Grafting Apple Tree's

Building a useful process tree

Jaron Bradley

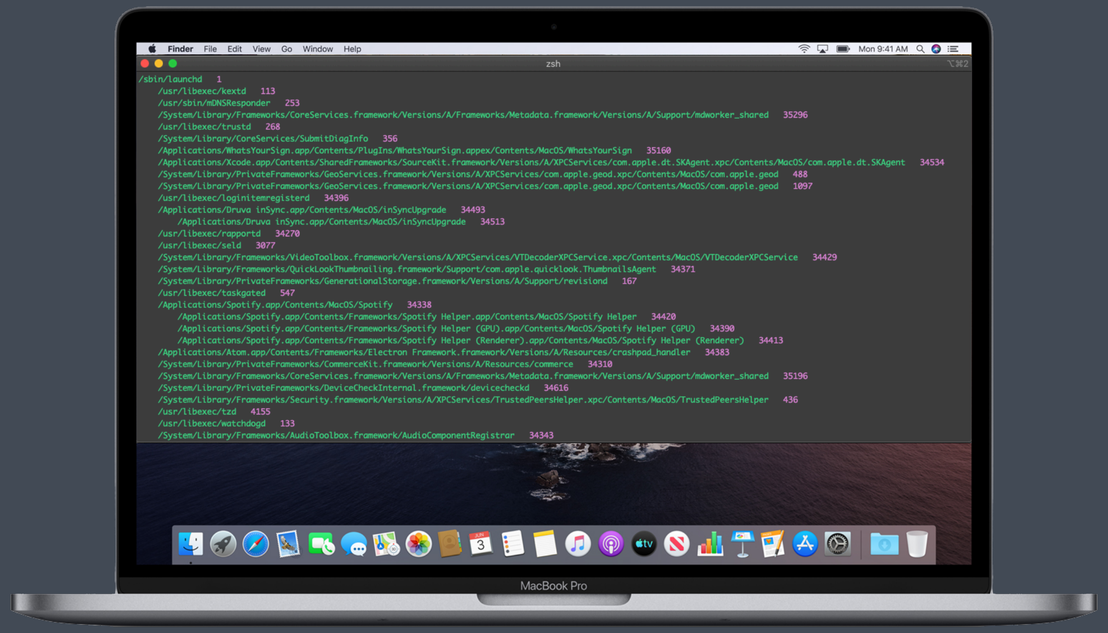
Detection R&D

Jamf Protect

jamf | PROTECT

jamf

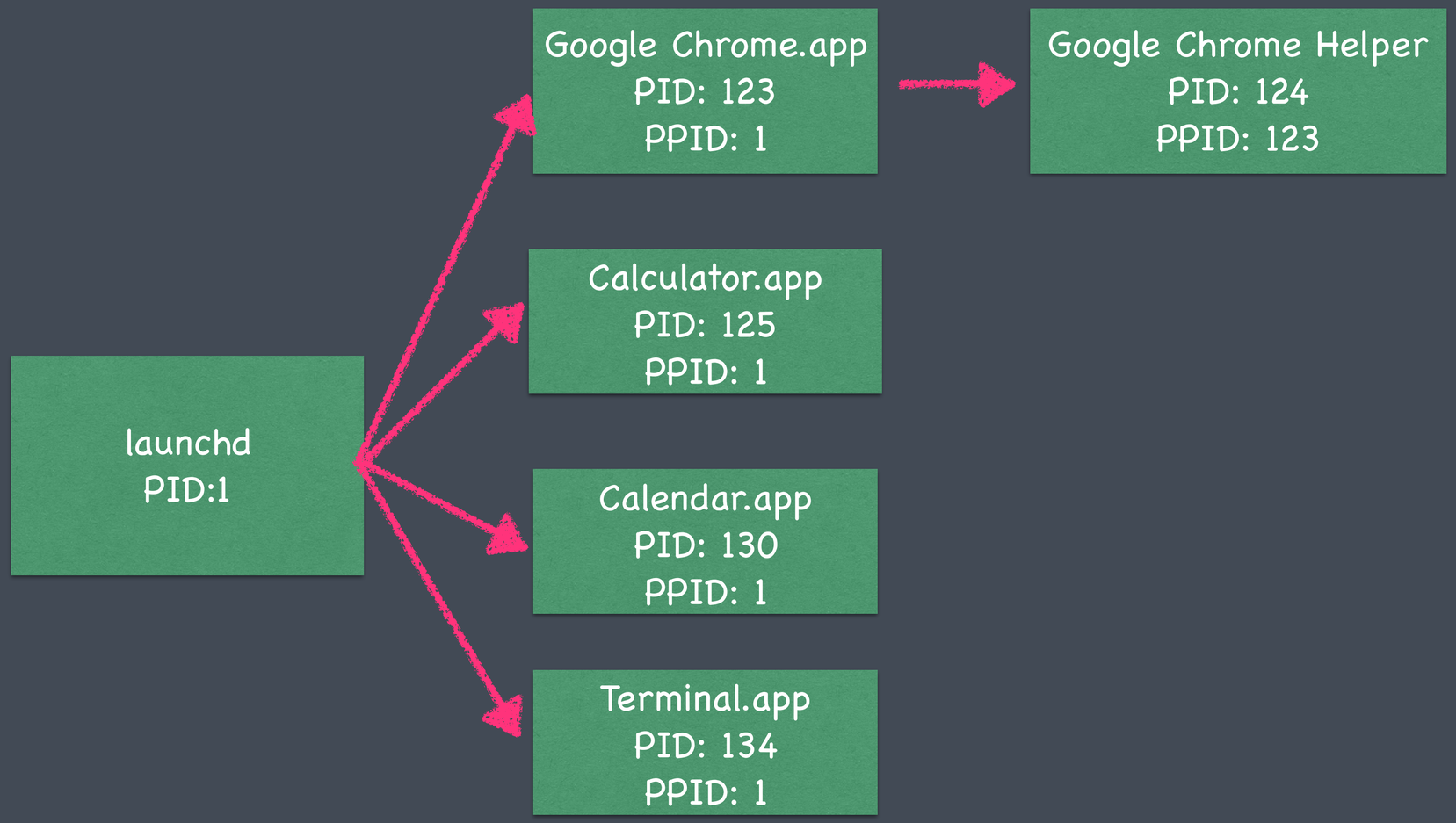
Incident Response and the Process Tree



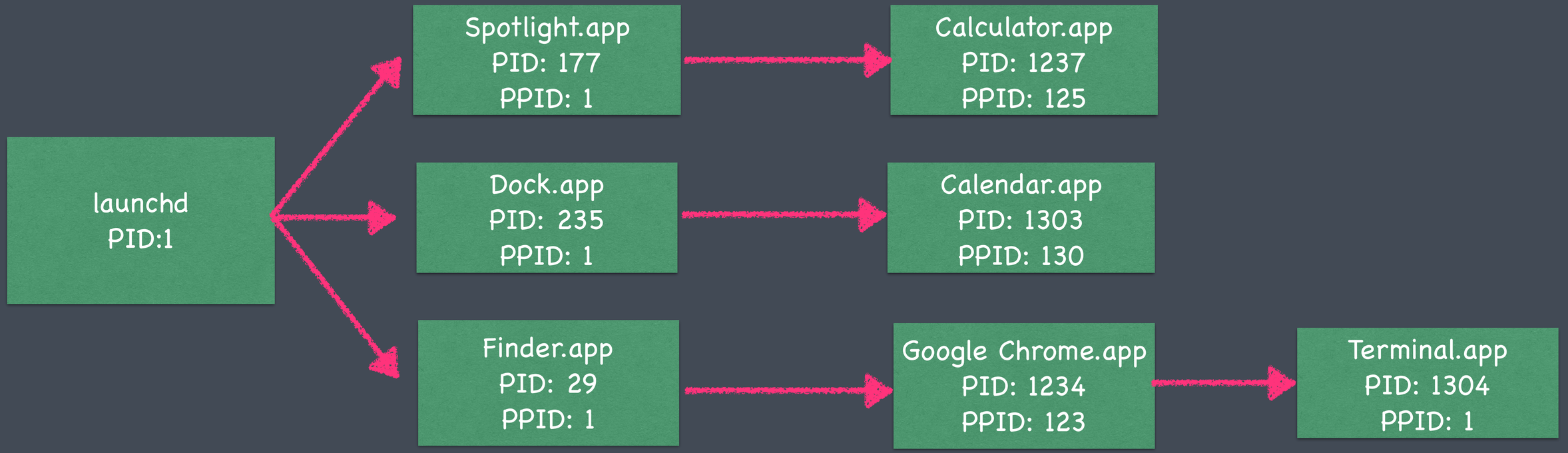





Standard Tree



A More Useful Tree



Launchctl Procinfo

```
bsd proc info = {
        pid = 34442
        unique pid = 34442
        ppid = 34421
        pgid = 34442
        status = stopped
        flags = 64-bit|has controlling tty|has controlling terminal
        uid = 501
        svuid = 501
        ruid = 501
        gid = 20
        svgid = 20
        rgid = 20
        comm name = zsh
        long name = zsh
        controlling tty devnode = 0x10000005
        controlling tty pgid = 34442
}
audit info
        session id = 100221
        uid = 501
        success mask = 0x3000
        failure mask = 0x3000
        flags = has_graphic_access,has_tty,has_console_access,has_authenticated
sandboxed = no
container = (no container)

responsible pid = 34316
responsible unique pid = 34316
responsible path = /Applications/iTerm.app/Contents/MacOS/iTerm2

pressured exit info = {
        dirty state tracked = 0
        dirty = 0
        pressured-exit capable = 0
}
```

```
        properties = {
                partial import = 0
                launchd bundle = 0
                xpc bundle = 1
                keepalive = 0
                runatload = 0
                low priority i/o = 0
                low priority background i/o = 0
                dataless file mode = 0
                legacy timer behavior = 0
                exception handler = 0
                multiple instances = 0
                supports transactions = 1
                supports pressured exit = 1
                supports idle hysteresis = 0
                enter kdp before kill = 0
                wait for debugger = 0
                app = 0
                system app = 0
                creates session = 0
                inetd-compatible = 0
                inetd listener = 0
                abandon process group = 0
                one-shot = 0
                event monitor = 0
