

How to Scan for Secure Confidential Data using Identity Finder in OSX

Important: Identity Finder for Mac is unable to search Outlook email. Manually inspect files that may contain confidential data but were not searched/identified by the Identity Finder scan.

Launch Identity Finder using the shortcut on your desktop:



NOTE: If you do not have an Identity Finder Icon on your desktop, please click the magnifying glass in the top right hand corner of your screen. Type “Identity Finder” this will search for and show you the application. Please double click to open it.

Choose a password. Choosing a password will allow Identity Finder to save any configuration changes made and remembers the items you have indicated as false positives, so that they do not appear in future scan results.

NOTE: If you already have a password, you do not need to set a new one. Please enter your password and continue to the next step. If you have forgotten your password, please submit a ticket here: <https://it.sas.cornell.edu/>

A screenshot of the 'Identity Finder Profile Password' dialog box. The title bar reads 'Identity Finder Profile Password'. Inside the dialog, there is a gear icon and the text 'New Identity Finder Profile'. Below this, a paragraph explains: '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.' There are two text input fields: 'Enter Password:' and 'Confirm Password:'. At the bottom, there are 'Cancel' and 'OK' buttons.

Identity Finder Profile Password

 **New Identity Finder Profile**

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:

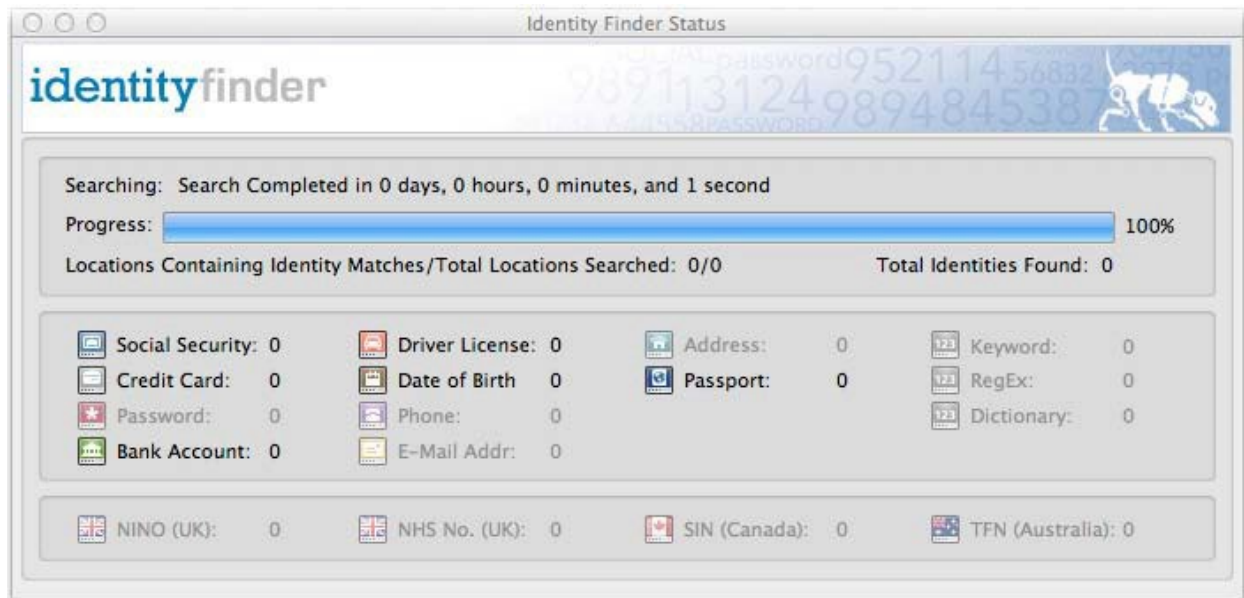
Confirm Password:

Specifying what to scan: Please make sure to select the following items and click “Search”.



NOTE: If these items have already been selected, grayed out or you have already selected them from a previous scan, please continue to the next step.

Once you click search you will see the **scan status window**. You can minimize the main identity finder window if you would like to continue working and allow the scan to complete before processing your results. You can also just close the scan status window, if you would like to begin processing your results immediately.



NOTE: The duration of an identity finder scan will vary greatly depending on the processing power and hard drive speed of your computer, and the amount of data being scanned. Some users will experience scan times of 5---10 minutes, while others will see scans lasting 3---4 hours. If your scan is still running at the end of the day, you should lock your session and leave it running overnight.

Processing Scan Results: You are responsible for taking action on each item discovered. Click once on a scan result to see more details in the **preview pane**:

The screenshot shows the Identity Finder application window. The main pane displays a list of scan results with columns for Location, Date Modified, Size, and Identity Match. One result is selected: `local/Library/VirtualBox/Machi...` with a date of `10/14/2010`, size of `89 KB`, and identity `4378582104788`.

