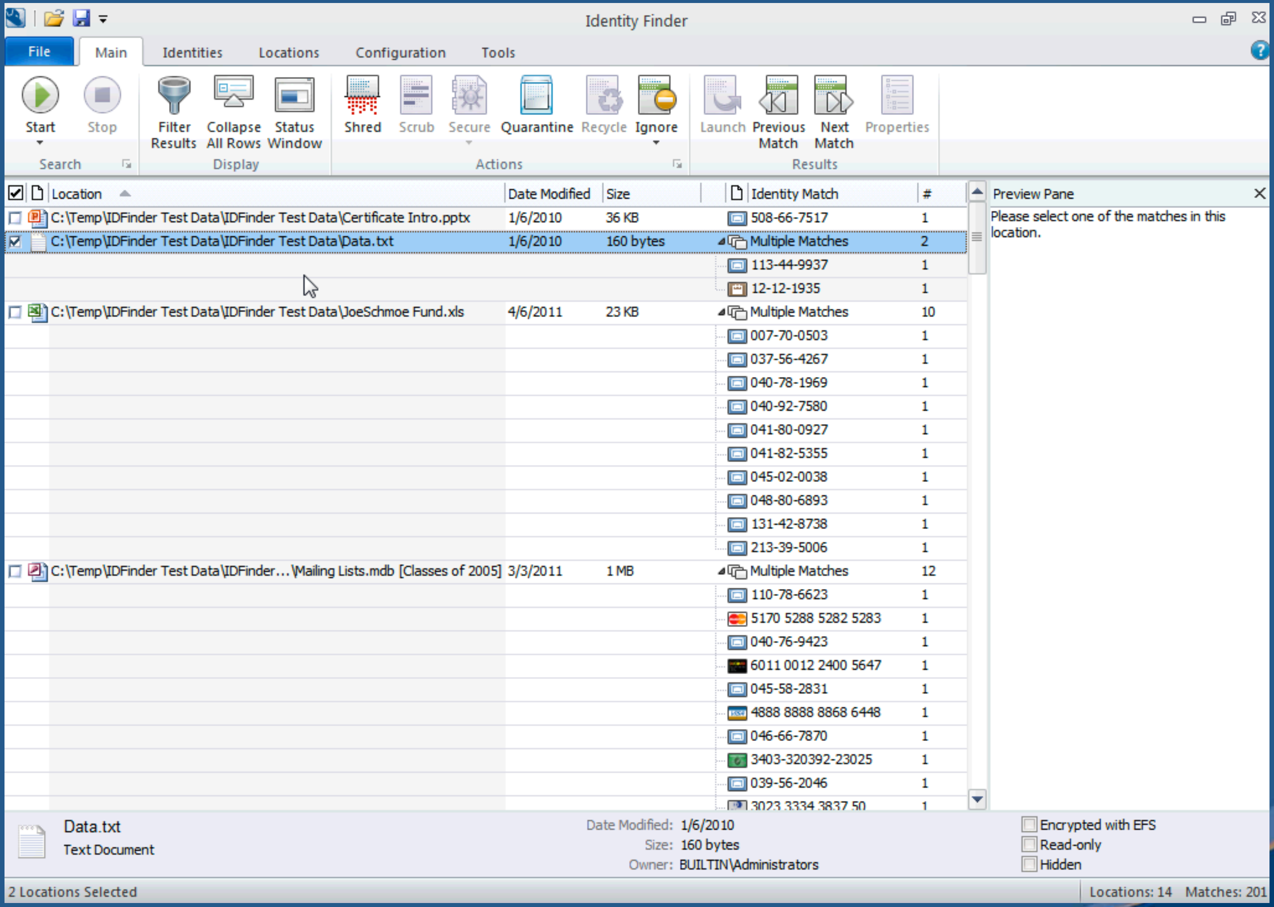
Search Results Summary

Total locations searched during this session:	16
Locations containing at least one match:	14
Total number of matches across all locations:	201

Please choose how you would like to proceed:

Performing a scan

Behind the search results window, the items found will appear on the main Identity Finder window:



☑	Location	Date Modified	Size	Identity Match	#
□	C:\Temp\IDFinder Test Data\IDFinder Test Data\Certificate Intro.pptx	1/6/2010	36 KB	508-66-7517	1
☑	C:\Temp\IDFinder Test Data\IDFinder Test Data\Data.txt	1/6/2010	160 bytes	Multiple Matches	2
				113-44-9937	1
				12-12-1935	1
□	C:\Temp\IDFinder Test Data\IDFinder Test Data\JoeSchmoe Fund.xls	4/6/2011	23 KB	Multiple Matches	10
				007-70-0503	1
				037-56-4267	1
				040-78-1969	1
				040-92-7580	1
				041-80-0927	1
				041-82-5355	1
				045-02-0038	1
				048-80-6893	1
				131-42-8738	1
				213-39-5006	1
□	C:\Temp\IDFinder Test Data\IDFinder…\Mailing Lists.mdb [Classes of 2005]	3/3/2011	1 MB	Multiple Matches	12
				110-78-6623	1
				5170 5288 5282 5283	1
				040-76-9423	1
				6011 0012 2400 5647	1
				045-58-2831	1
				4888 8888 8868 6448	1
				046-66-7870	1
				3403-320392-23025	1
				039-56-2046	1
				3023 3334 3837 50	1

Please select one of the matches in this location.

Data.txt
Text Document

Date Modified: 1/6/2010
Size: 160 bytes
Owner: BUILTIN\Administrators

□ Encrypted with EFS
□ Read-only
□ Hidden

2 Locations Selected

Locations: 14 Matches: 201

WESTERN CONNECTICUT STATE UNIVERSITY

What if sensitive data is found?

- Once Identity Finder presents the results of the search, decisions need to be made on the actions to take on each result:

  - First, it needs to be looked at to see if it can be ignored. False positives, test data and DCL3 data without identity data (i.e. names, addresses, etc) can all be ignored.

    A *false positive* is a result that turns out NOT to be sensitive data but was marked as if it was. (i.e. a product SKU that looks like an SSN).

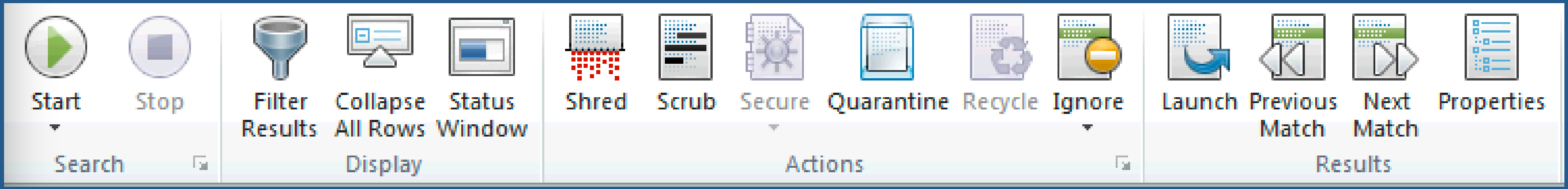
  - Next, records retention procedures will need to be used to determine the action to be performed on the result.

How do I know what actions to perform?

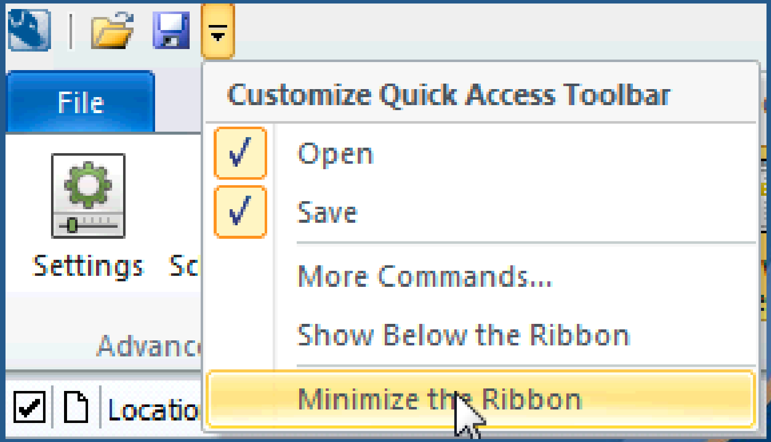
- Based on Records Retention procedures, users will determine what action to take:
  - If the data can be ignored, use the Ignore action.
  - If the data does not need to be kept; after requesting and receiving approval, use the Shred action.
  - If the data needs to be kept, it needs to be moved from its current location to an approved location:
    - Files – The entire file can be moved using the Quarantine action or the data can be redacted (if allowed by Record Retention procedures) using the Scrub action
    - E-mail – The message needs to be manually moved out of mail and into a separate Outlook file (.pst) located in an approved location.