                penalty box = 0
                pended non-demand spawn = 0
                role account = 0
                launch only once = 0
                system support = 0
                app-like = 0
                inferred program = 0
                joins gui session = 0
                joins host session = 0
                parameterized sandbox = 1
                resolve program = 0
                abandon coalition = 0
                high bits aslr = 0
                extension = 0
                nano allocator = 0
                no initgroups = 0
                start on fs mount = 0
                endpoints initialized = 1
                is copy = 0
                disallow all lookups = 0
                system service = 0
                protected by submitter = 0
        }
```

Responsible Pid

Slack	1377	0.1	4:27.42	32	0	0.0	0.00	jbradley
Slack Helper (Renderer)	1438	0.6	2:12.55	21	5	0.0	0.00	jbradley
Slack Helper (GPU)	1412	0.4	6:13.37	10	5	0.1	4:51.76	jbradley
Slack Helper	2658	0.0	39.74	10	0	0.0	0.00	jbradley
Slack Helper	1432	0.0	52.57	7	0	0.0	0.00	jbradley
com.apple.audio.SandboxHelper	2659	0.0	0.01	2	0	0.0	0.00	jbradley
MTLCompilerService	1464	0.0	0.08	2	0	0.0	0.00	jbradley
VTDecoderXPCService	1439	0.0	0.06	2	0	0.0	0.00	jbradley
com.apple.audio.SandboxHelper	2939	0.0	0.01	2	0	0.0	0.00	jbradley
SystemUIServer	1393	0.1	8.04	4	0	0.0	0.00	jbradley
MTLCompilerService	3594	0.0	0.05	2	0	0.0	0.00	jbradley
screencapture	6131		0.12	3	0	0.0	0.00	jbradley
fseventsd	116	0.1	1:15.51	11	2	0.0	0.00	root
UserEventAgent	515	0.1	6.98	3	0	0.0	0.00	jbradley

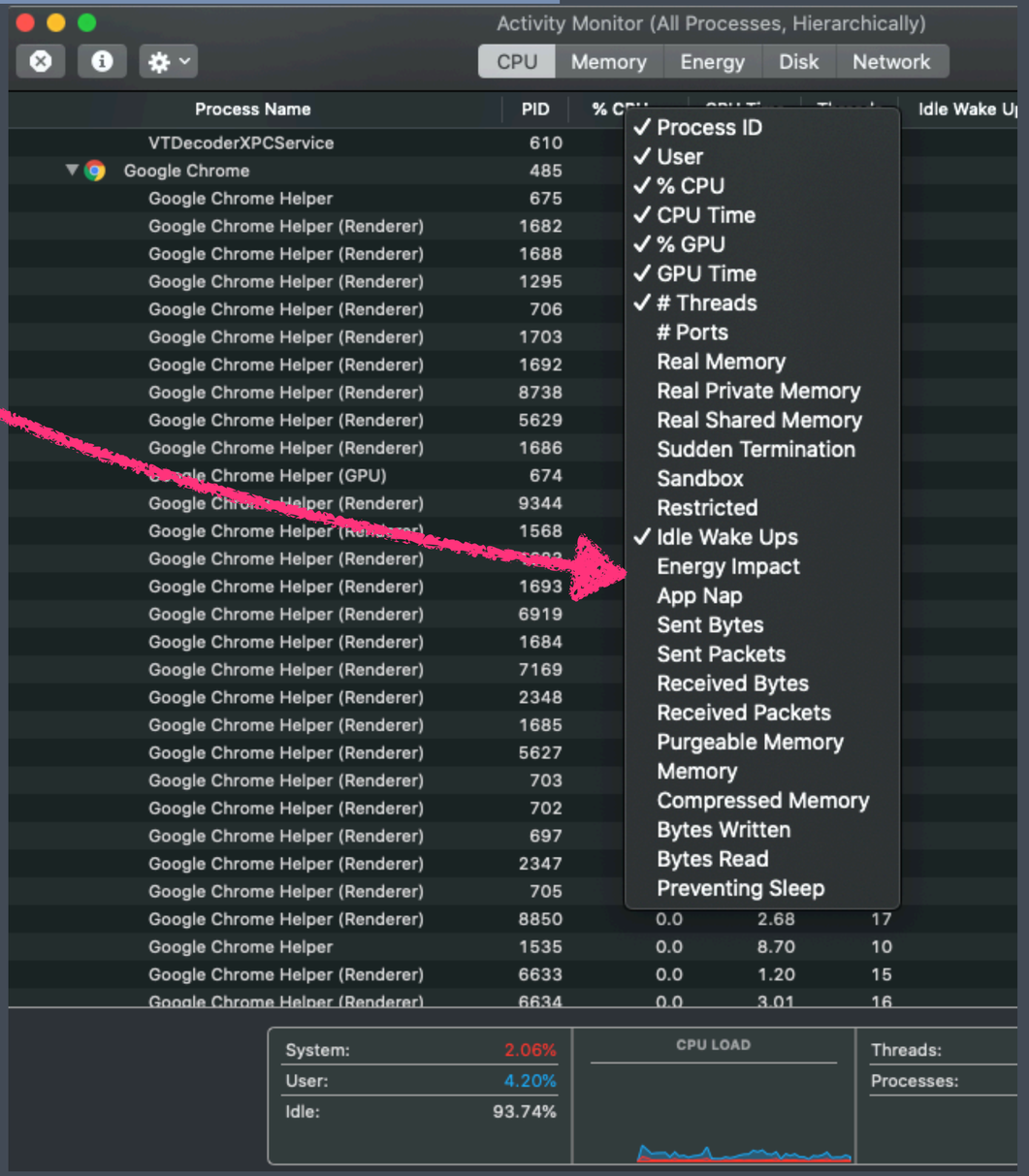
```
jbradley@sophistafunk Debug % ps -eo pid=,ppid=,command= | grep 2939  | grep -v grep
 2939     1 /System/Library/Frameworks/AudioToolbox.framework/XPCServices/com.apple.audio.SandboxHelper.xpc/Contents/MacOS/com.apple.audio.SandboxHelper
```

Responsible Pid

```
$ sudo launchctl procinfo 2939

bsd proc info = {
    pid = 2939
    unique pid = 2939
    ppid = 1   Wat?
    pgid = 2939
}
responsible pid = 1377  heh?
responsible unique pid = 1377
responsible path = /Applications/Slack.app/Contents/MacOS/Slack
```

Responsible Pid

No PPID option!?



