APPLE: REVERSE ENGINEERING AND DEMYSTIFYING *OS PRIVATE FRAMEWORKS

Daniil Nababkin (@cr7pt0pl4gu3)

OPEN SOURCE?

Apple is generally classified as a closed-source company; however, many pieces of code are open-source: https://opensource.apple.com.

There are private and public frameworks, where private are closed-source and designed to be used only by Apple themselves. Public frameworks are closed-source as well, but they are documented.

For most developers, public frameworks provide well-designed APIs and functionalities that derive stability and get constant support from Apple.

But what if we want to use private frameworks as well?

We may also want to search for security vulnerabilities and apply for a bounty: https://developer.apple.com/security-bounty/.

DYLD SHARED CACHE

*"When Apple builds *OS we take all the commonly-used dynamic libraries and pre-link them together into a single shared file."* – most apple frameworks reside in the dyld shared cache file.

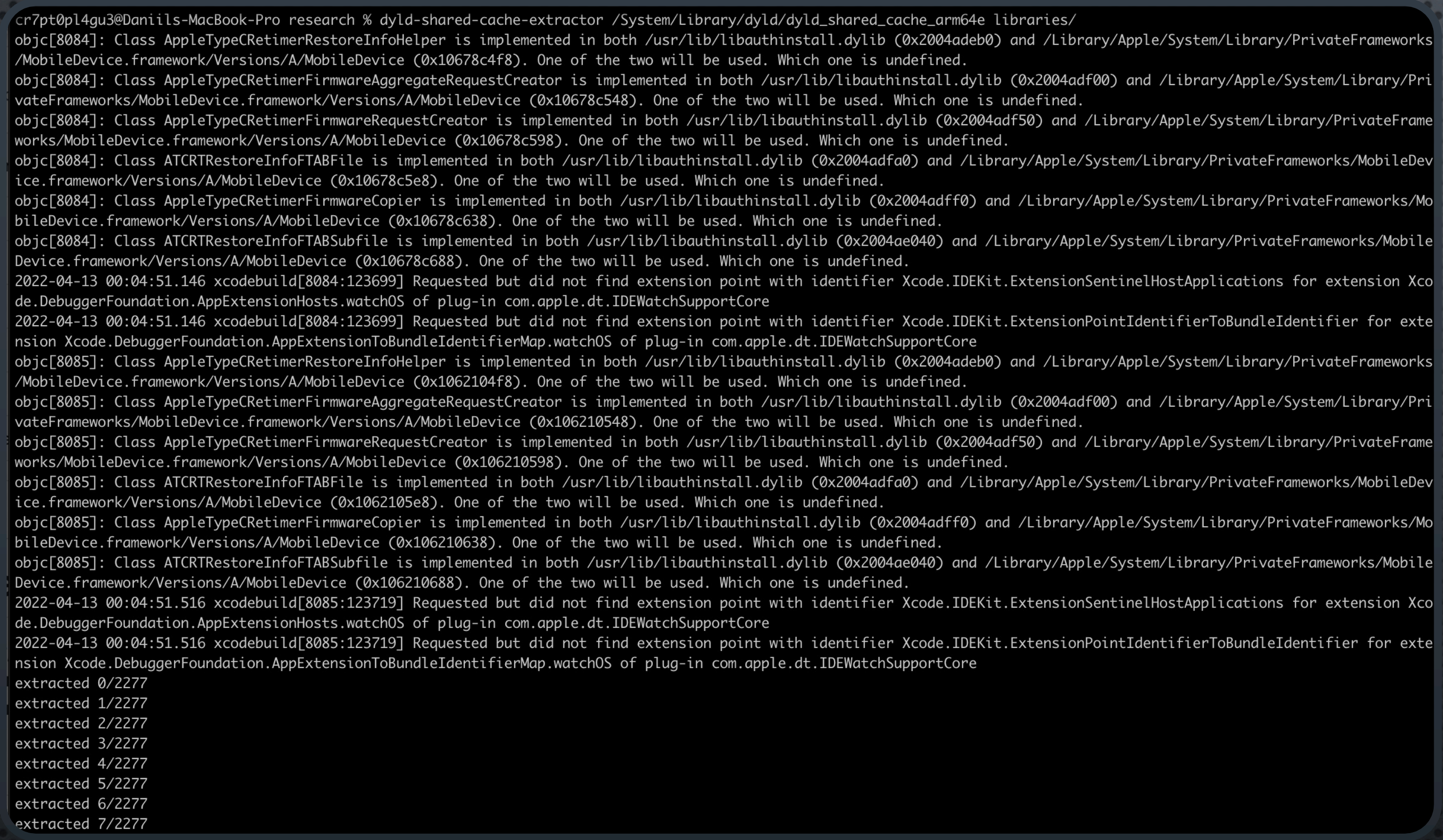
The problem arises - we can't recover the source code, headers, exports, etc.