The preview pane on the right shows the content of the selected file, which is a system log. The log entries include:

```

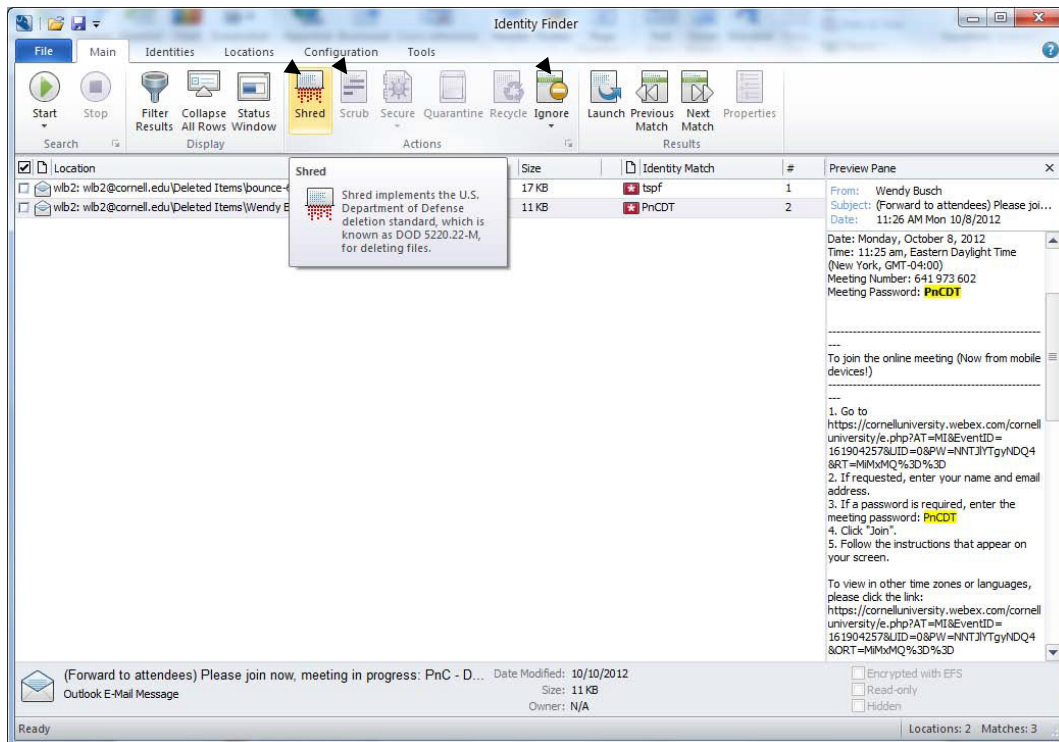
Location: /Users/bjm11/bonnie local/Library/VirtualBox/Machines/furfur/Logs/VBox.log
File Type: text
Identities: 1 Visa Credit Card Number

01:13:00.115 EFER          =0000000000000000
01:13:00.115 PAT           =0007010600070106
01:13:00.115 STAR          =0000000000000000
01:13:00.115 CSTAR        =0000000000000000
01:13:00.115 LSTAR        =0000000000000000
01:13:00.115 SFMASK        =0000000000000000
01:13:00.115 KERNELGSBASE =0000000000000000
01:13:00.115 ***
01:13:00.115 Guest paging mode: 32-bit, changed 17808 times, A20 enabled
01:13:00.115 Shadow paging mode: PAE
01:13:00.115 Host paging mode: AMD64+NX
01:13:00.115 ***
01:13:00.115 Active Timers (pVM=1876d000)
01:13:00.115 pTimerR3 offNext offPrev offSched Clock Time      Expire      State
Description
01:13:00.115 1a0060c0 ffe4270 00000000 00000000 Real          7178858    7178867
2-ACTIVE      EMT Yielder
01:13:00.115 19fea330 ffff7a10 0001bd90 00000000 Real          7178858    7178874 2-
ACTIVE      VGA Refresh Timer
01:13:00.115 19fe1d40 00000000 000085f0 00000000 Real          7178858    7188647
2-ACTIVE      Cache-Commit
01:13:00.115 1a001ae0 00000000 00000000 00000000 Virt          4378574222181
4378575480329 2-ACTIVE      Audio timer
01:13:00.115 19fe4750 00000420 00000000 00000000 VrSy          4378574063291
4378582104788 2-ACTIVE      i8254 Programmable Interval Timer
01:13:00.115 19fe4b70 00020270 ffffbe0 00000000 VrSy          4378574072804
4378990000000 2-ACTIVE      MC146818 RTC/CMOS - Second
01:13:00.115 1a004de0 00000000 ffd990 00000000 VrSy          4378574082105
5186010453301 2-ACTIVE      ACPI Timer
01:13:00.115 ***
01:13:00.115 Shadow GDT (GCAddr=ff54e000):
01:13:00.115 ffd8 - 80d80087 ff08900 - base=ff0080d8 limit=00000087 dpl=0 TSS32Avail
Present 16-bit HyperTSSTrap08
01:13:00.115 ffe0 - 80500087 ff08900 - base=ff008050 limit=00000087 dpl=0 TSS32Avail