Path - Submitted By

```
com.apple.xpc.launchd.oneshot.0x10000008.Messages = {
        active count = 4
        copy count = 0
        one shot = 1
        path = (submitted by loginwindow.187)
        state = running
        bundle id = com.apple.iChat

        program = /System/Applications/Messages.app/Contents/MacOS/Messages
        arguments = {
                /System/Applications/Messages.app/Contents/MacOS/Messages
                -psn_0_110619
        }

        inherited environment = {
                SSH_AUTH_SOCK => /private/tmp/com.apple.launchd.D8IFICj0oY/Listeners
        }

        default environment = {
                PATH => /usr/bin:/bin:/usr/sbin:/sbin
        }
```

Path - Plist

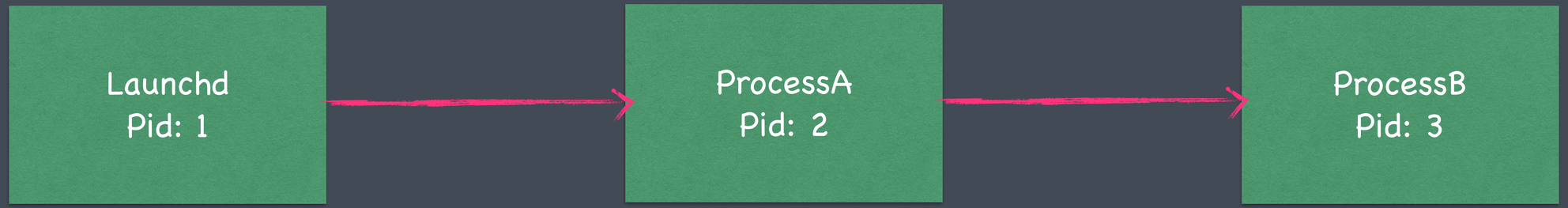
```
com.apple.Dock.agent = {
        active count = 14
        copy count = 0
        one shot = 0
        path = /System/Library/LaunchAgents/com.apple.Dock.plist
        state = running
```

Dead Pids as Parents

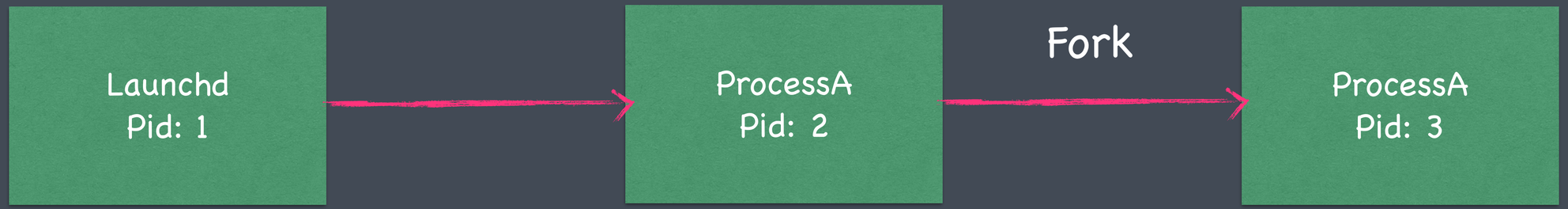
```
com.googlecode.iterm2.17084 = {
        active count = 5
        copy count = 0
        one shot = 0
        path = (submitted by Autoupdate.37758)
        state = running
        bundle id = com.googlecode.iterm2

        program = /Applications/iTerm.app/Contents/MacOS/iTerm2
        arguments = {
                /Applications/iTerm.app/Contents/MacOS/iTerm2
        }
```

```
>>> sudo launchctl procinfo 37758
program path = (could not resolve path)
Could not print Mach info for pid 37758: 0x5
Could not get proc info PID 37758: 3: No such process
auditon(): 3: No such process

Could not get responsible PID for PID 37758: 3: No such process

proc_get_dirty(): 3: No such process


entitlements = (no entitlements)

Could not get code signing info: 3: No such process

(pid 37758 is not managed by launchd)

>>>
```

Filling in the Blanks - Fork/Exec

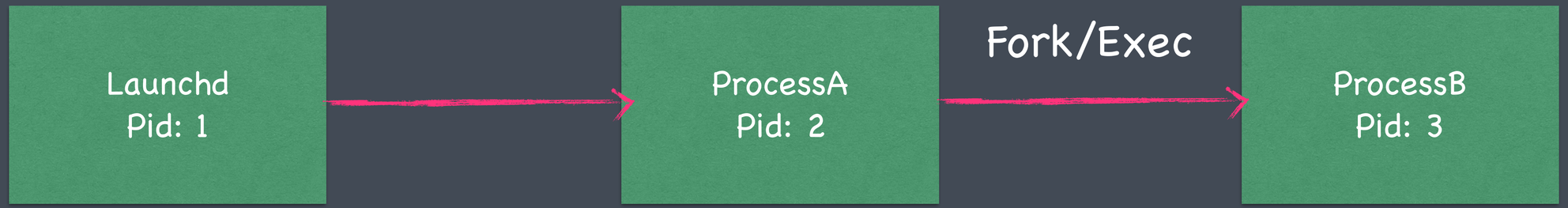


Filling in the Blanks -> Fork

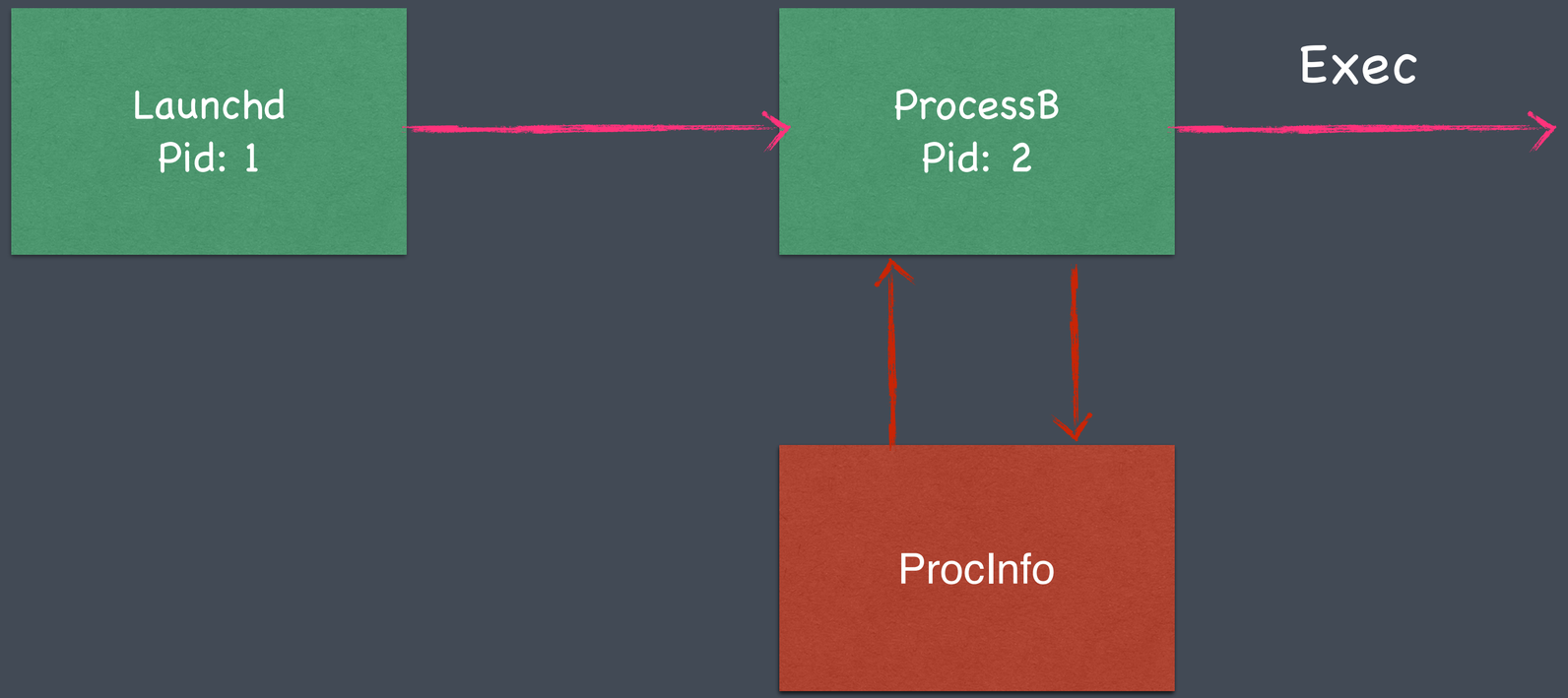


Filling in the Blanks -> Exec

Filling in the Blanks -> Fork+Exec



Finding True Parents of Exec'ed Parents



jamf

Introducing TrueTree

- Command Line Based
- Lightweight
- Fast
- Open Source Swift
- “Post Mortem” Analysis
- Great for IR Engagements
- Requires Root :(

TRUETREE

TrueTree --standard

```
/sbin/launchd   1
    /Applications/Xcode.app/Contents/Frameworks/IDEFoundation.framework/Versions/A/XPCServices/com.apple.dt.Xcode.KeychainService.xpc/Co
    /System/Library/Frameworks/QuickLook.framework/Versions/A/XPCServices/QuickLookSatellite.xpc/Contents/MacOS/QuickLookSatellite   585
    /Applications/VMware Fusion.app/Contents/Library/vmnet-netifup   15883
    /usr/libexec/lsd   258
    /usr/libexec/nsurlsessiond   260
    /usr/libexec/seld   16336
    /System/Library/PrivateFrameworks/PackageKit.framework/Versions/A/Resources/system_installd   997
    /System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService   1567
    /usr/libexec/trustd   270
    /System/Library/PrivateFrameworks/UserActivity.framework/Agents/useractivityd   474
```