What can we do? Let's extract the dyld shared cache and begin to reverse engineer target libraries!

EXTRACTING THE DYLD SHARED CACHE

WE WILL USE THIS PROJECT TO AID US: HTTPS://GITHUB.COM/KEITH/DYLD-SHARED-CACHE-EXTRACTOR

THE PROCESS OF EXTRACTION (ARM64 + X86_64)

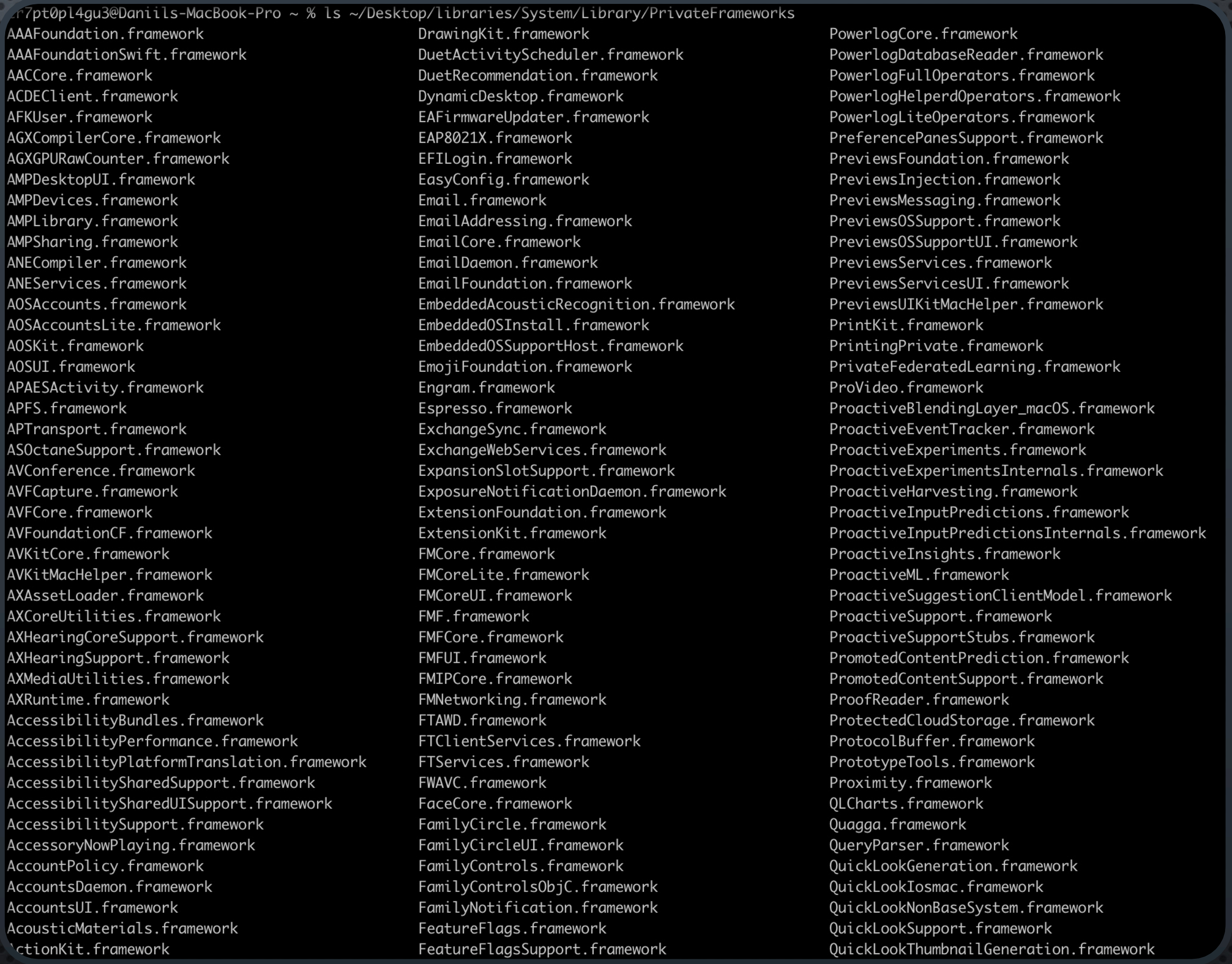


```
cr7pt0pl4gu3@Daniils-MacBook-Pro research % dyld-shared-cache-extractor /System/Library/dyld/dyld_shared_cache_arm64e libraries/
objc[8084]: Class AppleTypeCRetimerRestoreInfoHelper is implemented in both /usr/lib/libauthinstall.dylib (0x2004adeb0) and /Library/Apple/System/Library/PrivateFrameworks
/MobileDevice.framework/Versions/A/MobileDevice (0x10678c4f8). One of the two will be used. Which one is undefined.
objc[8084]: Class AppleTypeCRetimerFirmwareAggregateRequestCreator is implemented in both /usr/lib/libauthinstall.dylib (0x2004adf00) and /Library/Apple/System/Library/Pri
vateFrameworks/MobileDevice.framework/Versions/A/MobileDevice (0x10678c548). One of the two will be used. Which one is undefined.
objc[8084]: Class AppleTypeCRetimerFirmwareRequestCreator is implemented in both /usr/lib/libauthinstall.dylib (0x2004adf50) and /Library/Apple/System/Library/PrivateFrame
works/MobileDevice.framework/Versions/A/MobileDevice (0x10678c598). One of the two will be used. Which one is undefined.
objc[8084]: Class ATCRTRestoreInfoFTABFile is implemented in both /usr/lib/libauthinstall.dylib (0x2004adfa0) and /Library/Apple/System/Library/PrivateFrameworks/MobileDev
ice.framework/Versions/A/MobileDevice (0x10678c5e8). One of the two will be used. Which one is undefined.
objc[8084]: Class AppleTypeCRetimerFirmwareCopier is implemented in both /usr/lib/libauthinstall.dylib (0x2004adff0) and /Library/Apple/System/Library/PrivateFrameworks/Mo
bileDevice.framework/Versions/A/MobileDevice (0x10678c638). One of the two will be used. Which one is undefined.
objc[8084]: Class ATCRTRestoreInfoFTABSubfile is implemented in both /usr/lib/libauthinstall.dylib (0x2004ae040) and /Library/Apple/System/Library/PrivateFrameworks/Mobile
Device.framework/Versions/A/MobileDevice (0x10678c688). One of the two will be used. Which one is undefined.
2022-04-13 00:04:51.146 xcodebuild[8084:123699] Requested but did not find extension point with identifier Xcode.IDEKit.ExtensionSentinelHostApplications for extension Xco
de.DebuggerFoundation.AppExtensionHosts.watchOS of plug-in com.apple.dt.IDEWatchSupportCore
2022-04-13 00:04:51.146 xcodebuild[8084:123699] Requested but did not find extension point with identifier Xcode.IDEKit.ExtensionPointIdentifierToBundleIdentifier for exte
