Objective-See
a non-profit 501(c)(3) foundation.

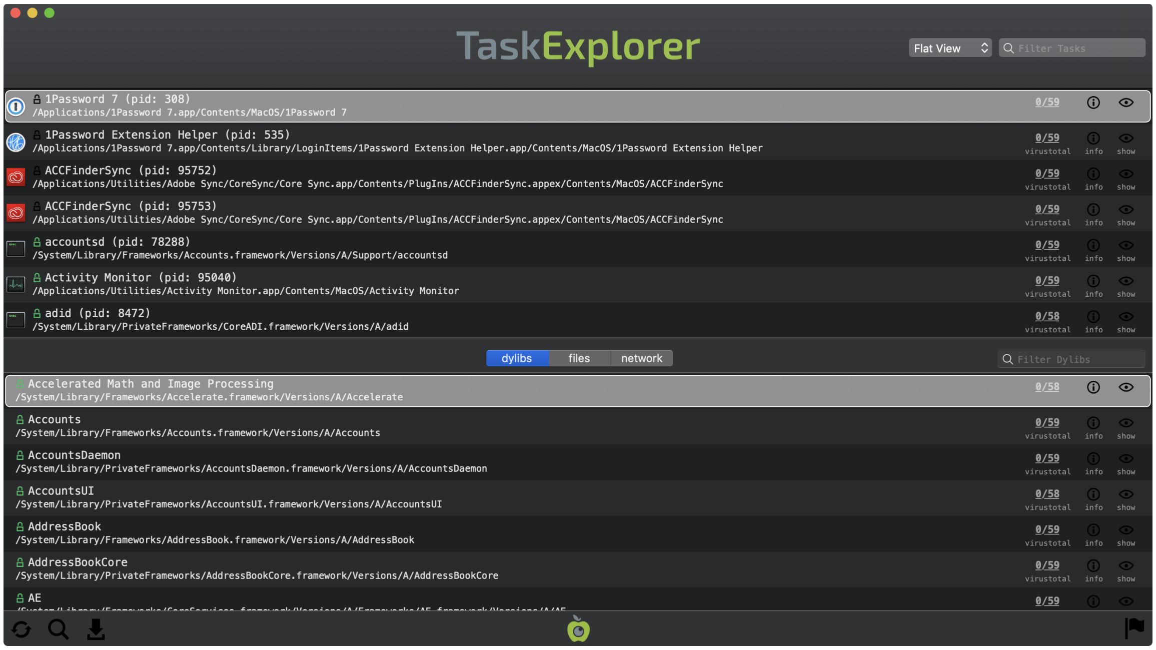
TaskExplorer

⬇ download

Explore all the tasks (processes) running on your Mac with TaskExplorer.

Quickly see a task's signature status, loaded dylibs, open files, network connection, and much more!

compatibility: OS X 10.8+
current version: 2.0.2 (**change log**)
zip's sha-1: DD39421245CC238597444843DB7ED4A3E33EA426