TrueTree

```
/System/Library/LaunchDaemons/ssh.plist
    /usr/libexec/sshd-keygen-wrapper (Exec'ed into below process)   50010
        /usr/sbin/sshd   50010
            /usr/sbin/sshd   50014
            /bin/zsh   50015
            /bin/dash   50018
/Library/Apple/System/Library/CoreServices/SafariSupport.bundle/Contents/Resources/com.apple.SafariCloudHistoryPushAgent.plist
    /Library/Apple/System/Library/CoreServices/SafariSupport.bundle/Contents/MacOS/SafariCloudHistoryPushAgent   12015
/Applications/WhatsYourSign.app/Contents/PlugIns/WhatsYourSign.appex/Contents/MacOS/WhatsYourSign   10672
/System/Library/Input Methods/PressAndHold.app/Contents/PlugIns/PAH_Extension.appex/Contents/MacOS/PAH_Extension   515
/System/Library/LaunchDaemons/com.apple.ocspd.plist
    /usr/sbin/ocspd   11870
/System/Library/PrivateFrameworks/GeoServices.framework/Versions/A/XPCServices/com.apple.geod.xpc/Contents/MacOS/com.apple.geod   261
/Applications/Cisco Webex Meetings.app/Contents/MacOS/Cisco Webex Meetings (TrueParent:46639 "PTUpdate" has Terminated)
    /Applications/Cisco Webex Meetings.app/Contents/PlugIns/webexmta.app/Contents/MacOS/webexmta   46712
    /Applications/Cisco Webex Meetings.app/Contents/MacOS/CiscoSparkHelper   46743
/System/Library/LaunchAgents/com.apple.parsecd.plist
    /System/Library/PrivateFrameworks/CoreParsec.framework/parsecd   441
```

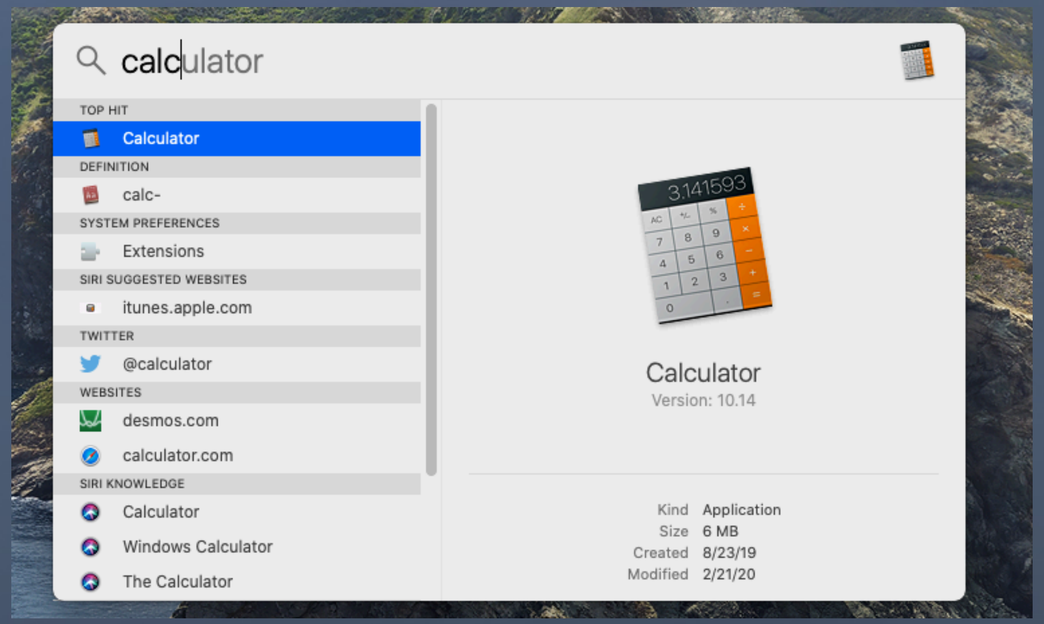
TrueTree --timestamps

```
/sbin/launchd   1   2020-02-11 02:09:27 +0000
    /System/Library/LaunchDaemons/com.apple.MobileFileIntegrity.plist
        /usr/libexec/amfid   180   2020-02-11 02:09:36 +0000
    /System/Library/Frameworks/CoreMediaIO.framework/Versions/A/XPCServices/com.apple.cmio.registerassistantservice.xpc/Contents/MacOS/com.apple.cmio.registerassistantservice   3
    /System/Library/LaunchDaemons/com.apple.opendirectoryd.plist
        /usr/libexec/opendirectoryd   147   2020-02-11 02:09:36 +0000
    /System/Library/LaunchAgents/com.apple.cache_delete.plist
        /System/Library/PrivateFrameworks/CacheDelete.framework/deleted   497   2020-02-11 02:09:52 +0000
    /System/Library/LaunchAgents/com.apple.mdworker.shared.plist
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   2244   2020-02-11 04:09:58 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   1290   2020-02-11 02:12:54 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   2246   2020-02-11 04:09:58 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   1994   2020-02-11 03:31:24 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   2338   2020-02-11 04:13:37 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   2033   2020-02-11 03:35:52 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   2124   2020-02-11 03:41:36 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   2242   2020-02-11 04:09:58 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   1816   2020-02-11 03:14:36 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   2133   2020-02-11 03:47:55 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   2339   2020-02-11 04:13:37 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   2243   2020-02-11 04:09:58 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   2245   2020-02-11 04:09:58 +0000
        /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Versions/A/Support/mdworker_shared   1991   2020-02-11 03:30:58 +0000
```

Use Case - Dock

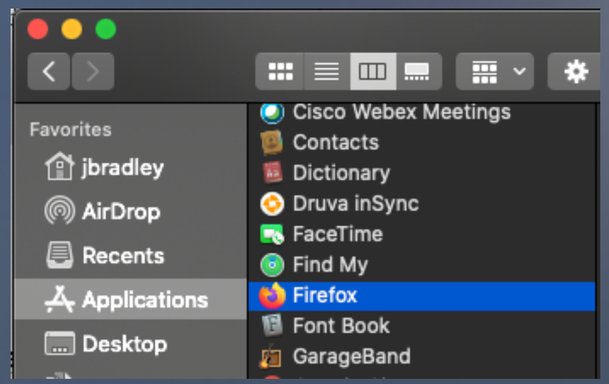
```
/System/Library/LaunchDaemons/com.apple.endpointsecurity.endpointsecurityd.plist
    /usr/libexec/endpointsecurityd    121
/System/Library/LaunchDaemons/com.apple.audio.systemsoundserverd.plist
    /usr/sbin/systemsoundserverd    547
/System/Library/LaunchAgents/com.apple.Dock.plist
    /System/Library/CoreServices/Dock.app/Contents/MacOS/Dock    537
        /System/Applications/System Preferences.app/Contents/MacOS/System Preferences    17789
            /System/Library/PrivateFrameworks/AOSUI.framework/Versions/A/XPCServices/AccountProfileRemoteViewService.xpc/Contents/MacOS/AccountProfileRemoteViewService    17790
            /System/Library/PreferencePanes/SharingPref.prefPane/Contents/XPCServices/com.apple.preferences.sharing.remoteservice.xpc/Contents/MacOS/com.apple.preferences.sharing.remote
            /System/Library/PrivateFrameworks/FindMyMac.framework/XPCServices/com.apple.HasTRB.xpc/Contents/MacOS/com.apple.HasTRB    17800
        /Applications/LastPass.app/Contents/MacOS/LastPass    1363
        /System/Applications/Utilities/Activity Monitor.app/Contents/MacOS/Activity Monitor    15253
        /Applications/Keynote.app/Contents/MacOS/Keynote    15269
            /System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService    16209
            /System/Library/Frameworks/AppKit.framework/Versions/C/XPCServices/com.apple.appkit.xpc.openAndSavePanelService.xpc/Contents/MacOS/com.apple.appkit.xpc.openAndSavePanelServ
            /System/Library/Frameworks/Quartz.framework/Versions/A/Frameworks/QuickLookUI.framework/Versions/A/XPCServices/QuickLookUIService.xpc/Contents/MacOS/QuickLookUIService    15
            /System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService    15274
        /Applications/Xcode.app/Contents/MacOS/Xcode    14983
            /Applications/Xcode.app/Contents/SharedFrameworks/DVTSourceControl.framework/Versions/A/XPCServices/com.apple.dt.Xcode.sourcecontrol.WorkingCopyScanner.xpc/Contents/MacOS/c
            /Applications/Xcode.app/Contents/Developer/Toolchains/XcodeDefault.xctoolchain/usr/lib/sourcekitd.framework/Versions/A/XPCServices/SourceKitService.xpc/Contents/MacOS/Sourc
            /Applications/Xcode.app/Contents/SharedFrameworks/XCBuild.framework/Versions/A/PlugIns/XCBBuildService.bundle/Contents/MacOS/XCBBuildService    14997
            /Applications/Xcode.app/Contents/SharedFrameworks/SourceKit.framework/Versions/A/XPCServices/com.apple.dt.SKAgent.xpc/Contents/MacOS/com.apple.dt.SKAgent    14996
            /Applications/Xcode.app/Contents/SharedFrameworks/DVTSourceControl.framework/Versions/A/XPCServices/com.apple.dt.Xcode.sourcecontrol.SSHHelper.xpc/Contents/MacOS/com.apple.
            /Applications/Xcode.app/Contents/Developer/Platforms/MacOSX.platform/Developer/Library/GPUToolsPlatform/GPUToolsAgent.app/Contents/MacOS/GPUToolsAgent    14988
            /Applications/Xcode.app/Contents/Frameworks/IDEFoundation.framework/Versions/A/XPCServices/com.apple.dt.Xcode.KeychainService.xpc/Contents/MacOS/com.apple.dt.Xcode.Keychain
        /System/Applications/Calendar.app/Contents/MacOS/Calendar    22618
```