Performing a scan - Actions

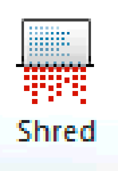
On the "Main" ribbon, the following actions will be available:



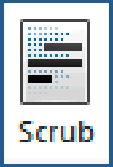
If you do not see the ribbons, you will need to make sure that the "Minimize the Ribbon" option is unchecked by selecting the option shown below located on the top left hand corner of the Identity Finder program window.



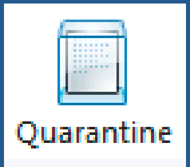
Performing a scan - Actions



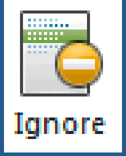
Choosing “Shred” permanently deletes the file using the U.S. Department of Defense deletion standard.



Choosing “Scrub” removes the highlighted information from the location while keeping all other data intact.



Choosing “Quarantine” moves the selected file to a quarantine location and permanently shreds it from its current location



Choosing “Ignore” adds the file to an ignore list so that it is not searched again. This would be useful in the case of a false positive.

Quarantine Locations

- Every user will have specific quarantine locations for specific types/locations of data.
- Files located on your H:\ or K:\ drive that contain data will need to be moved to the “SECURE” folder on your H:\ drive or K:\ drive, depending on where the data originated.

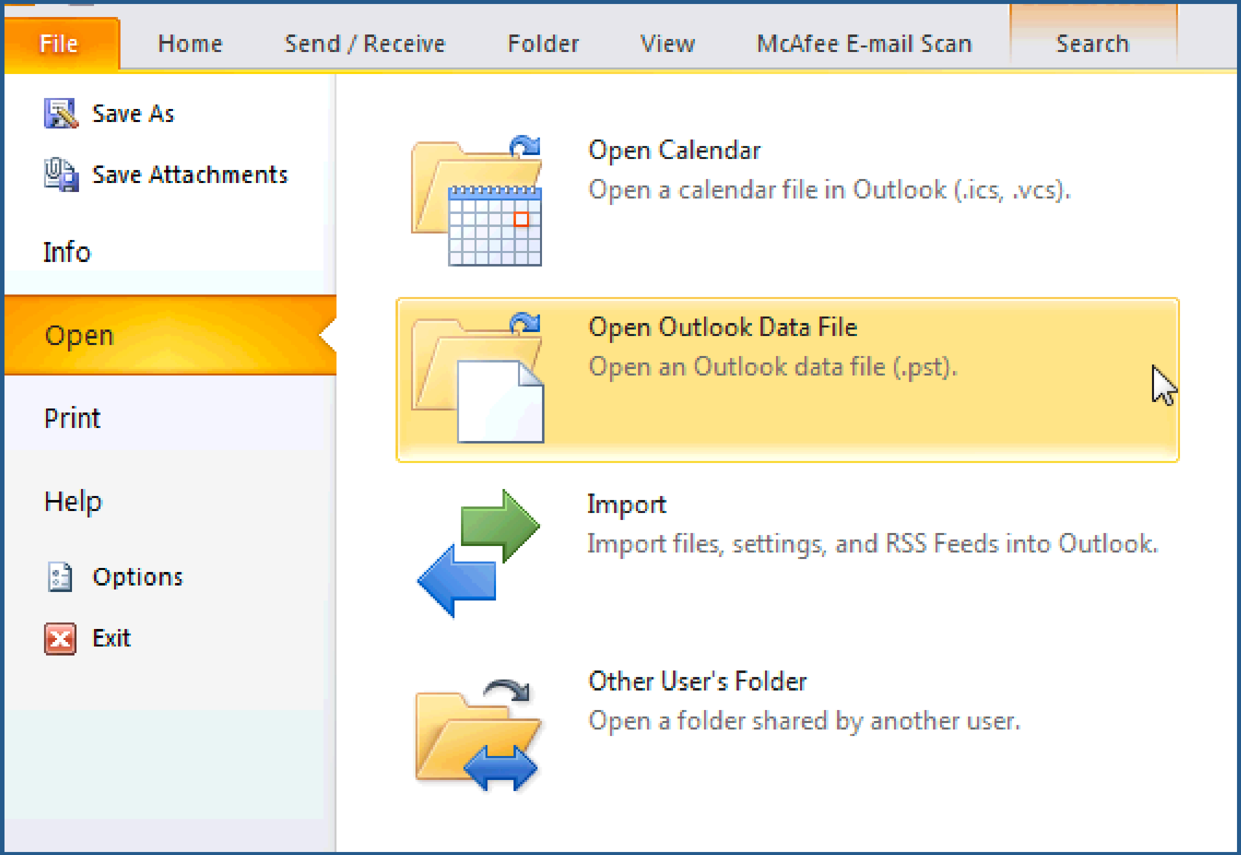
  Example: ***K:\<dept>\SECURE*** *or* ***H:\SECURE***
- Once the data has been quarantined to the “SECURE” staging area during the amnesty period, those files will then be moved to a secure location by University Computing and all users will be notified where the location is and when this move will take place.