nsion Xcode.DebuggerFoundation.AppExtensionToBundleIdentifierMap.watchOS of plug-in com.apple.dt.IDEWatchSupportCore
objc[8085]: Class AppleTypeCRetimerRestoreInfoHelper is implemented in both /usr/lib/libauthinstall.dylib (0x2004adeb0) and /Library/Apple/System/Library/PrivateFrameworks
/MobileDevice.framework/Versions/A/MobileDevice (0x1062104f8). One of the two will be used. Which one is undefined.
objc[8085]: Class AppleTypeCRetimerFirmwareAggregateRequestCreator is implemented in both /usr/lib/libauthinstall.dylib (0x2004adf00) and /Library/Apple/System/Library/Pri
vateFrameworks/MobileDevice.framework/Versions/A/MobileDevice (0x106210548). One of the two will be used. Which one is undefined.
objc[8085]: Class AppleTypeCRetimerFirmwareRequestCreator is implemented in both /usr/lib/libauthinstall.dylib (0x2004adf50) and /Library/Apple/System/Library/PrivateFrame
works/MobileDevice.framework/Versions/A/MobileDevice (0x106210598). One of the two will be used. Which one is undefined.
objc[8085]: Class ATCRTRestoreInfoFTABFile is implemented in both /usr/lib/libauthinstall.dylib (0x2004adfa0) and /Library/Apple/System/Library/PrivateFrameworks/MobileDev
ice.framework/Versions/A/MobileDevice (0x1062105e8). One of the two will be used. Which one is undefined.
objc[8085]: Class AppleTypeCRetimerFirmwareCopier is implemented in both /usr/lib/libauthinstall.dylib (0x2004adff0) and /Library/Apple/System/Library/PrivateFrameworks/Mo
bileDevice.framework/Versions/A/MobileDevice (0x106210638). One of the two will be used. Which one is undefined.
objc[8085]: Class ATCRTRestoreInfoFTABSubfile is implemented in both /usr/lib/libauthinstall.dylib (0x2004ae040) and /Library/Apple/System/Library/PrivateFrameworks/Mobile
Device.framework/Versions/A/MobileDevice (0x106210688). One of the two will be used. Which one is undefined.
2022-04-13 00:04:51.516 xcodebuild[8085:123719] Requested but did not find extension point with identifier Xcode.IDEKit.ExtensionSentinelHostApplications for extension Xco
de.DebuggerFoundation.AppExtensionHosts.watchOS of plug-in com.apple.dt.IDEWatchSupportCore
2022-04-13 00:04:51.516 xcodebuild[8085:123719] Requested but did not find extension point with identifier Xcode.IDEKit.ExtensionPointIdentifierToBundleIdentifier for exte
nsion Xcode.DebuggerFoundation.AppExtensionToBundleIdentifierMap.watchOS of plug-in com.apple.dt.IDEWatchSupportCore
extracted 0/2277
extracted 1/2277
extracted 2/2277
extracted 3/2277
extracted 4/2277
extracted 5/2277
extracted 6/2277
extracted 7/2277
```