Use Case - Spotlight




```
/System/Library/LaunchDaemons/com.apple.opendirectoryd.plist
    /usr/libexec/opendirectoryd    149
/System/Library/LaunchAgents/com.apple.cloudd.plist
    /System/Library/PrivateFrameworks/CloudKitDaemon.framework/Support/cloudd    527
/System/Library/Frameworks/Security.framework/Versions/A/XPCServices/authd.xpc/Contents/MacOS/authd    216
/System/Library/LaunchDaemons/com.apple.rapportd.plist
    /usr/libexec/rapportd    7616
/System/Library/LaunchAgents/com.apple.cloudpaird.plist
    /System/Library/CoreServices/cloudpaird    1573
/System/Library/PrivateFrameworks/AmbientDisplay.framework/Versions/A/XPCServices/com.apple.AmbientDisplayAgent.xpc/
/System/Library/LaunchAgents/com.apple.Spotlight.plist
    /System/Library/CoreServices/Spotlight.app/Contents/MacOS/Spotlight    1395
        /System/Applications/Calculator.app/Contents/MacOS/Calculator    1313
```

Use Case - Finder TrueTree




```
/System/Library/LaunchAgents/com.apple.secinitd.plist
    /usr/libexec/secinitd    426
    /usr/libexec/secinitd    1108
    /usr/libexec/secinitd    265
/System/Library/LaunchAgents/com.apple.AirPlayUIAgent.plist
    /System/Library/CoreServices/AirPlayUIAgent.app/Contents/MacOS/AirPlayUIAgent    704
/System/Library/LaunchAgents/com.apple.Finder.plist
    /System/Library/CoreServices/Finder.app/Contents/MacOS/Finder    543
        /Applications/Firefox.app/Contents/MacOS/firefox    18253
            /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container    18257
            /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container    18255
            /System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService
            /Applications/Firefox.app/Contents/MacOS/plugin-container.app/Contents/MacOS/plugin-container    18256
            /Applications/Firefox.app/Contents/MacOS/updater.app/Contents/MacOS/org.mozilla.updater    18276
        /System/Library/Frameworks/AudioToolbox.framework/XPCServices/com.apple.audio.SandboxHelper.xpc/Contents/MacOS/com.apple.audio.S
        /System/Library/Frameworks/Quartz.framework/Versions/A/Frameworks/QuickLookUI.framework/Versions/A/XPCServices/QuickLookUIServic
/System/Library/LaunchAgents/com.apple.TextInputMenuAgent.plist
    /System/Library/CoreServices/TextInputMenuAgent.app/Contents/MacOS/TextInputMenuAgent    709
/System/Library/LaunchDaemons/com.apple.tailspind.plist
    /usr/libexec/tailspind    4864
```

Use Case - Login Windows

```
/System/Library/LaunchDaemons/com.apple.loginwindow.plist
    /System/Library/CoreServices/loginwindow.app/Contents/MacOS/loginwindow    185
        /Applications/Spotify.app/Contents/MacOS/Spotify    519
        /System/Applications/Mail.app/Contents/MacOS/Mail    500
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    1557
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    13131
            /System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService    1574
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    13130
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    13132
            /System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService    1544
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    1528
            /System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService    1567
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    1529
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    13133
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    1556
            /System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompilerService.xpc/Contents/MacOS/MTLCompilerService    1545
        /Applications/Slack.app/Contents/MacOS/Slack    467
            /System/Library/Frameworks/AudioToolbox.framework/XPCServices/com.apple.audio.SandboxHelper.xpc/Contents/MacOS/com.apple.audio.SandboxHelper    1356
            /System/Library/Frameworks/VideoToolbox.framework/Versions/A/XPCServices/VTDecoderXPCService.xpc/Contents/MacOS/VTDecoderXPCService    576
            /System/Library/Frameworks/AppKit.framework/Versions/C/XPCServices/SandboxedServiceRunner.xpc/Contents/MacOS/SandboxedServiceRunner    1334
            /Applications/Slack.app/Contents/Frameworks/Slack Helper (Renderer).app/Contents/MacOS/Slack Helper (Renderer)    15232
            /Applications/Slack.app/Contents/Frameworks/Slack Helper (GPU).app/Contents/MacOS/Slack Helper (GPU)    564
```

Use Case - Open

```
/Applications/Safari.app/Contents/MacOS/Safari (TrueParent:16095 "open" has Terminated)
    /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent
    /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent
    /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.Networking.xpc/Contents/MacOS/com.apple.WebKit.Networking
```

Use Case - AppleScript

```
/sbin/launchd   1
    /System/Library/Frameworks/Security.framework/Versions/A/XPCServices/authd.xpc/Contents/MacOS/authd   216
    /Library/Developer/PrivateFrameworks/CoreSimulator.framework/Versions/A/XPCServices/SimulatorTrampoline.xpc/Contents/MacOS/SimulatorTrampoline   2789
    /Applications/Safari.app/Contents/MacOS/Safari (TrueParent:3401 "osascript" has Terminated)
        /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.Networking.xpc/Contents/MacOS/com.apple.WebKit.Networking   3404   2020-02-18 19:50:16 +0000
        /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent   3407   2020-02-18 19:50:17 +0000
        /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent   3403   2020-02-18 19:50:16 +0000
    /System/Library/LaunchAgents/com.apple.powerchime.plist
        /System/Library/CoreServices/PowerChime.app/Contents/MacOS/PowerChime   2067   2020-02-18 18:18:00 +0000
    /System/Library/LaunchDaemons/com.apple.dasd-OSX.plist
```

Use Case - SSH Standard

```
/System/Library/DriverExtensions/AppleUserHIDDrivers.dext/AppleUserHIDDrivers    16658
/System/Library/CoreServices/NotificationCenter.app/Contents/XPCServices/com.apple.notificationcenterui.WeatherSummary.xpc
/Applications/WhatsYourSign.app/Contents/PlugIns/WhatsYourSign.appex/Contents/MacOS/WhatsYourSign    15281
/System/Library/PrivateFrameworks/ApplePushService.framework/apsd    149
/usr/libexec/hidd    172
/usr/libexec/coreduetd    144
/usr/sbin/sshd    16850
    /usr/sbin/sshd    16854
        /bin/zsh    16855
            /bin/dash    16860
/usr/libexec/pboard    439
/System/Library/Frameworks/GSS.framework/Helpers/GSSCred    373
/System/Library/PrivateFrameworks/AppleMediaServices.framework/Versions/A/Resources/amsaccountsd    710
```