Identity Finder and Email

- You will not be able to Scrub or Quarantine emails in Identity Finder
- If you find data in your email, you must manually quarantine the emails following a specific process.
- The quarantine location for email will be located at H:\SECURE\MAIL and an email archive named "<username>-secure.pst" will be located at this location.
- Emails will need to be moved from your mailbox to the archive file.

Moving Quarantine Emails to the Secure Archive

In Outlook, select the “File” tab, then select “Open”, then “Open Outlook Data File”.



Open Calendar
Open a calendar file in Outlook (.ics, .vcs).

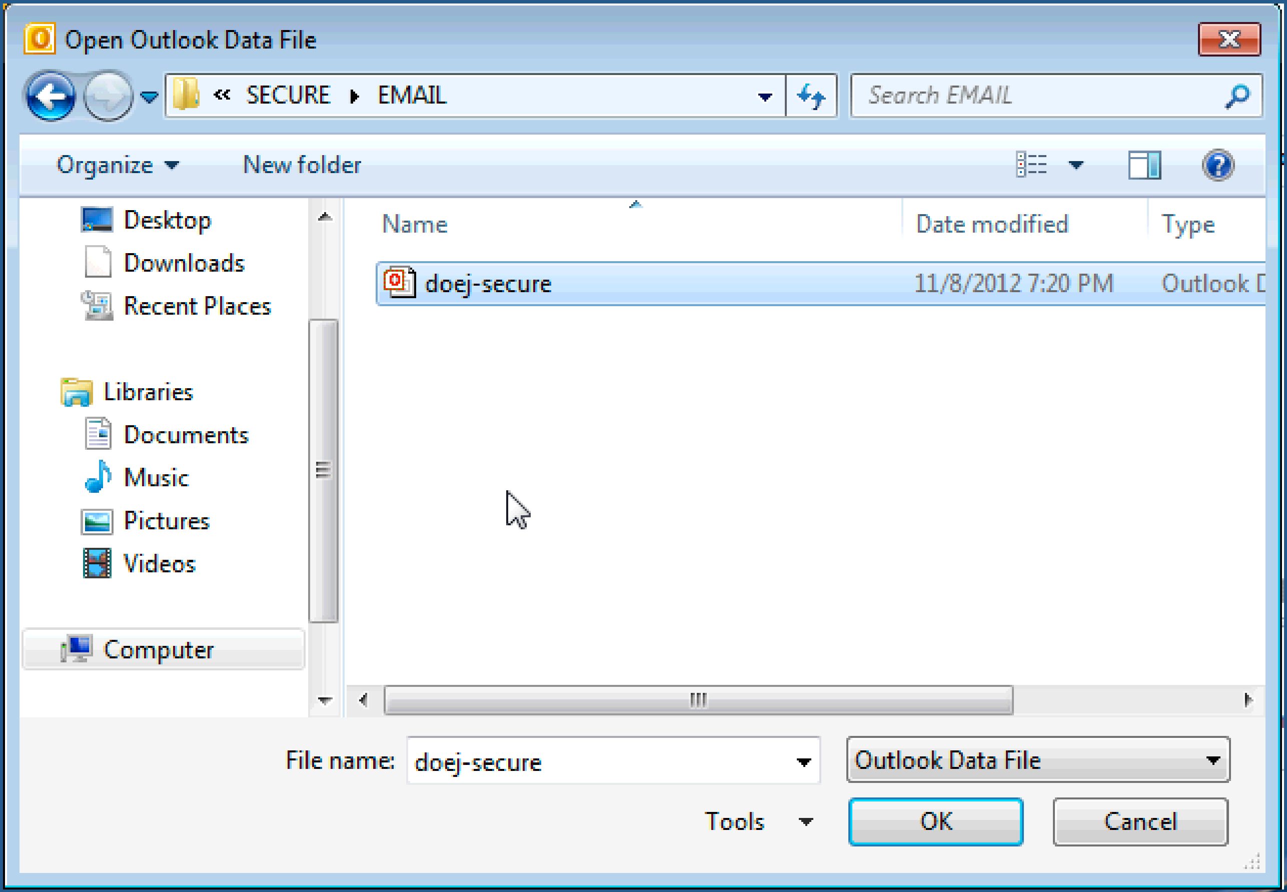
Open Outlook Data File
Open an Outlook data file (.pst).