REVERSE ENGINEERING TOOL OF CHOICE: BINARY NINJA

A LOT OF FRAMEWORKS TO CHOOSE FROM

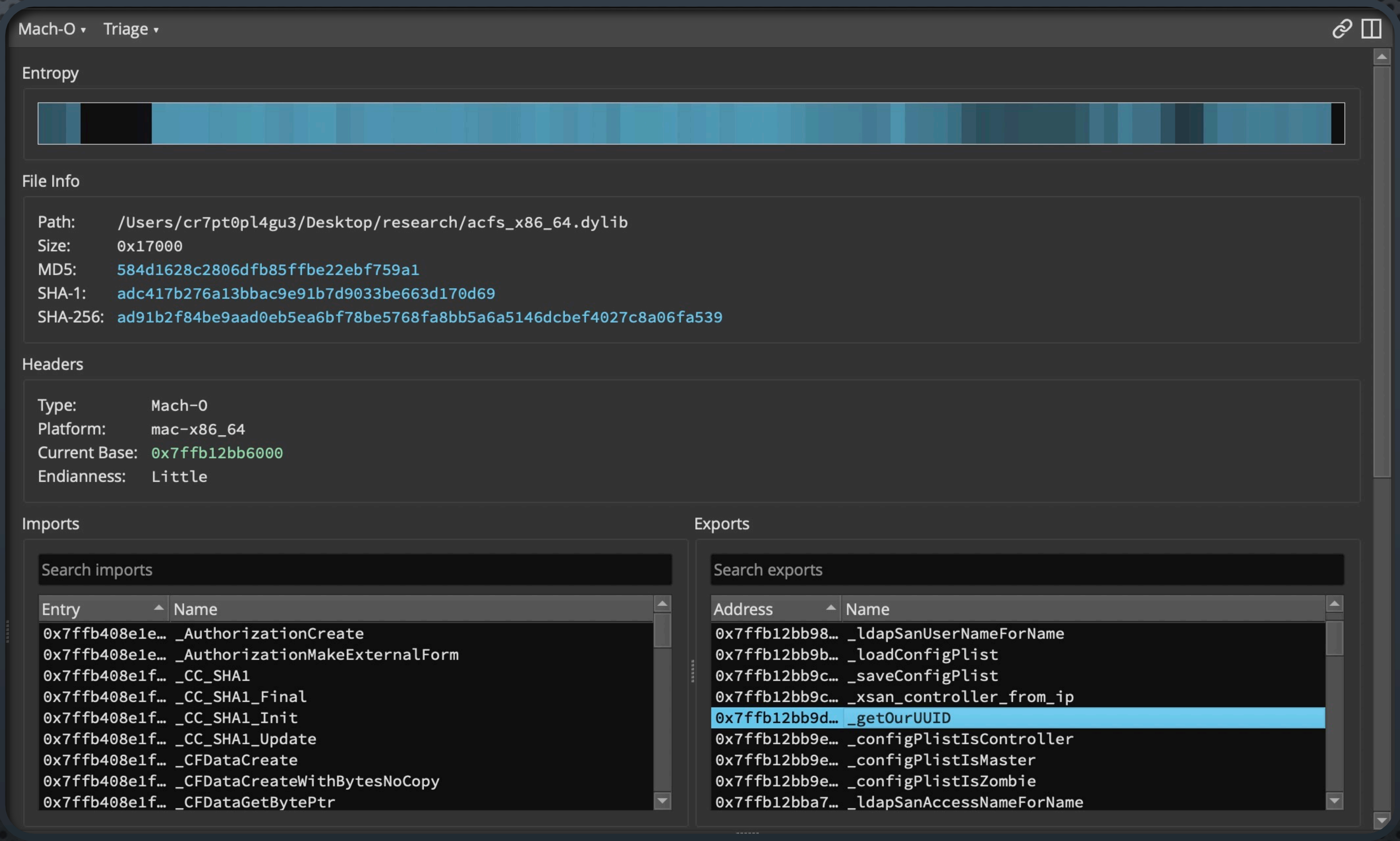
- The list on the right is not complete and only shows an exhibit of what is available
- For this presentation I decided to reverse engineer the “ACFS” and “SystemAdministration” frameworks



```
r7pt0pl4gu3@Daniils-MacBook-Pro ~ % ls ~/Desktop/libraries/System/Library/PrivateFrameworks
AAAFoundation.framework                         DrawingKit.framework                            PowerlogCore.framework
AAAFoundationSwift.framework                    DuetActivityScheduler.framework                 PowerlogDatabaseReader.framework
AACCore.framework                               DuetRecommendation.framework                    PowerlogFullOperators.framework
ACDEClient.framework                            DynamicDesktop.framework                        PowerlogHelperdOperators.framework
AFKUser.framework                               EAFirmwareUpdater.framework                     PowerlogLiteOperators.framework
AGXCompilerCore.framework                       EAP8021X.framework                              PreferencePanesSupport.framework
AGXGPURawCounter.framework                      EFILogin.framework                              PreviewsFoundation.framework
AMPDesktopUI.framework                          EasyConfig.framework                            PreviewsInjection.framework
AMPDevices.framework                            Email.framework                                 PreviewsMessaging.framework
AMPLibrary.framework                            EmailAddressing.framework                       PreviewsOSSupport.framework
AMPSharing.framework                            EmailCore.framework                             PreviewsOSSupportUI.framework
ANECompiler.framework                           EmailDaemon.framework                           PreviewsServices.framework
ANEServices.framework                           EmailFoundation.framework                       PreviewsServicesUI.framework
AOSAccounts.framework                           EmbeddedAcousticRecognition.framework           PreviewsUIKitMacHelper.framework
AOSAccountsLite.framework                       EmbeddedOSInstall.framework                     PrintKit.framework
AOSKit.framework                                EmbeddedOSSupportHost.framework                 PrintingPrivate.framework
AOSUI.framework                                 EmojiFoundation.framework                       PrivateFederatedLearning.framework
APAESActivity.framework                         Engram.framework                                ProVideo.framework
APFS.framework                                  Espresso.framework                              ProactiveBlendingLayer_macOS.framework
APTransport.framework                           ExchangeSync.framework                          ProactiveEventTracker.framework
ASOctaneSupport.framework                       ExchangeWebServices.framework                   ProactiveExperiments.framework