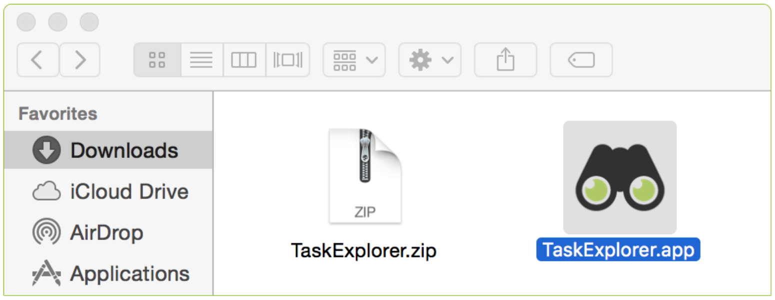
```
1Password 7 (pid: 308)                                                          0/59
/Applications/1Password 7.app/Contents/MacOS/1Password 7
1Password Extension Helper (pid: 535)                                           0/59 virustotal info show
/Applications/1Password 7.app/Contents/Library/LoginItems/1Password Extension Helper.app/Contents/MacOS/1Password Extension Helper
ACCFinderSync (pid: 95752)                                                      0/59 virustotal info show
/Applications/Utilities/Adobe Sync/CoreSync/Core Sync.app/Contents/PlugIns/ACCFinderSync.appex/Contents/MacOS/ACCFinderSync
ACCFinderSync (pid: 95753)                                                      0/59 virustotal info show
/Applications/Utilities/Adobe Sync/CoreSync/Core Sync.app/Contents/PlugIns/ACCFinderSync.appex/Contents/MacOS/ACCFinderSync
accountsd (pid: 78288)                                                          0/59 virustotal info show
/System/Library/Frameworks/Accounts.framework/Versions/A/Support/accountsd
Activity Monitor (pid: 95040)                                                   0/59 virustotal info show
/Applications/Utilities/Activity Monitor.app/Contents/MacOS/Activity Monitor
adid (pid: 8472)                                                                0/58 virustotal info show
/System/Library/PrivateFrameworks/CoreADI.framework/Versions/A/adid

Accelerated Math and Image Processing                                           0/58
/System/Library/Frameworks/Accelerate.framework/Versions/A/Accelerate
Accounts                                                                        0/59 virustotal info show
/System/Library/Frameworks/Accounts.framework/Versions/A/Accounts
AccountsDaemon                                                                  0/59 virustotal info show
/System/Library/PrivateFrameworks/AccountsDaemon.framework/Versions/A/AccountsDaemon
AccountsUI                                                                      0/58 virustotal info show
/System/Library/PrivateFrameworks/AccountsUI.framework/Versions/A/AccountsUI
AddressBook                                                                     0/59 virustotal info show
/System/Library/Frameworks/AddressBook.framework/Versions/A/AddressBook
AddressBookCore                                                                 0/59 virustotal info show
/System/Library/PrivateFrameworks/AddressBookCore.framework/Versions/A/AddressBookCore
AE                                                                              0/59
```

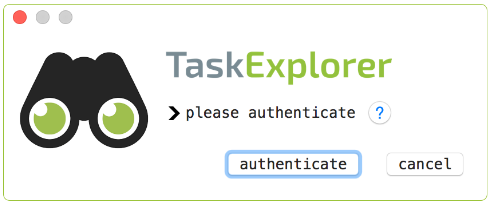
TaskExplorer allows one to visually explore all running processes. Notable features of TaskExplorer include:

- Signing Status
  quickly view, (or filter) tasks that are signed by Apple, 3rd-parties, or are unsigned
- VirusTotal Integration
  detection ratios can reveal known malware, while unknown files can be submitted for analysis
- Loaded Dynamic Libraries
  for each task, view it's loaded dylibs
- Open Files
  view all files that a particular task has opened
- Network Connections
  see the network connection (and its details) created by a task
- Global Search
  quickly search to find specific items, or unsigned binaries, established network connections, and more!

To use TaskExplorer, first **download** the zip archive containing the application. Depending on your browser, you may need to manually unzip the application by double-clicking on the zipped archive:

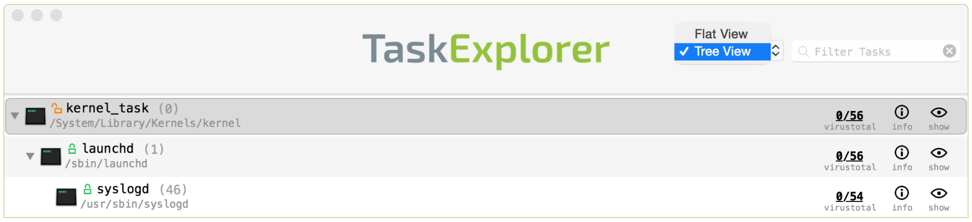


To run the application and begin exploring tasks, simply double click on 'TaskExplorer.app' The first time TaskExplorer is run, it will display an authorization prompt in order to gain necessary privileges. These privileges are required so that TaskExplorer can enumerate information about remote processes (such as loaded dylibs).