Use Case - SSH TrueTree

```
/System/Library/LaunchDaemons/ssh.plist
    /usr/libexec/sshd-keygen-wrapper (Exec'ed into below process)   50010
        /usr/sbin/sshd   50010
            /usr/sbin/sshd   50014
            /bin/zsh   50015
            /bin/dash   50018
/Library/Apple/System/Library/CoreServices/SafariSupport.bundle/Contents/Resources/com.apple.SafariCloudHistoryPushAgent.plist
    /Library/Apple/System/Library/CoreServices/SafariSupport.bundle/Contents/MacOS/SafariCloudHistoryPushAgent   12015
/Applications/WhatsYourSign.app/Contents/PlugIns/WhatsYourSign.appex/Contents/MacOS/WhatsYourSign   10672
/System/Library/Input Methods/PressAndHold.app/Contents/PlugIns/PAH_Extension.appex/Contents/MacOS/PAH_Extension   515
/System/Library/LaunchDaemons/com.apple.ocspd.plist
    /usr/sbin/ocspd   11870
/System/Library/PrivateFrameworks/GeoServices.framework/Versions/A/XPCServices/com.apple.geod.xpc/Contents/MacOS/com.apple.geod   261
/Applications/Cisco Webex Meetings.app/Contents/MacOS/Cisco Webex Meetings (TrueParent:46639 "PTUpdate" has Terminated)
    /Applications/Cisco Webex Meetings.app/Contents/PlugIns/webexmta.app/Contents/MacOS/webexmta   46712
    /Applications/Cisco Webex Meetings.app/Contents/MacOS/CiscoSparkHelper   46743
/System/Library/LaunchAgents/com.apple.parsecd.plist
    /System/Library/PrivateFrameworks/CoreParsec.framework/parsecd   441
```

Use Case - SSH Enabled

```
/System/Library/LaunchDaemons/com.apple.colorsyncd.plist
    /usr/libexec/colorsyncd    344
/System/Library/LaunchDaemons/com.apple.xpc.smd.plist
    /usr/libexec/smd    297
        /usr/libexec/sshd-keygen-wrapper (Exec'ed into below process)    17939
            /usr/sbin/sshd    17939
                /usr/sbin/sshd    17942
                /bin/zsh    17943
/System/Library/LaunchAgents/com.apple.FollowUpUI.plist
    /System/Library/PrivateFrameworks/CoreFollowUp.framework/Versions/A/Resources/F
        /System/Library/Frameworks/Metal.framework/Versions/A/XPCServices/MTLCompil
/System/Library/LaunchAgents/com.apple.homed.plist
    /System/Library/PrivateFrameworks/HomeKitDaemon.framework/Support/homed    448
```

Use Case - Launchctl Standard

launchctl submit -l com.evil.whatever -- calculator.app

```
/usr/libexec/colorsync.displayservices    343
/System/Library/CoreServices/LocationMenu.app/Contents/MacOS/LocationMenu    777
/Library/PrivilegedHelperTools/com.vmware.VMMonHelper    15902
/System/Library/PrivateFrameworks/CloudKitDaemon.framework/Support/cloudd    413
/System/Library/CoreServices/logind    166
/System/Applications/Calculator.app/Contents/MacOS/Calculator    16528
/System/Library/CoreServices/diagnostics_agent    708
/usr/sbin/securityd    153
```

Use Case - Launchctl TrueTree

```
/sbin/launchd   1
    /System/Library/LaunchDaemons/com.apple.sysmond.plist
        /usr/libexec/sysmond   362
    /System/Library/LaunchAgents/com.apple.trustd.agent.plist
        /usr/libexec/trustd   270
        /usr/libexec/trustd   410
        /usr/libexec/trustd   1003
    /System/Applications/Calculator.app/Contents/MacOS/Calculator (TrueParent:16527 "launchctl" has Terminated)
    /System/Library/LaunchAgents/com.apple.AMPLibraryAgent.plist
        /System/Library/PrivateFrameworks/AMPLibrary.framework/Versions/A/Support/AMPLibraryAgent   520
    /System/Library/LaunchDaemons/com.apple.kextd.plist
        /usr/libexec/kextd   113
```

Use Case - Office Macros Standard

```
/sbin/launchd   1
    /System/Library/PrivateFrameworks/BridgeOSSoftwareUpdate.framework/Support/bosUpdateProxy   354
    /usr/libexec/biometrickitd   386
    /usr/libexec/TouchBarServer   339
    /usr/libexec/secd   410
    /usr/libexec/sysmond   360
    /usr/libexec/trustd   409
   /System/Library/PrivateFrameworks/IMDPersistence.framework/XPCServices/IMDPersistenceAgent.xpc/Contents/MacOS/IMDPersistenceAgent   456
   /usr/libexec/airportd   277
   /System/Library/PrivateFrameworks/CloudPhotoLibrary.framework/Versions/A/Support/cloudphotod   913
   /System/Library/PrivateFrameworks/MediaRemote.framework/Support/mediaremoted   116
   /System/Library/Frameworks/Python.framework/Versions/2.7/Resources/Python.app/Contents/MacOS/Python   3883
   /System/Library/PrivateFrameworks/CacheDelete.framework/deleted   497
   /Applications/Cisco Webex Meetings.app/Contents/MacOS/Cisco Webex Meetings   3651
       /Applications/Cisco Webex Meetings.app/Contents/PlugIns/webexmta.app/Contents/MacOS/webexmta   3654
       /Applications/Cisco Webex Meetings.app/Contents/MacOS/CiscoSparkHelper   3685
   /usr/local/jamf/bin/jamfAgent   828
   /System/Library/CoreServices/CoreServicesUIAgent.app/Contents/MacOS/CoreServicesUIAgent   564
   /System/Library/CoreServices/Dock.app/Contents/XPCServices/com.apple.dock.extra.xpc/Contents/MacOS/com.apple.dock.extra   541
   /System/Library/PrivateFrameworks/IMTranscoding.framework/XPCServices/IMTranscoderAgent.xpc/Contents/MacOS/IMTranscoderAgent   1269
   /System/Library/PrivateFrameworks/CoreCDP.framework/Versions/A/Resources/cdpd   463
   /usr/libexec/routined   420
```

Use Case - Office Macros TrueTree

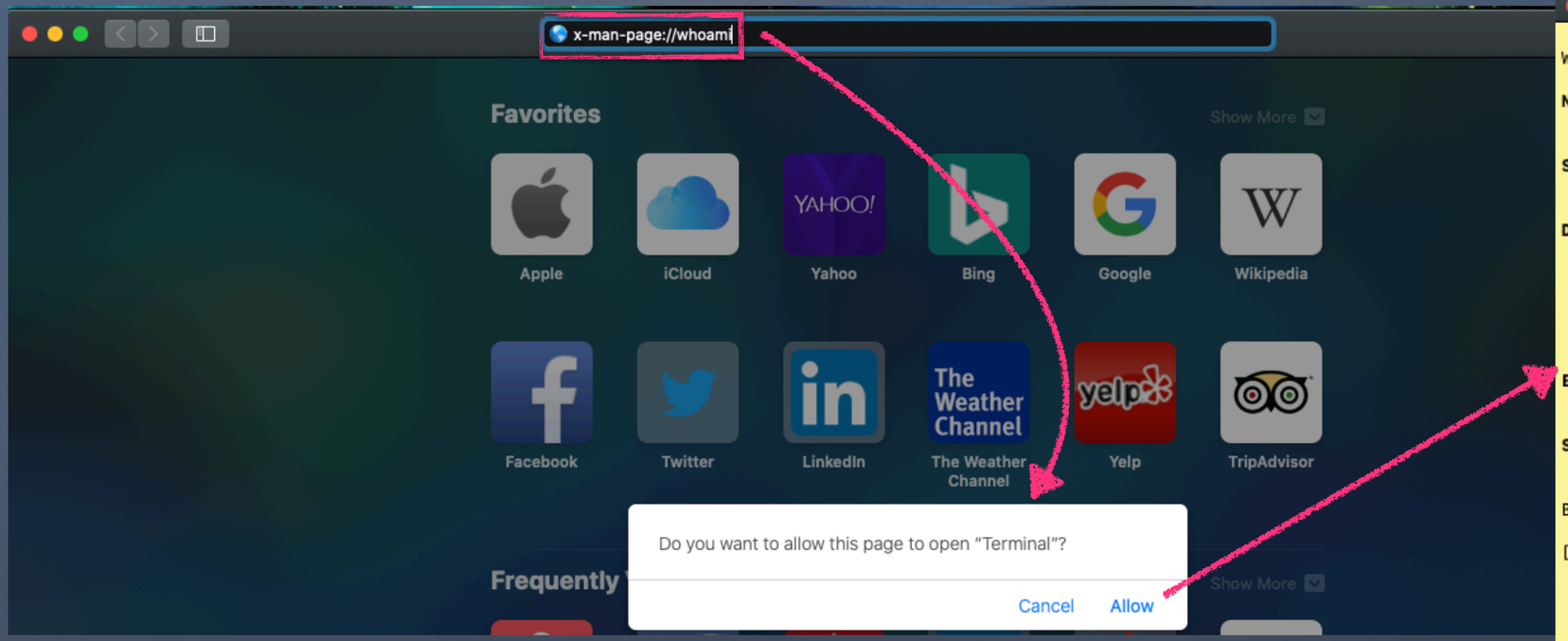
```
/sbin/launchd   1
    /System/Library/LaunchAgents/com.apple.imagent.plist
        /System/Library/PrivateFrameworks/IMCore.framework/imagent.app/Contents/MacOS/imagent   452
            /System/Library/PrivateFrameworks/IMTranscoding.framework/XPCServices/IMTranscoderAgent.xpc/Contents/MacOS/IMTranscoderAgent   1269
    /System/Library/PrivateFrameworks/ViewBridge.framework/Versions/A/XPCServices/ViewBridgeAuxiliary.xpc/Contents/MacOS/ViewBridgeAuxiliary   453
    /Library/Application Support/OpenDNS Roaming Client/com.opendns.osx.DNSCryptProxy.plist
        /Library/Application Support/OpenDNS Roaming Client/dnscrypt-proxy   2990
    /System/Library/LaunchAgents/com.apple.knowledge-agent.plist
        /usr/libexec/knowledge-agent   403
    /System/Library/LaunchAgents/com.apple.rcd.plist
        /System/Library/CoreServices/rcd.app/Contents/MacOS/rcd   2569
    /System/Library/LaunchAgents/com.apple.icloud.fmfd.plist
        /usr/libexec/fmfd   478
    /System/Library/LaunchAgents/com.apple.pluginkit.pkd.plist
        /usr/libexec/pkd   444
    /System/Library/LaunchAgents/com.apple.UserEventAgent-Aqua.plist
        /usr/libexec/UserEventAgent   401
    /System/Library/LaunchDaemons/com.apple.dprivacyd.plist
        /usr/libexec/dprivacyd   1313
    /System/Library/LaunchAgents/com.apple.CryptoTokenKit.ahp.agent.plist
        /System/Library/Frameworks/CryptoTokenKit.framework/ctkahp.bundle/Contents/MacOS/ctkahp   847
    /System/Library/LaunchAgents/com.apple.coreservices.uiagent.plist
        /System/Library/CoreServices/CoreServicesUIAgent.app/Contents/MacOS/CoreServicesUIAgent   564
            /Applications/Microsoft Excel.app/Contents/MacOS/Microsoft Excel   3872
                /System/Library/Frameworks/Python.framework/Versions/2.7/Resources/Python.app/Contents/MacOS/Python   3883
            /System/Library/PrivateFrameworks/XprotectFramework.framework/Versions/A/XPCServices/XprotectService.xpc/Contents/MacOS/XprotectService   2353
            /Library/Application Support/Microsoft/MAU2.0/Microsoft AutoUpdate.app/Contents/MacOS/Microsoft Update Assistant.app/Contents/MacOS/Microsoft Update Assistant   3876
    /System/Library/LaunchDaemons/com.apple.timezoneupdates.tzd.plist
        /usr/libexec/tzd   1368
    /System/Library/LaunchAgents/com.apple.talagent.plist
        /System/Library/CoreServices/talagent   449
```

