USING IDENTITY FINDER
Contents
INTRODUCTION ......................................................................................................................... 3
Purpose ......................................................................................................................................... 3
Audience and Scope .................................................................................................................... 3
Licensing ....................................................................................................................................... 3
Privacy Warning ........................................................................................................................... 4
FIRST STEPS ................................................................................................................................ 5
Opening the Program .................................................................................................................... 5
Recommended Information to Search For .................................................................................... 5
OCR for PDF’s, JPG and Other Files ............................................................................................ 5
LOCATIONS ................................................................................................................................. 7
Whole System Scans Excluding E-mails or Specific Folders ......................................................... 7
Whole System Scans Including E-mails ........................................................................................ 12
Local Folders and Files, Mapped Drives and Searching Inside E-mail PST Files ......................... 14
BOX ............................................................................................................................................... 18
INTRODUCTION

Identity Finder is a software utility used to search for personal information such as social security numbers, credit card numbers, bank accounts etc. It can search in local and remote drives as well as emails and Berkeley’s bConnected implementation of BOX\(^1\).

Purpose

The purpose of this document is to show users the required steps needed in order to scan a system in the desired locations.

Audience and Scope

**Audience**

- Individuals scanning their own computers, emails or file shares.
- Departments scanning, servers or user workstations.
- Scanning in response to a breach to determine data effected.

**Scope**

Identity Finder’s primary use is for devices that routinely handle data classified as PL-2 or greater, based on UC Berkeley’s data classification\(^2\) in which each system is classified into a protection level (PL) depending on the type of data that it stores. Identity Finder can be used for the scanning of:

- The whole system, and excluding emails and/or folders.
- The whole system.
- Individual folders and files (including shared drives), and whether to look inside of PST files.
- BOX.

Licensing

**Receiving Licenses**

Licenses should be made available for the purposes of users/departments with clear needs such as:

- A department that routinely deals with PL-2 or higher data, which would like to monitor and ensure such data is only found in expected, designated systems.
- A department launching a project to verify particular kinds of non-public data is not found in the department.

\(^1\) https://bconnected.berkeley.edu/collaboration-services/box

\(^2\) https://security.berkeley.edu/data-classification#table
• An individual or department involved in incident response, in order to verify what types of data may be in scope for the incident.

**License Structure**
There are two types of options for allocating licenses:

• **Per machine – 1 license.**
  One individual machine may be scanned. File shares, databases, and web sites via the additional DB, and web module may not be used (but the OCR module on the individual machine’s drives may be used).

• **Per department - # of full-time FTE in department.**
  All devices within the department may be scanned (within the privacy constraints). Departmental resources such as file shares, databases, and web sites may be scanned. If these resources are managed by IST but are for the sole use of the department, they too may be scanned.

**Disallowed Scanning**
Campus-wide resources, such as CalShare or Research Hub, may not be scanned within the terms of the license.

**Privacy Warning**
The University protects the privacy of Electronic Communication Records. Please make sure you have proper permissions to scan a system. For more information, view the scanning guidance provided by UC Berkeley Security. If you have additional questions on whether it is acceptable to scan a particular system, contact IT Policy at itpolicy@berkeley.edu.

---


4 [https://security.berkeley.edu/content/guidance-departments-scanning-ssns-stored-servers-and-workstations](https://security.berkeley.edu/content/guidance-departments-scanning-ssns-stored-servers-and-workstations)
FIRST STEPS

Opening the Program

1. Once you start up Identity Finder and get to the Search Wizard, select “Open Advanced Interface”

Recommended Information to Search For

1. In the main window click “Identities” then select: Social Security, Credit Card, Password Entry, Bank Account, Driver License, Date of Birth, Passport Number

OCR for PDF’s, JPG and Other Files

By default, OCR is enabled for certain file types such as PDF’s. It is not enabled for example for JPG files. To view the list of files that are scanned:

1. In the main window click “Configuration”, then “Settings”, which should open up another window
2. In the new window, go to “File Types”, then click the dropdown next to “Search these file types:” and select “Custom”. Click the “Manage” button. 

   NOTE: If you do not want to change the file types being searched, change from “Custom” to “Common” in the dropdown.

3. In the new window, view and select the file types you would like to include in the scan. In our example we will add “jpg” by clicking the check box next to it.
LOCATIONS

You can easily specify the location of where the scan is performed by adjusting the location settings, which will be discussed in more details below.