please authenticate

in a hierarchical 'Tree View' mode. Use the drop-down selected in the top right corner of the app to toggle between the two views:



kernel_task (0) /System/Library/Kernels/kernel 0/56 virustotal info show

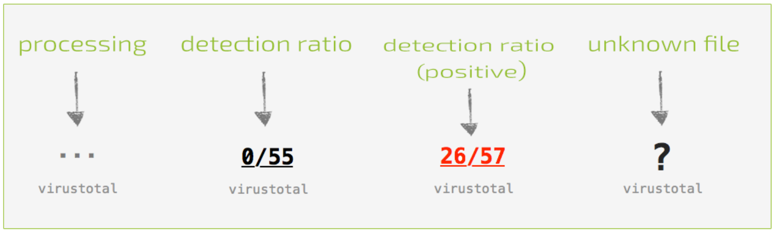
launchd (1) /sbin/launchd 0/56 virustotal info show

syslogd (46) /usr/sbin/syslogd 0/54 virustotal info show

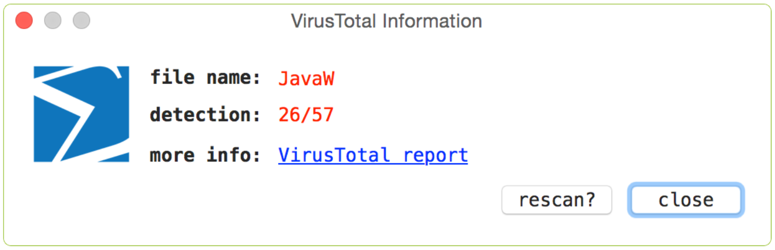
Tasks can be filtered using the 'Filter Tasks' search box, found at the top right corner of the app. Simply begin typing to filter all tasks based on their names, paths or pids. For example, typing 'Chrome' will show only tasks that contain 'Chrome' in their name or path. TaskExplorer also contains special 'hash-tag' filters that can filter tasks based on concepts such as 'all non-Apple (3rd-party) tasks' or 'all unsigned tasks' (see the **'Search and Filtering'** section below for details).

Each row the top task pane, contains the icon, name, process id (pid), and path of the task. A lock icon next to the task's name, indicates whether the task belongs to Apple, 🔒, or a 3rd-party (but still signed) 🔒, or is unsigned 🔓. On the right-hand side of each task's row are various informational and actionable buttons. These buttons provide information about item's **VirusTotal** (anti-virus) scan results, general information about the task, and the ability to view the item in Finder.

Task explorer automatically queries VirusTotal with a hash of the binary in order to retrieve any information. While VirusTotal is being queried, this button displays '■ ■ ■'. Once the query is complete, the title of the button is automatically updated with either the detection ratio, or a **'?'** if the binary is not known to VirusTotal.



With the query complete, the button can be clicked to reveal a popup containing VirusTotal-specific information about the file. If the file is unknown, clicking the 'submit?' button will submit the file for analysis. Known files contain a link to the full analysis report and a 'rescan?' button that will rescan the file. If known malware is detected, the item's name and VirusTotal button will be highlighted in red.

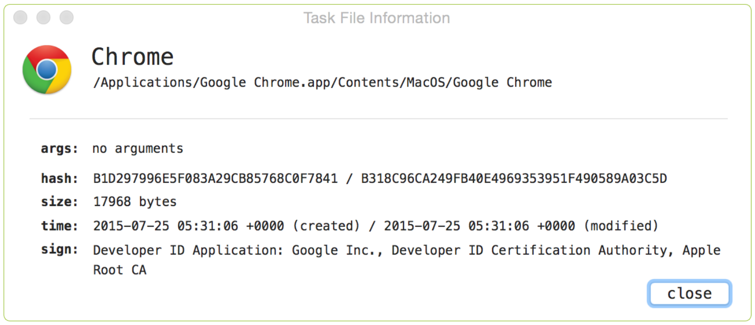


file name: JavaW

detection: 26/57

more info: VirusTotal report

The 'info' button will display detailed information about the task, including its commandline arguments, hashes, and signed status:



Chrome
/Applications/Google Chrome.app/Contents/MacOS/Google Chrome

args: no arguments

hash: B1D297996E5F083A29CB85768C0F7841 / B318C96CA249FB40E4969353951F490589A03C5D

size: 17968 bytes

time: 2015-07-25 05:31:06 +0000 (created) / 2015-07-25 05:31:06 +0000 (modified)

sign: Developer ID Application: Google Inc., Developer ID Certification Authority, Apple Root CA