AVConference.framework                          ExpansionSlotSupport.framework                  ProactiveExperimentsInternals.framework
AVFCapture.framework                            ExposureNotificationDaemon.framework            ProactiveHarvesting.framework
AVFCore.framework                               ExtensionFoundation.framework                   ProactiveInputPredictions.framework
AVFoundationCF.framework                        ExtensionKit.framework                          ProactiveInputPredictionsInternals.framework
AVKitCore.framework                             FMCore.framework                                ProactiveInsights.framework
AVKitMacHelper.framework                        FMCoreLite.framework                            ProactiveML.framework
AXAssetLoader.framework                         FMCoreUI.framework                              ProactiveSuggestionClientModel.framework
AXCoreUtilities.framework                       FMF.framework                                   ProactiveSupport.framework
AXHearingCoreSupport.framework                  FMFCore.framework                               ProactiveSupportStubs.framework
AXHearingSupport.framework                      FMFUI.framework                                 PromotedContentPrediction.framework
AXMediaUtilities.framework                      FMIPCore.framework                              PromotedContentSupport.framework
AXRuntime.framework                             FMNetworking.framework                          ProofReader.framework
AccessibilityBundles.framework                  FTAWD.framework                                 ProtectedCloudStorage.framework
AccessibilityPerformance.framework              FTClientServices.framework                      ProtocolBuffer.framework
AccessibilityPlatformTranslation.framework      FTServices.framework                            PrototypeTools.framework
AccessibilitySharedSupport.framework            FWAVC.framework                                 Proximity.framework
AccessibilitySharedUISupport.framework          FaceCore.framework                              QLCharts.framework
AccessibilitySupport.framework                  FamilyCircle.framework                          Quagga.framework
AccessoryNowPlaying.framework                   FamilyCircleUI.framework                        QueryParser.framework
AccountPolicy.framework                         FamilyControls.framework                        QuickLookGeneration.framework
AccountsDaemon.framework                        FamilyControlsObjC.framework                    QuickLookIosmac.framework
AccountsUI.framework                            FamilyNotification.framework                    QuickLookNonBaseSystem.framework
AcousticMaterials.framework                     FeatureFlags.framework                          QuickLookSupport.framework
ctionKit.framework                              FeatureFlagsSupport.framework                   QuickLookThumbnailGeneration.framework
```