Use Case - Time Based Assumptions

```
/System/Library/LaunchAgents/com.apple.coreservices.uiagent.plist
    /System/Library/CoreServices/CoreServicesUIAgent.app/Contents/MacOS/CoreServicesUIAgent    564    2020-02-11 02:09:56 +0000
        /Applications/Microsoft Excel.app/Contents/MacOS/Microsoft Excel    3872    2020-02-11 15:14:59 +0000
        /System/Library/PrivateFrameworks/XprotectFramework.framework/Versions/A/XPCServices/XprotectService.xpc/Contents/MacOS/XprotectService
```

```
/System/Library/LaunchDaemons/com.apple.loginwindow.plist
    /System/Library/CoreServices/loginwindow.app/Contents/MacOS/loginwindow    185    2020-02-11 02:09:36 +0000
        /System/Applications/Mail.app/Contents/MacOS/Mail    493    2020-02-11 02:09:52 +0000
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.Networking.xpc/Contents/MacOS/com.apple.WebKit.Networking    4033    2020-02-11 15:34:38 +0000
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    3868    2020-02-11 15:14:41 +0000
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    3870    2020-02-11 15:14:48 +0000
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    3867    2020-02-11 15:14:41 +0000
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    3865    2020-02-11 15:14:41 +0000
            /Library/Apple/System/Library/Frameworks/SafariServices.framework/Versions/A/XPCServices/com.apple.SafariServices.xpc/Contents/MacOS/com.apple.SafariServices    4034    2020-02-11 15:34:38 +0000
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.Networking.xpc/Contents/MacOS/com.apple.WebKit.Networking    857    2020-02-11 02:10:15 +0000
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    3864    2020-02-11 15:14:41 +0000
            /System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent    3866    2020-02-11 15:14:41 +0000
        /Applications/iTerm.app/Contents/MacOS/iTerm2    477    2020-02-11 02:09:51 +0000
            /usr/bin/login    586    2020-02-11 02:09:57 +0000
```

Use Case - WindTail



man whoami — 80×48

```
WHOAMI(1)                 BSD General Commands Manual                WHOAMI(1)

NAME
     whoami -- display effective user id

SYNOPSIS
     whoami

DESCRIPTION
     The whoami utility has been obsoleted by the id(1) utility, and is equiv-
     alent to ``id -un''.  The command ``id -p'' is suggested for normal
     interactive use.

     The whoami utility displays your effective user ID as a name.

EXIT STATUS
     The whoami utility exits 0 on success, and >0 if an error occurs.

SEE ALSO
     id(1)

BSD                             June 6, 1993                             BSD

[Process completed]
```

Use Case - URLScheme (Safari) Standard

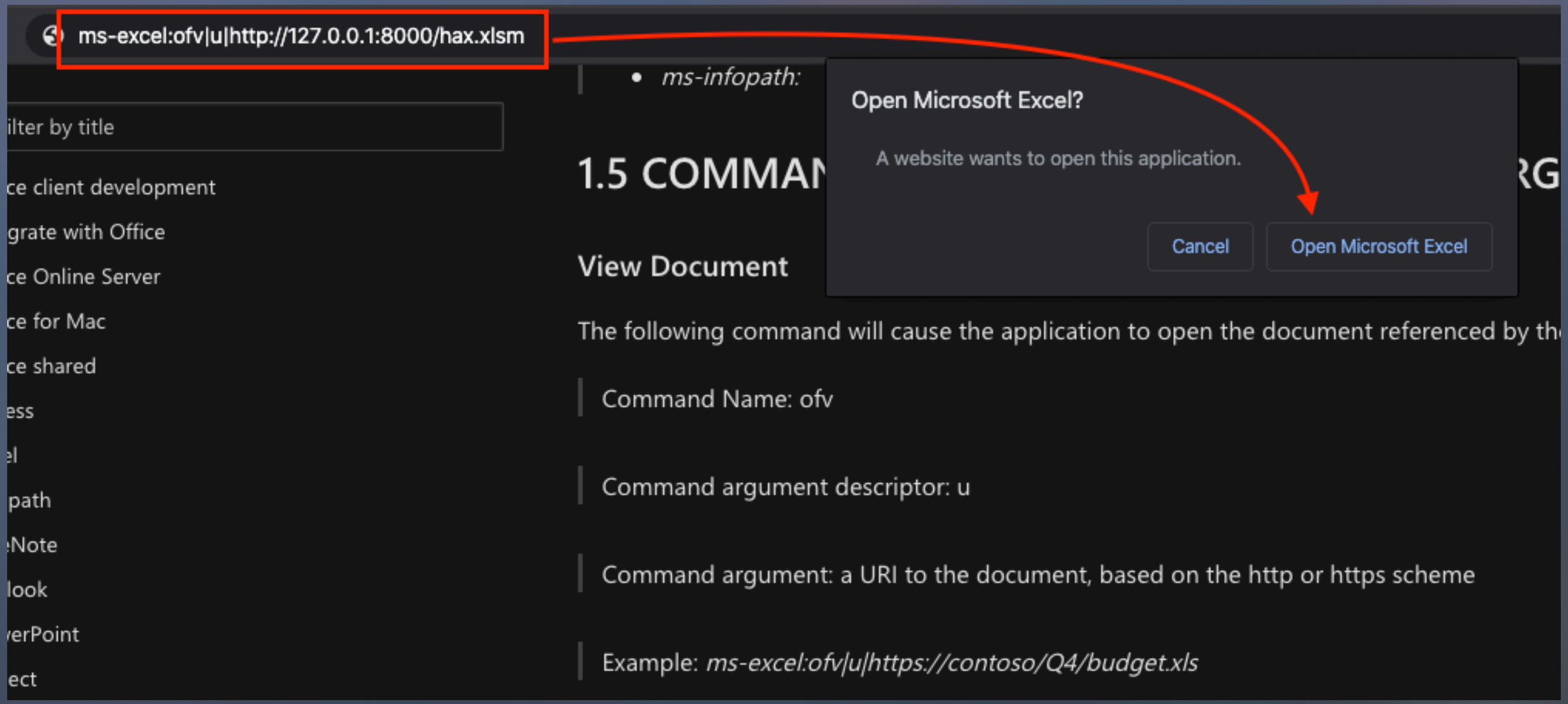
```
/sbin/launchd   1
    /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/DictionaryServices.framework/Versions/A/XPCServices/com.
    /System/Library/PrivateFrameworks/ClassKit.framework/Versions/A/progressd   616
    /usr/libexec/airportd   277
    /usr/sbin/coreaudiod   224
    /Applications/Spotify.app/Contents/Frameworks/Spotify Helper.app/Contents/MacOS/Spotify Helper   12340
    /System/Library/CoreServices/cloudpaird   839
    /System/Library/PrivateFrameworks/XprotectFramework.framework/Versions/A/XPCServices/XprotectService.xpc/Contents/MacOS/XprotectS
    /usr/libexec/coreduetd   144
    /System/Library/Frameworks/CryptoTokenKit.framework/ctkahp.bundle/Contents/MacOS/ctkahp   847
    /usr/libexec/opendirectoryd   147
    /System/Library/PrivateFrameworks/HomeKitDaemon.framework/Support/homed   442
    /usr/libexec/secinitd   1161
    /System/Applications/Utilities/Terminal.app/Contents/MacOS/Terminal   27113
    /System/Library/PrivateFrameworks/AMPLibrary.framework/Versions/A/Support/AMPLibraryAgent   499
    /usr/libexec/diskmanagementd   309
    /System/Library/PrivateFrameworks/CoreAnalytics.framework/Support/analyticsd   218
    /System/Library/PrivateFrameworks/CacheDelete.framework/deleted   497
    /System/Library/PrivateFrameworks/DeviceCheckInternal.framework/devicecheckd   3053
    /Applications/WhatsYourSign.app/Contents/PlugIns/WhatsYourSign.appex/Contents/MacOS/WhatsYourSign   19024
    /System/Library/PrivateFrameworks/CoreDuetContext.framework/Versions/A/Resources/ContextStoreAgent   443
    /System/Library/CoreServices/Dock.app/Contents/XPCServices/com.apple.dock.extra.xpc/Contents/MacOS/com.apple.dock.extra   541
```