Import
Import files, settings, and RSS Feeds into Outlook.

Other User's Folder
Open a folder shared by another user.

Moving Quarantine Emails to the .PST file

Navigate to the Outlook file on your H:\ drive, select it, then choose “OK”.



Name	Date modified	Type
doej-secure	11/8/2012 7:20 PM	Outlook D

File name: doej-secure

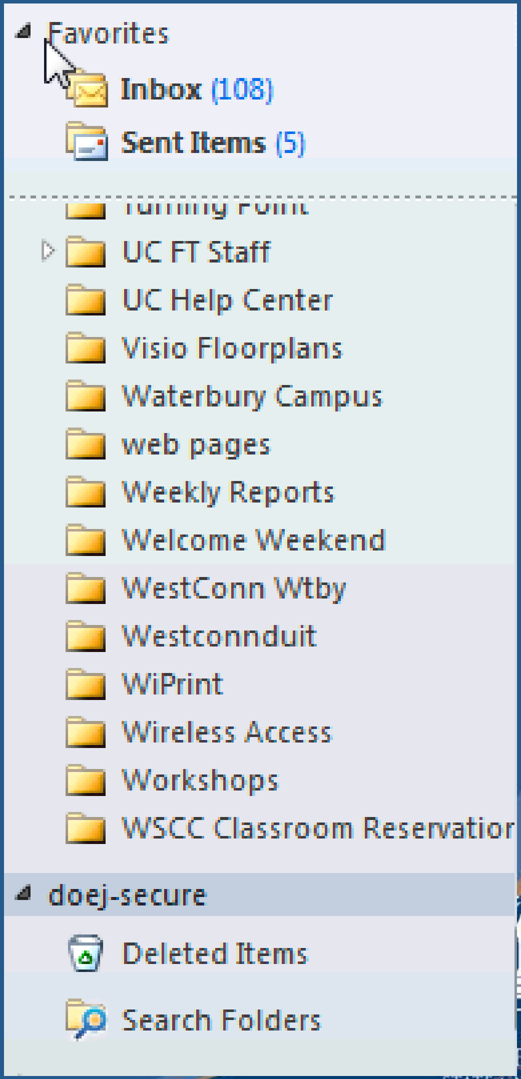
Outlook Data File

Moving Quarantine Emails to the Secure Archive

Once the file is open, you will need to navigate to it by scrolling down in your Outlook folder list to below your existing folders