ASSESSING EXPORTS

WE FIRST OPEN THE DESIRED FRAMEWORK IN BINARY NINJA'S TRIAGE MODE TO LOOK FOR THE FUNCTIONS EXPORTED. OUT OF THEM, THE "GETOURUUID()" FUNCTION SEEMS INTERESTING AND IS EASY TO DEMONSTRATE ON.



File Info

```
Path:     /Users/cr7pt0pl4gu3/Desktop/research/acfs_x86_64.dylib
Size:     0x17000
MD5:      584d1628c2806dfb85ffbe22ebf759a1
SHA-1:    adc417b276a13bbac9e91b7d9033be663d170d69
SHA-256:  ad91b2f84be9aad0eb5ea6bf78be5768fa8bb5a6a5146dcbef4027c8a06fa539
```

Headers

```
Type:          Mach-O
Platform:      mac-x86_64
Current Base:  0x7ffb12bb6000
Endianness:    Little
```

Imports

Search imports

Entry	Name
0x7ffb408e1e…	_AuthorizationCreate
0x7ffb408e1e…	_AuthorizationMakeExternalForm
0x7ffb408e1f…	_CC_SHA1
0x7ffb408e1f…	_CC_SHA1_Final
0x7ffb408e1f…	_CC_SHA1_Init
0x7ffb408e1f…	_CC_SHA1_Update
0x7ffb408e1f…	_CFDataCreate
0x7ffb408e1f…	_CFDataCreateWithBytesNoCopy
0x7ffb408e1f…	_CFDataGetBytePtr

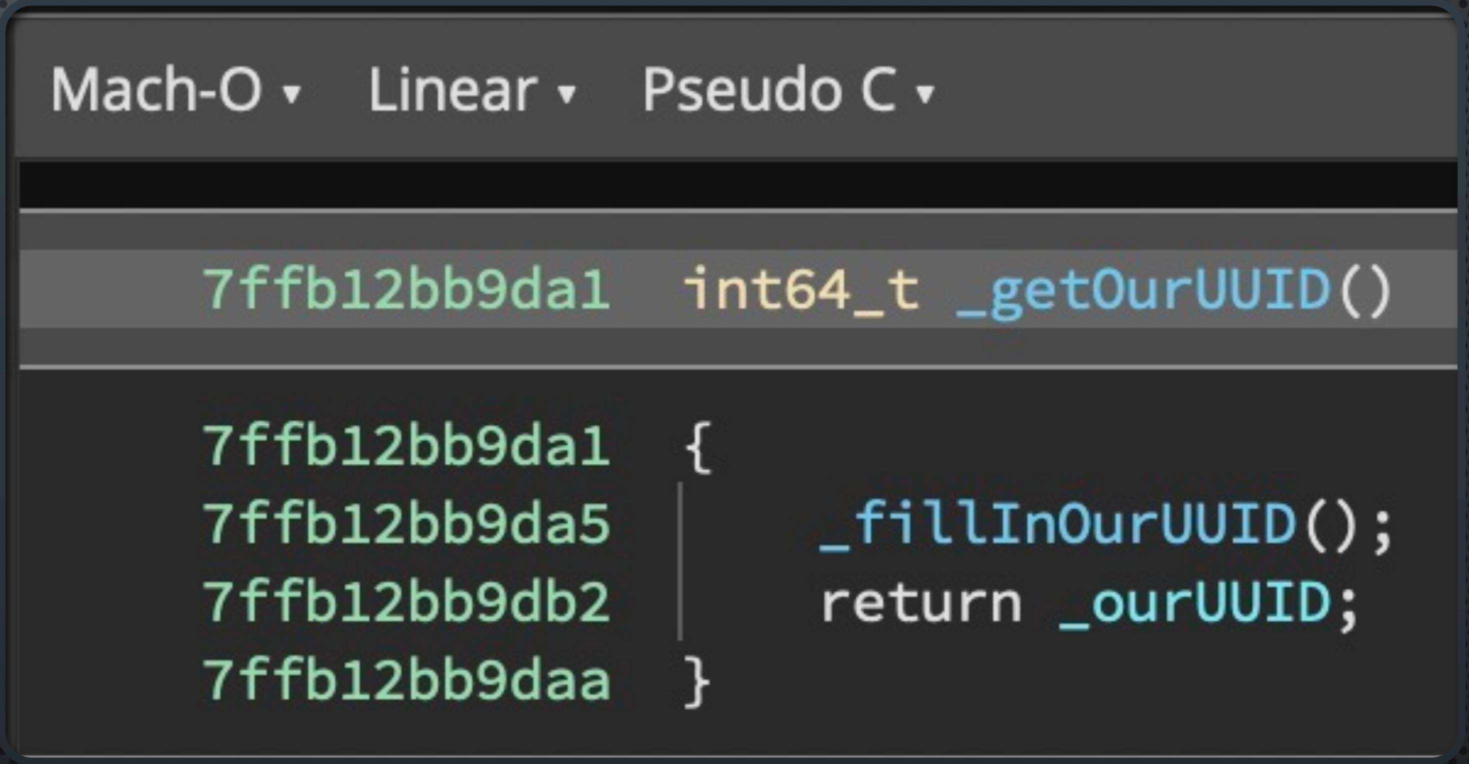
Exports

Search exports

Address	Name
0x7ffb12bb98…	_ldapSanUserNameForName
0x7ffb12bb9b…	_loadConfigPlist
0x7ffb12bb9c…	_saveConfigPlist
0x7ffb12bb9c…	_xsan_controller_from_ip
0x7ffb12bb9d…	_getOurUUID
0x7ffb12bb9e…	_configPlistIsController
0x7ffb12bb9e…	_configPlistIsMaster
0x7ffb12bb9e…	_configPlistIsZombie
0x7ffb12bba7…	_ldapSanAccessNameForName