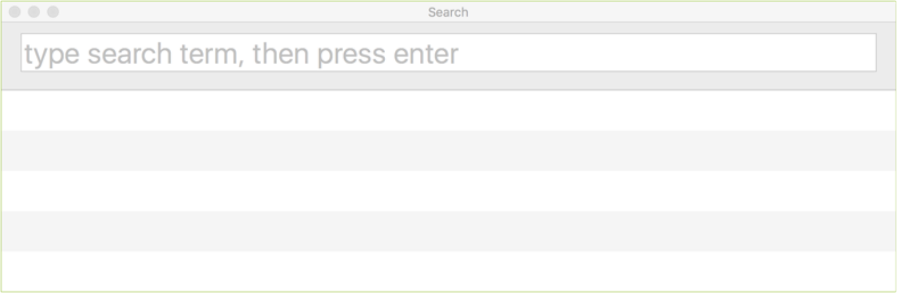
Clicking on the final button ('show') in the task's row, will show the task's binary in a Finder window.

(tasks') pane. For example, executable binaries will display a VirusTotal detection ratio, and each item (regardless of category), has an 'info' button that can be clicked to display more information about the selected item (dylib, file, or network connection).

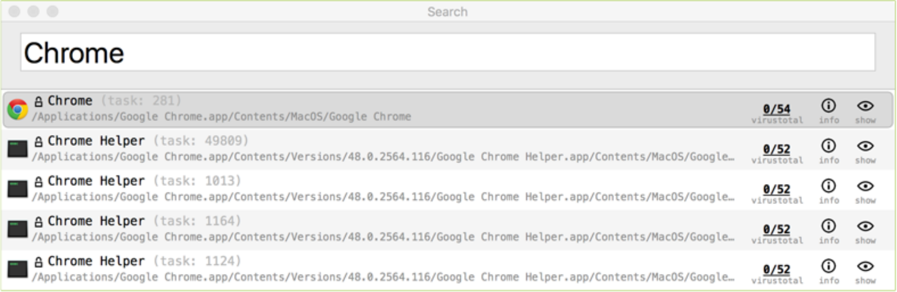
Similarly, the items can be filtered by the filter/search box found directory above the lower pane. While any item category (dylib, file, or network connection) can be filtered by simply typing in the field, the certain 'hash-tag' search filters (e.g `#nonapple`) only apply to executable binaries, and thus are only relevant when the bottom pane is displaying dylibs. The next section, 'Search and Filtering' provides more details on this.

Searching and Filtering

One of the more powerful features of TaskExplorer is its abilty to filter or search for tasks, dylibs, files, and/or network connections. As mentioned, one can search for Tasks via the 'Filter Tasks' search box (top right), as well as for a task's dylibs, files, or network connections via the filter/search box in the middle (right) of the UI above the lower pane. Note that this lower filter box will only search or filter what is currently being displayed in the lower pane. For a global search, click the 🔍 icon at the bottom left of the app to bring up the global search pane:



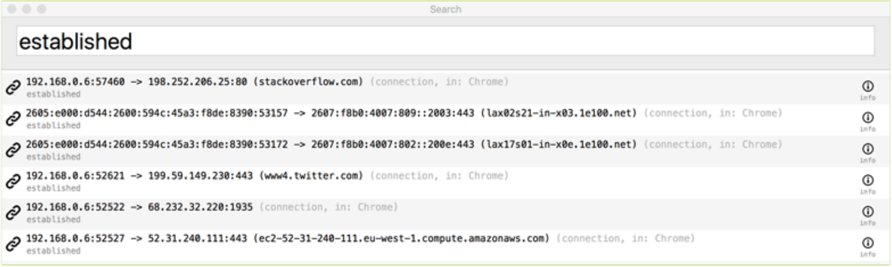
This global search, allows one to search all tasks, dylibs, files, and network connections, all at once! For example typing 'Chrome' (then hitting 'Enter') will show everything that has 'Chrome' in its path, name, etc:



```
Chrome

Chrome (task: 281)
/Applications/Google Chrome.app/Contents/MacOS/Google Chrome                                              0/54
Chrome Helper (task: 49809)
/Applications/Google Chrome.app/Contents/Versions/48.0.2564.116/Google Chrome Helper.app/Contents/MacOS/Google…   0/52
Chrome Helper (task: 1013)
/Applications/Google Chrome.app/Contents/Versions/48.0.2564.116/Google Chrome Helper.app/Contents/MacOS/Google…   0/52
Chrome Helper (task: 1164)
/Applications/Google Chrome.app/Contents/Versions/48.0.2564.116/Google Chrome Helper.app/Contents/MacOS/Google…   0/52
Chrome Helper (task: 1124)
/Applications/Google Chrome.app/Contents/Versions/48.0.2564.116/Google Chrome Helper.app/Contents/MacOS/Google…   0/52
```