Present 16-bit HyperTSS
01:13:00.115 ffe8 - 0000ffff 00a19b00 - base=00000000 limit=fffffff dpl=0 CodeER Accessed
Present Page 16-bit HyperCS64
01:13:00.115 ff0 - 0000ffff 00c19300 - base=00000000 limit=fffffff dpl=0 DataRW Accessed
Present Page 32-bit HyperDS
01:13:00.115 ff8 - 0000ffff 00c19b00 - base=00000000 limit=fffffff dpl=0 CodeER Accessed
Present Page 32-bit HyperCS
01:13:00.115 ***
01:13:00.115 ***** End of Guest state at power off *****
01:13:00.120 Changing the VM state from 'POWERING_OFF' to 'OFF'.
01:13:00.121 Console:powerDown(): A request to power off the VM has been issued
(mMachineState=Stopping, InUninit=0)
01:13:00.121 SharedFolders host service: disconnected, u32ClientID = 7
01:13:00.126 Changing the VM state from 'OFF' to 'DESTROYING'.
01:13:00.126 ***** Statistics *****

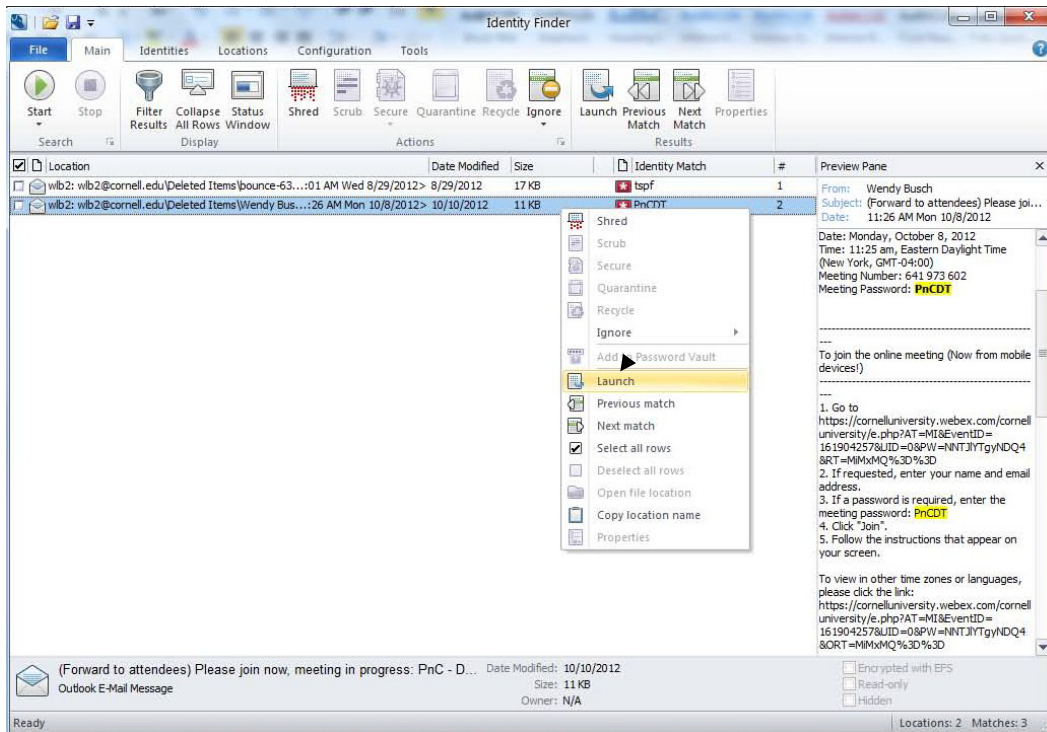
```

Important -- After reviewing the results you must either:

1. **Shred** the document – **If you no longer need the document please shred it.**
2. **Scrub** the document. Scrub is only an option for certain document types. If the scrub option is not active, see instructions below on manually editing to remove confidential data.
3. **Ignore** the result. Take this action if there is no confidential data present. If you do not choose “ignore” the result will appear in future scans.



To manually open a document for editing: Right click on the item and select “**launch.**” Once the document is opened you can manually remove the confidential data. Not all document types are editable.



Post---cleanup attestation: After completing the scan, and reviewing and acting on any scan results, all employees are required to complete an attestation statement at:

<https://it.cornell.edu/security-essentials-it-professionals/remediation-options-spirion>

Where to go for help: If you have any questions during this process, please contact SCL IT by submitting a tech ticket: <https://ssit.scl.cornell.edu/submit-tickets>