



# What's Your Sign?



↓ [Download](#)

Verifying a file's cryptographic signature can deduce its origin or trustability. Unfortunately there's no simple way to view a file's signature via the UI.

"What's Your Sign" adds a menu item to `Finder`. Simply right-, or control-click on any file to display its cryptographic signing information!



Supported OS: OS X 10.13+



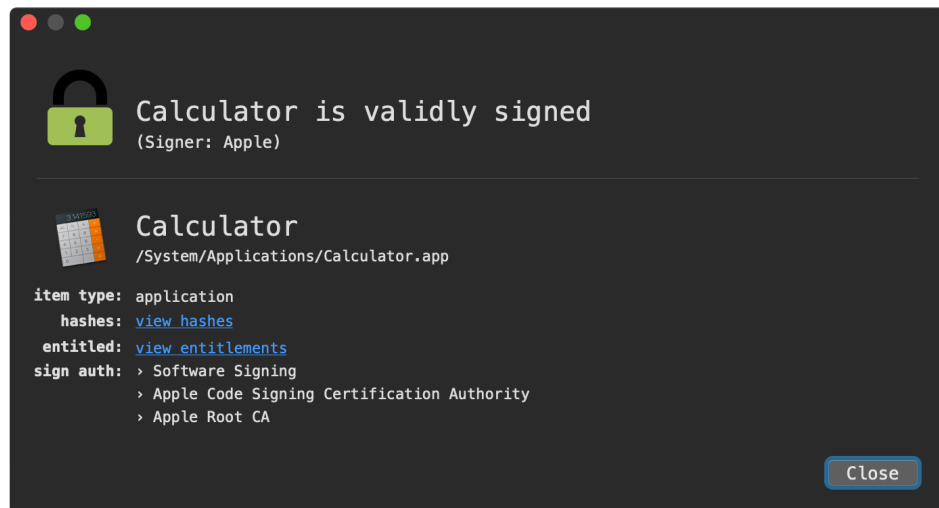
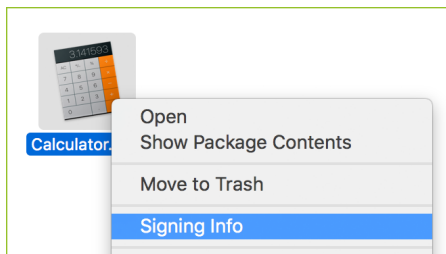
Current version: 2.2.1 ([change log](#))



Zip's SHA-1: 30C1F27A19A7C0207D6109B0CCFF99E17CBD128B



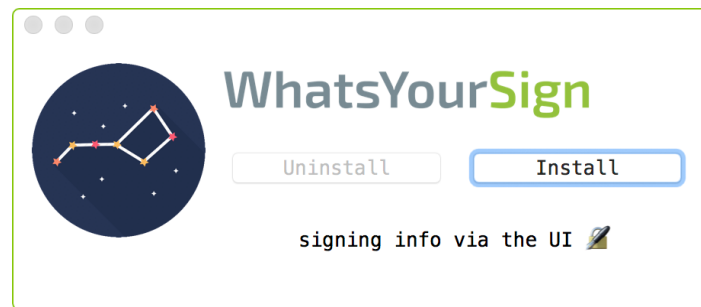
Source Code: [WhatsYourSign](#)



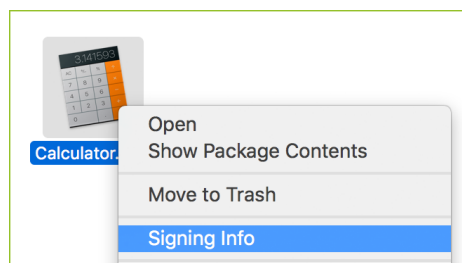
What's Your Sign is utility with a simple goal: from the UI, make it trivial to view any file's cryptographic signing information. A file or binary's cryptographic signature is important as it can determine its creator (Apple proper, a 3rd-party, etc). Moreover, it can help determine whether a file should be trusted. For example, binaries signed by Apple can (always?) be trusted, while files that are unsigned may be untrusted or even malicious.

To install What's Your Sign, first **download** the zip archive containing the application installer. Depending on your browser, you may need to manually unzip the application by double-clicking on the zipped archive:

Then, simply double-click on 'WhatsYourSign Installer.app'. Click 'Install' (or 'Upgrade') to install the tool:



Once What's Your Sign is installed, one can simply control- or right-click on any file, then select the 'Signing Info' menu option to view information about the file's cryptographic signing information.