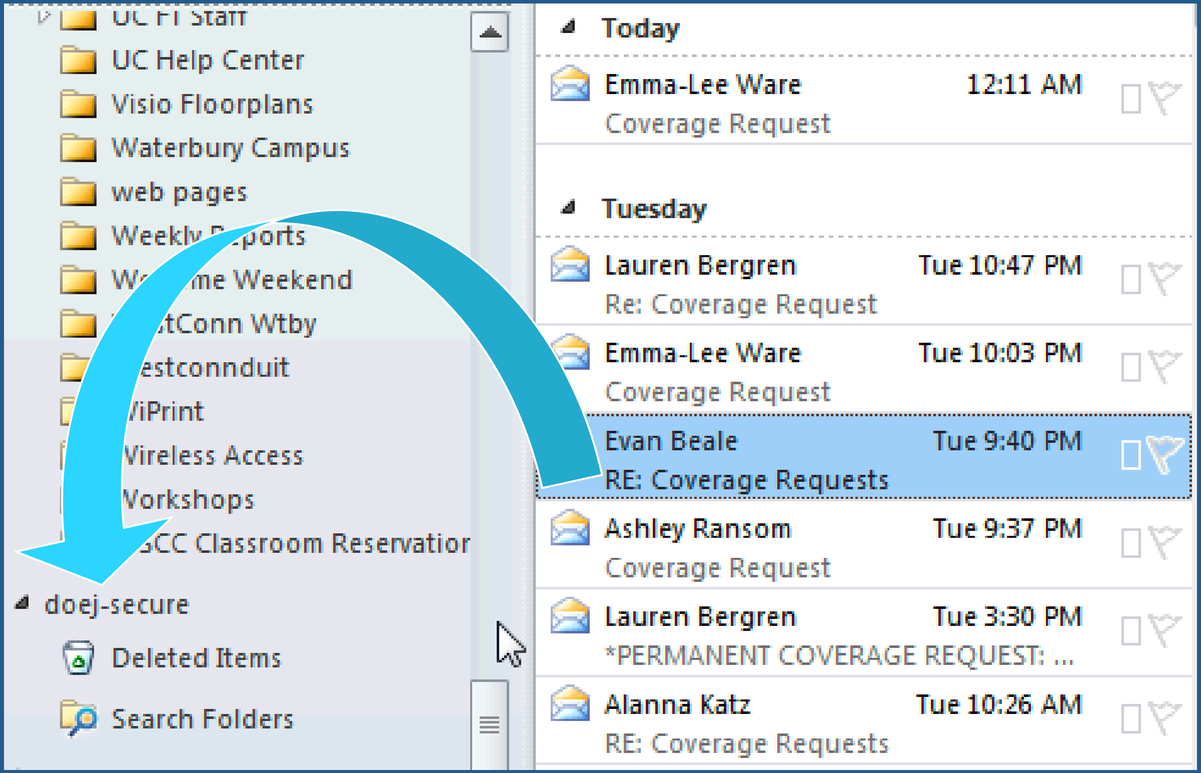
Select the item that lists <your-username>-secure.

Example: *doej-secure* as shown at right.



Moving Quarantine Emails to the Secure Archive

To move email messages into this location, select the email and drag it to the secure location.



Today		
Emma-Lee Ware	Coverage Request	12:11 AM
Tuesday		
Lauren Bergren	Re: Coverage Request	Tue 10:47 PM
Emma-Lee Ware	Coverage Request	Tue 10:03 PM
Evan Beale	RE: Coverage Requests	Tue 9:40 PM
Ashley Ransom	Coverage Request	Tue 9:37 PM
Lauren Bergren	*PERMANENT COVERAGE REQUEST: ...	Tue 3:30 PM
Alanna Katz	RE: Coverage Requests	Tue 10:26 AM

Important Notes

- Not all data can be scrubbed (such as .zip files)
- Files that can be scrubbed include HTML files, text files, and Office 2007 or newer files
- Secure and Recycle options are permanently disabled
- Allot enough time to run your scan
- When the scan is completed, close out of Identity Finder.
- Do not log off with Identity Finder open, having the operating system close the application. This will cause the scan to be invalid.
- Do not use the Configuration or Tools tabs unless directed to do so by University Computing staff.

What happens once locations are clean?

- Once the cleanup phase is complete (i.e. all locations have been searched and no more sensitive data is found in non-approved locations) you will need to regularly perform searches to make sure DCL3 data is not written to non-approved locations.

- You can proactively move files or email to the approved locations as part of your business procedures

Where to go from here

- Start scanning locations:
    - Scan your H drive first, then local hard drive(s)
    - Move to your remote user share(s)
    - Then to email, then search removable media
- For each search performed, work with the results so that:
    - False positives, test data and data without identity data are ignored
    - DCL3 data that needs to be kept is quarantined or scrubbed
    - DCL3 data that doesn't need to be kept is shredded after approval
- Repeat searches until there are no more results

Remember: Consult your Record Retentions Officer

Remember: When in doubt – don't shred. Quarantine instead.

Contacts

- Document retention standards are set by the State of Connecticut and can be found at:

  www.wcsu.edu/records

- Specific questions should be directed to your designated Data Steward for your Data Domain
- Questions regarding Data Retention Standards should be directed to: Mark Case, Records Retention Officer, casem@wcsu.edu

Questions/Closing Comments

Q & A