Other examples including typing 'established' to view all connected network connections, or 'listening' to show all listening sockets:

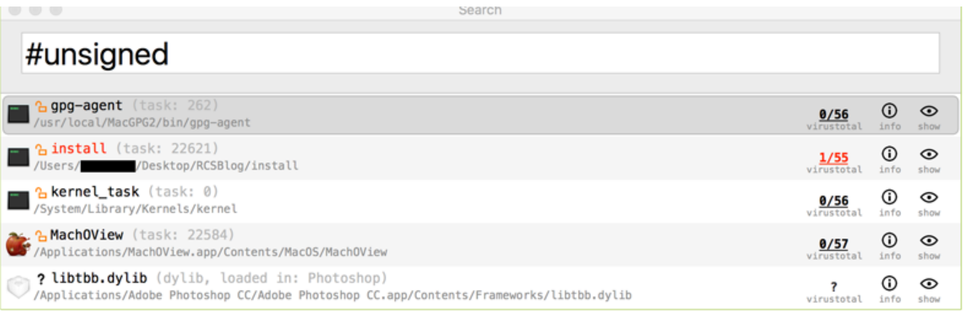


```
established

192.168.0.6:57460 -> 198.252.206.25:80 (stackoverflow.com) (connection, in: Chrome)
established
2605:e000:d544:2600:594c:45a3:f8de:8390:53157 -> 2607:f8b0:4007:809::2003:443 (lax02s21-in-x03.1e100.net) (connection, in: Chrome)
established
2605:e000:d544:2600:594c:45a3:f8de:8390:53172 -> 2607:f8b0:4007:802::200e:443 (lax17s01-in-x0e.1e100.net) (connection, in: Chrome)
established
192.168.0.6:52621 -> 199.59.149.230:443 (www4.twitter.com) (connection, in: Chrome)
established
192.168.0.6:52522 -> 68.232.32.220:1935 (connection, in: Chrome)
established
192.168.0.6:52527 -> 52.31.240.111:443 (ec2-52-31-240-111.eu-west-1.compute.amazonaws.com) (connection, in: Chrome)
established
```

TaskExplorer also contains special 'hash-tag' filters that can filter items (in any filter/search box) based on concepts such as 'all non-Apple (3rd-party) tasks' or 'all unsigned tasks' The list of current support 'hash-tag' filters includes:

- `#apple`
  only display items that belong to the OS (e.g. signed soley by Apple proper)
- `#nonapple`
  only display 3rd-party (non-OS) tasks
- `#signed`
  only display signed items
- `#unsigned`



Search

#unsigned

gpg-agent (task: 262)
/usr/local/MacGPG2/bin/gpg-agent
0/56

install (task: 22621)
/Users/[redacted]/Desktop/RCSBlog/install
1/55

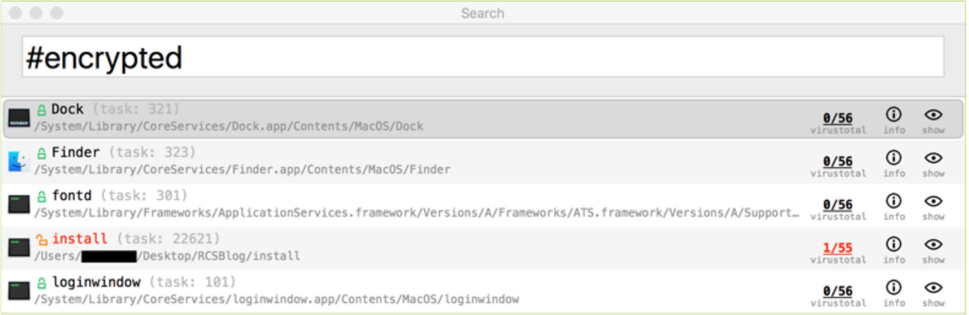
kernel_task (task: 0)
/System/Library/Kernels/kernel
0/56

MachOView (task: 22584)
/Applications/MachOView.app/Contents/MacOS/MachOView
0/57

? libtbb.dylib (dylib, loaded in: Photoshop)
/Applications/Adobe Photoshop CC/Adobe Photoshop CC.app/Contents/Frameworks/libtbb.dylib
?