REVERSE ENGINEERING THE FUNCTION

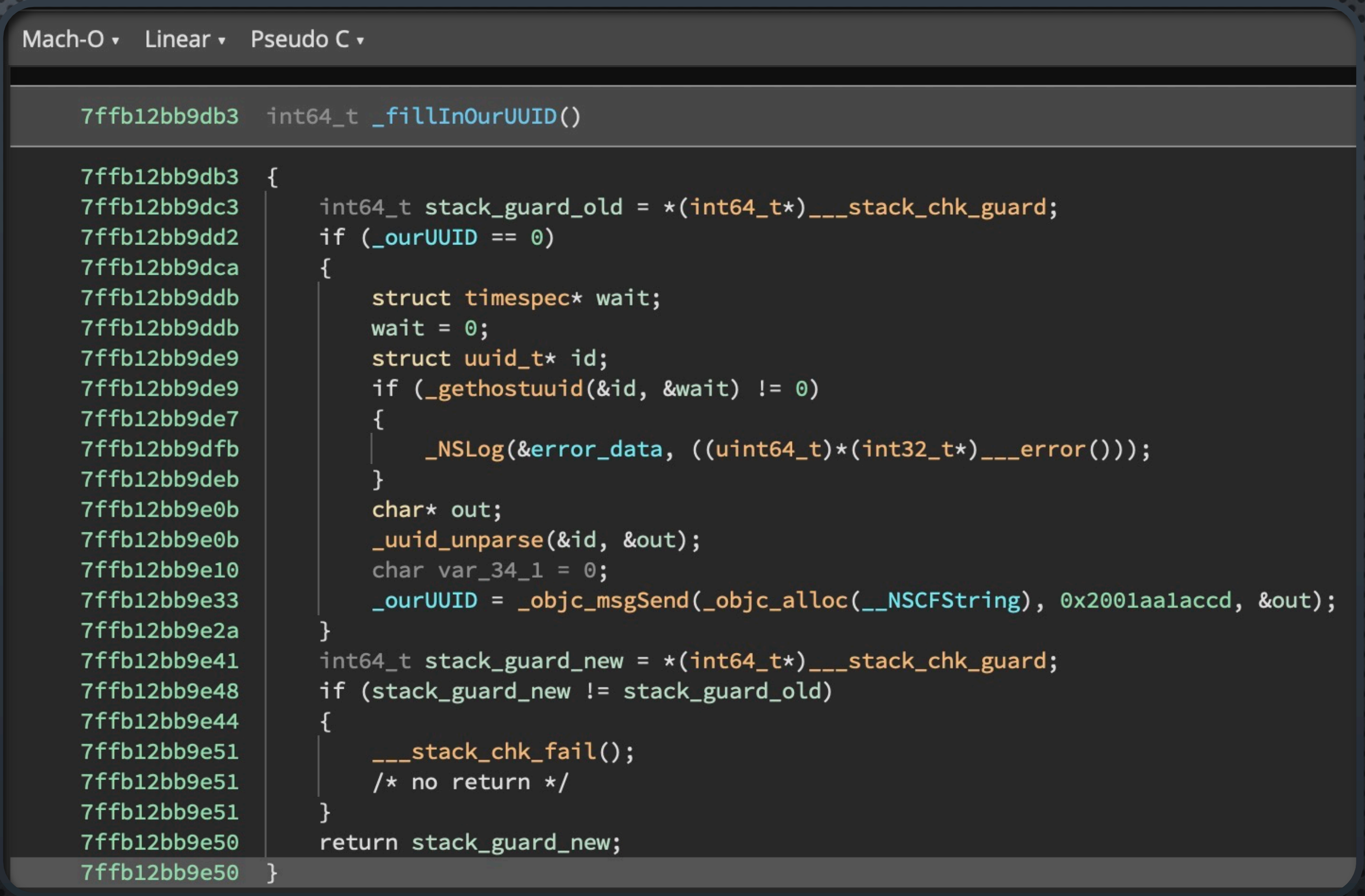
- We will assume that the function returns ID type instead of int64_t
- There is also a call to "fillInOurUUID()" function inside, which we need to reverse engineer as well
- Function returns ourUUID from the BSS segment (uninitialized static variables)



```
7ffb12bb9da1  int64_t _getOurUUID()

7ffb12bb9da1  {
7ffb12bb9da5      _fillInOurUUID();
7ffb12bb9db2      return _ourUUID;
7ffb12bb9daa  }
```