Whole System Scans Excluding E-mails or Specific Folders
This scan will allow you to scan the whole system but exclude the scans of e-mails or folders. Please make sure you have the proper permissions to scan as mentioned in the Privacy Warning above. If you do not, exclude e-mails (step 1) and User Folders (step 2).

1. To not scan e-mails
   a. Under the “Locations” tab make sure your options are selected as shown, notice E-Mails is not highlighted.

2. To exclude specific folders
   a. Under the “Locations” tab click on “Custom Folders”, which will pop-up a window.
b. Next add all local drives one by one. In the new window, click on the three dots next to folder and add the first local drive then click “OK”, and then “Add”. Repeat for all local drives.
c. Next part is selecting folders to exclude from scan. Follow the same process as above but this time make sure to select the “Add as Exclusion” check box, then click add. In our example, once the window pops up, we select the “Users” folder, click OK. Then “Add as Exclusion” and finally “Add”. Do this for all folder you do not wish to scan.
d. Your selection of folders to include and exclude can now be seen.
3. To start the scan go to “File” -> “Start Search”.

4. Once the scan is complete click “Advanced” to see your results.
Whole System Scans Including E-mails

This option will scan your entire system as well as e-mails if selected. Please make sure you have permission to scan as mentioned above in the Privacy Warning. If you do not have permission to scan the whole system, make sure to exclude disallowed locations as mentioned above.

1. Under the “Locations” tab make sure your options are selected as shown.

![Image of the “Locations” tab with selected options]

2. Recommended settings for “E-mails”
   a. First click on black arrow under “Emails” and select “Customize File Settings.”

![Image of “Emails” settings with selected options]

b. Make sure the checkboxes specified below are selected.

- View and manage E-mail applications to search

![Image of checkboxes selected for E-mail search settings]
3. To start the scan go to “File” -> “Start Search”.

4. Once the scan is complete click “Advanced” to see your results.
Local Folders and Files, Mapped Drives and Searching Inside E-mail PST Files
These settings will allow you to specify local folders and files, mapped drives and whether to search inside of PST files within these locations.

1. Under the “Locations” tab click on custom folders, this will cause the settings window to open.

2. Clicking on the right three dots of Folder, allows you to specify the folder you would like to search in. In our case we will search the desktop and Shared Drive X:
3. Click “OK” then “Add”. Add any other folder Locations you would like to search, in our case we will also add Shared Drive X:.

4. Your directories should now be listed as show below.
5. Click “Apply” then “OK”, your locations tab will look like the one below.

6. If you would like to also scan PST files in the location you specified.
   a. On “Locations” tab, click the black arrow under “Emails” and select “Customize Email setting”.
   b. Select the settings as shown.

   c. Select “Apply” then “OK”.

   NOTE: If you are not scanning PST files, make sure “E-mails” are deselected.
1. In Locations, click on “Emails” to deselect it.
2. Your Locations will then look as follows.

7. To start the scan go to “File” -> “Start Search”.

8. Once the scan is complete click “Advanced” to see your results.
BOX
In order to use Identity Finder in BOX, use the following steps:

1. In order to connect to folder as shown in step 2, a separate BOX password will need to be set up.
b. Once you click continue, it will take you to the familiar Berkeley CalNet Authentication service.

c. You should now be logged into BOX. On the right hand side next to your name, click the down arrow and select “Account Settings”.

d. On the new screen, scroll down to the “Create External Password” section, click edit password and create a strong password.
2. Connecting to your BOX folder.
   NOTE: This step has to be taken in order for Identify Finder to work in Step 3
   a. Open my computer, click on the location and type in the following address:
      `\dav.box.com@SSL\DavWWWRoot\dav` and press enter. A popup window will appear, asking for credentials. Enter your email, and the password you created in step 1.
   b. You should now see all the files you have in BOX (in our case just one).
3. Using Identify Finder on BOX.
   a. Once you start up Identity Finder and get to the Search Wizard, select “Open Advanced Interface”.
   b. In the main window, click on the “Locations” tab, click on “Custom Folders”, and “Enable Custom Folder Search”.
   c. In the window that opens, type in the same address as before in the folder section: `\dav.box.com@SSL\DavWWWRoot\dav`, then click add. It should now appear as a folder location in the list. Then click apply and OK.
d. Click on File, the Start Search.

Once clicked on Add, it should now appear on this list

The list now contains our BOX folder

e. The results will show up, in our case finding a SSN in our file on BOX.
f. To see your results click advanced in the above “Search Summary”.