Use Case - URLScheme (Safari)

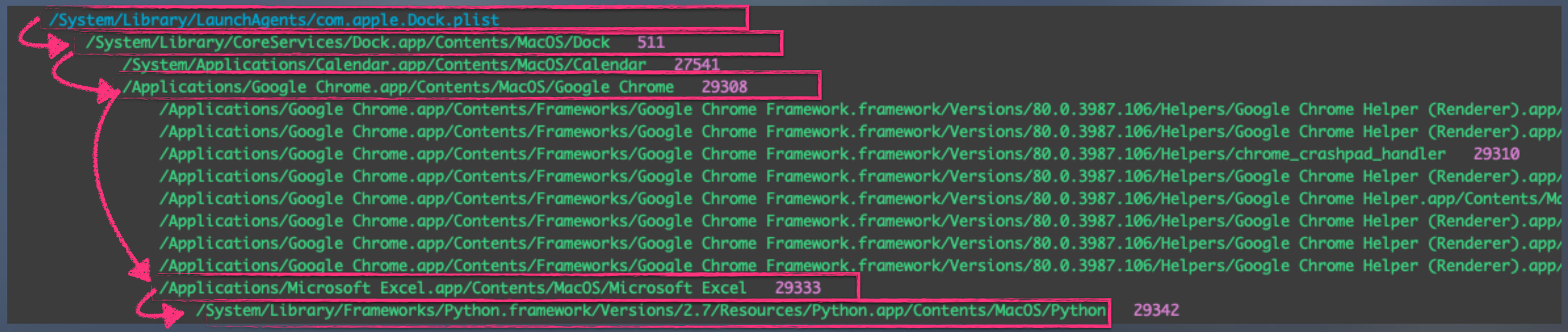
```
/sbin/launchd   1
    /System/Library/LaunchAgents/com.apple.imagent.plist
        /System/Library/PrivateFrameworks/IMCore.framework/imagent.app/Contents/MacOS/imagent   452
            /System/Library/PrivateFrameworks/IMTranscoding.framework/XPCServices/IMTranscoderAgent.xpc/Contents/MacOS/IMTranscoderAgent   1269
    /System/Library/PrivateFrameworks/ViewBridge.framework/Versions/A/XPCServices/ViewBridgeAuxiliary.xpc/Contents/MacOS/ViewBridgeAuxiliary   453
    /Library/Application Support/OpenDNS Roaming Client/com.opendns.osx.DNSCryptProxy.plist
        /Library/Application Support/OpenDNS Roaming Client/dnscrypt-proxy   2990
    /System/Library/LaunchAgents/com.apple.knowledge-agent.plist
        /usr/libexec/knowledge-agent   403
    /System/Library/LaunchAgents/com.apple.rcd.plist
        /System/Library/CoreServices/rcd.app/Contents/MacOS/rcd   2569
    /System/Library/LaunchAgents/com.apple.icloud.fmfd.plist
        /usr/libexec/fmfd   478
    /System/Library/LaunchAgents/com.apple.pluginkit.pkd.plist
        /usr/libexec/pkd   444
    /System/Library/LaunchAgents/com.apple.UserEventAgent-Aqua.plist
        /usr/libexec/UserEventAgent   401
    /System/Library/LaunchDaemons/com.apple.sandboxd.plist
        /usr/libexec/sandboxd   2914   2020-02-11 09:30:37 +0000
    /System/Library/LaunchDaemons/com.apple.CrashReporterSupportHelper.plist
        /System/Library/CoreServices/CrashReporterSupportHelper   1115   2020-02-11 02:10:54 +0000
    /System/Library/LaunchAgents/com.apple.coreservices.uiagent.plist
        /System/Library/CoreServices/CoreServicesUIAgent.app/Contents/MacOS/CoreServicesUIAgent   5465   2020-02-11 17:29:11 +0000
            /System/Applications/Utilities/Terminal.app/Contents/MacOS/Terminal   5481   2020-02-11 17:29:27 +0000
    /System/Library/LaunchAgents/com.apple.UserEventAgent-Aqua.plist
        /usr/libexec/UserEventAgent   401   2020-02-11 02:09:48 +0000
    /System/Library/LaunchAgents/com.apple.pluginkit.pkd.plist
        /usr/libexec/pkd   444   2020-02-11 02:09:49 +0000
```

Use Case - URLScheme (Chrome)

```
/Applications/Google Chrome.app/Contents/MacOS/Google Chrome (TrueParent:25863 "Google Chrome H" has Terminated)
    /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/80.0.3987.106/Helpers/Google Chrome
    /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/80.0.3987.106/Helpers/Google Chrome
    /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/80.0.3987.106/Helpers/Google Chrome
    /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/80.0.3987.106/Helpers/Google Chrome
    /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/80.0.3987.106/Helpers/Google Chrome
    /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/80.0.3987.106/Helpers/Google Chrome
    /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/80.0.3987.106/Helpers/Google Chrome
    /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/80.0.3987.106/XPCServices/AlertNoti
    /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/80.0.3987.106/Helpers/Google Chrome
    /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/80.0.3987.106/Helpers/Google Chrome
    /System/Applications/Utilities/Terminal.app/Contents/MacOS/Terminal    27396
```


ms-excel:ofv|u|http://127.0.0.1:8000/hax.xlsm
ilter by title
ce client development
grate with Office
ce Online Server
ce for Mac
ce shared
ess
el
path
Note
look
erPoint
ect
ms-infopath:
1.5 COMMAN
RG
Open Microsoft Excel?
A website wants to open this application.
Cancel
Open Microsoft Excel
View Document
The following command will cause the application to open the document referenced by th
Command Name: ofv
Command argument descriptor: u
Command argument: a URI to the document, based on the http or https scheme
Example: ms-excel:ofv|u|https://contoso/Q4/budget.xls

Use Case - URLScheme + Office Macro (Chrome) Standard



themittenmac.com

TrueTree is available for download

www.themittenmac.com

Source Code available on GitHub

Special Thanks:
Jonathan Levin
Patrick Wardle
Cyrus Ingraham
Josh Stein


jamf
Thank you
iPad mini
iPad mini
iPad mini
iPad mini
iPad mini
MacBook Pro
MacBook Pro
MacBook Pro
MacBook Pro