Clicking on the 'Signing Info' menu option will display an informative window that displays the selected file's cryptographic signing information (or lack thereof). Files that are signed by Apple proper will contain a green lock icon:



**Calculator is validly signed (Apple)****Calculator.app**

/Applications/Calculator.app

**item type:** application  
**hashes:** [view hashes](#)  
**entitled:** [view entitlements](#)  
**sign auth:**

- > Software Signing
- > Apple Code Signing Certification Authority
- > Apple Root CA

close

Files that are signed, but do not belong to Apple proper (i.e are from the Mac App Store, or simply signed with an Apple Developer ID) will contain a black lock icon:

**Telegram is validly signed (Mac App Store)****Telegram.app**

/Applications/Telegram.app

**item type:** application  
**hashes:** [view hashes](#)  
**entitled:** [view entitlements](#)  
**sign auth:**

- > Apple Mac OS Application Signing
- > Apple Worldwide Developer Relations Certification Authority
- > Apple Root CA

close

Finally, files that are unsigned will contain a red unlock icon:

**OSX\_Mokes is not signed****OSX\_Mokes**

/Users/patrickw/Downloads/malware/Mokes/OSX\_Mokes

**item type:** Mach-O 64-bit executable x86\_64  
**hashes:** [view hashes](#)  
**entitled:** none  
**sign auth:** unsigned ('errSecCSUnsigned')

close

Also, signed items, whose signing certificate has been revoked, will similarly contain a red unlock icon. For example, the certificate used to sign the Transmission application (that was infected with OSX/KeRanger), was revoked by Apple:

**Transmission signed, but certificate has been revoked!**



## Transmission.app

/Users/patrickw/Downloads/malware/KeRanger/Transmission.app

item type: application  
 hashes: [view hashes](#)  
 entitled: none  
 sign auth: > Developer ID Application: POLISAN BOYA SANAYI VE TICARET ANONIM SIRKETI (Z7276PX673)  
               > Developer ID Certification Authority  
               > Apple Root CA

close

What's Your Sign will also compute hashes for any item. Note that for Application bundles the hash values represent the hash of main executable binary. Simply click on the 'view hashes' text to view an item's MD5, SHA1, and SHA256 hashes:



MD5: 11BD3D9C77E0D0B82D2C5B7E2CA96900  
 SHA1: 7FBA4F296717C8F709CD49363EC6FF0792D1AED9  
 SHA256: 3CC74F0D131431E2B3648698C75456D7B335CEB0E6320578B6B0BE8F3C596EB5

hashes

close



## Calculator.app

/Applications/Calculator.app

item type: application  
 hashes: [view hashes](#)  
 entitled: [view entitlements](#)  
 sign auth: > Software Signing  
               > Apple Code Signing Certification Authority  
               > Apple Root CA

close

For any item that is entitled, What's Your Sign will extract such entitlements. (For more information on entitlements, see Apple's [documentation](#) on the subject). Simply click on the 'view entitlements' text to view an item's entitlements. For example, here we can see the `system_shove` binary contains the all powerful `com.apple.rootless.install` entitlement:



```
{
  "com.apple.rootless.install" = 1;
}
```

entitlements

close



## system\_shove

/System/Library/PrivateFrameworks/PackageKit.framework/Versions/A/Resources/system\_sho...

item type: Mach-O 64-bit executable x86\_64  
 hashes: [view hashes](#)  
 entitled: [view entitlements](#)  
 sign auth: > Software Signing  
               > Apple Code Signing Certification Authority  
               > Apple Root CA


close

To uninstall What's Your Sign simply re-run the 'WhatsYourSign Installer.app'. Clicking the 'Uninstall' button will fully remove What's Your Sign from your mac:



# WhatsYourSign



signing info via the UI 

## FAQs

**Q:** How can I tell if What's Your Sign is installed and running?

**A:** Simply right- or control- click on any file (in Finder, the desktop, etc). If a 'Signing Info' option is available in the dropdown menu, that means What's Your Sign is installed.

One can also check if the `/Applications/WhatsYourSign.app` directory exists and contains `WhatsYourSign.appex` bundle in the `/Contents/Plugins` directory.

**Q:** Why are there multiple What's Your Sign processes running?

**A:** What's Your Sign integrates with Finder as a ("Finder Sync") plugin. The operating systems determines how/when to load the What's Your Sign plugin, and may load multiple instances of it. Thus, it's totally normal to see multiple instances of What's Your Sign running.

**Q:** Why does What's Your Sign access the network?

**A:** The system API's (e.g., `SecAssessmentTicketLookup`) used to check a file's notarization status may connect to Apple's notarization servers.