- `#flagged`
  only display items flagged by VirusTotal

- `#encrypted`
  only display items flagged that are encrypted (with OSX's native encryption scheme)



Search

#encrypted

Dock (task: 321)
/System/Library/CoreServices/Dock.app/Contents/MacOS/Dock
0/56

Finder (task: 323)
/System/Library/CoreServices/Finder.app/Contents/MacOS/Finder
0/56

fontd (task: 301)
/System/Library/Frameworks/ApplicationServices.framework/Versions/A/Frameworks/ATS.framework/Versions/A/Support…
0/56

install (task: 22621)
/Users/[redacted]/Desktop/RCSBlog/install
1/55

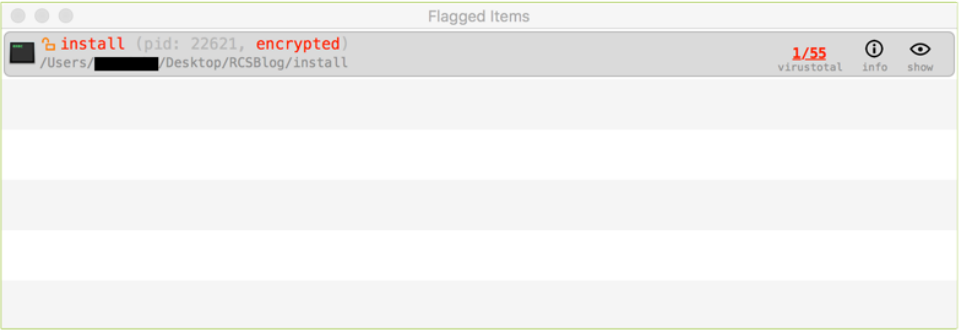
loginwindow (task: 101)
/System/Library/CoreServices/loginwindow.app/Contents/MacOS/loginwindow
0/56

- `#packed`
  only display items that are packed (note: beta, may list unpacked, but high entropy items)

- `#notfound`
  only display items are not found on disk (i.e. binaries that have self-deleted)

Flagged Items

TaskExplorer is integrated with **VirusTotal**. If any task or dynamic library is flagged (by VirusTotal) as known malware, this will be shown in the 'Flagged Items' pane. To access this pane, click the ⚑ icon at the bottom right of the app. (Note: this icon will be red (🚩) is any items have been flagged. For example, here we see TaskExplorer has flagged HackingTeam's encrypted malware installer:



Flagged Items

install (pid: 22621, encrypted)
/Users/[redacted]/Desktop/RCSBlog/install
1/55

Commandline Interface

TaskExplorer (as of `version 2.0`), can be run via the commandline. There are various benefits to this, including the ability to programmatically enumerate or scan all running tasks and dynamic libraries. Note that TaskExplorer, when run from the commandline, must be executed as root (or via `sudo`).

Execute the TaskExplorer binary (note: specify the full path to the TaskExplorer binary *within* its application bundle) with `-h` or `-help` to display information about the self-explanatory commandline options:

```
TASKEXPLORER USAGE:
 -h or -help  display this usage info
```

```
options:
 -pretty      json output is 'pretty-printed'
 -pid [pid]   just scan/explore the specified task
 -skipVT      do not query VirusTotal (when '-explore' is specified)
 -detailed    for each task; include dylibs, files, & network connections
```

```
Note:
To capture the output from TaskExplorer, (as it writes to STDOUT), simply pipe it
to a file out of your choice:

$ ./TaskExplorer.app/Contents/MacOS/TaskExplorer -explore >
/path/to/some/file.json
```

FAQs

Q: Why is TaskExplorer asking me to enter my password?
A: In order to gather information about system tasks (such as commandline arguments and loaded dylibs), the operating system requires TaskExplorer execute with elevated privileges.