REVERSE ENGINEERING THE FUNCTION

- AFTER SPENDING SOME TIME RENAMING VARIABLES, CREATING STRUCTS AND DEFINING NECESSARY TYPES, THE FUNCTION LOOKS LIKE THAT
- ESSENTIALLY, THIS FUNCTION IS OBJECTIVE-C WRAPPER OF UNIX "GETHOSTUUID()/UUID_UNPARSE()" METHODS
- WE CAN ALSO UTILIZE A DEBUGGER TO RESOLVE SELECTORS, UNDEFINED DATA, SYMBOLS, ETC. THIS PROCESS IS NOT SHOWN HERE FOR SIMPLICITY

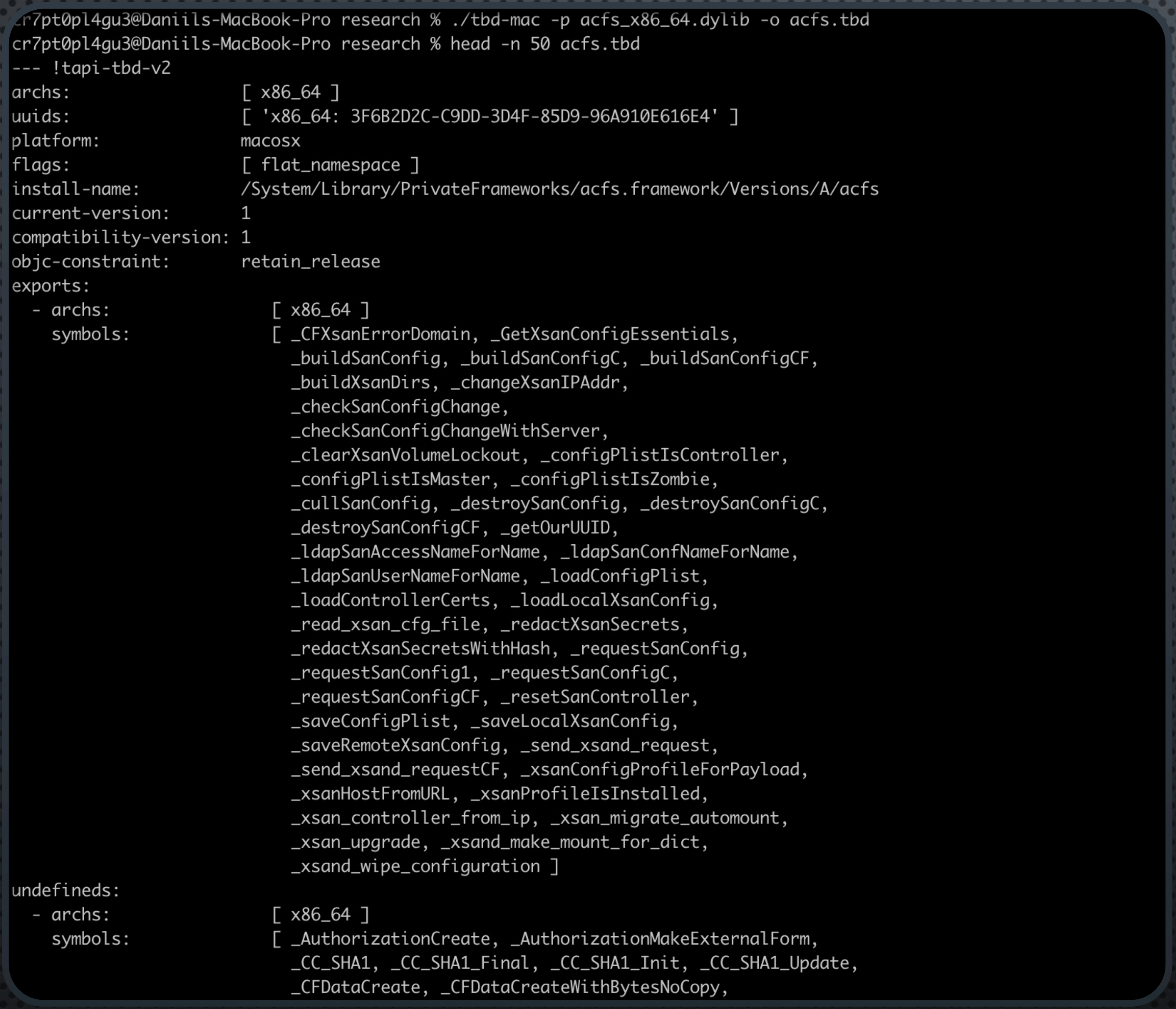


```
7ffb12bb9db3  int64_t _fillInOurUUID()

7ffb12bb9db3  {
7ffb12bb9dc3      int64_t stack_guard_old = *(int64_t*)___stack_chk_guard;
7ffb12bb9dd2      if (_ourUUID == 0)
7ffb12bb9dca      {
7ffb12bb9ddb          struct timespec* wait;
7ffb12bb9ddb          wait = 0;
7ffb12bb9de9          struct uuid_t* id;
7ffb12bb9de9          if (_gethostuuid(&id, &wait) != 0)
7ffb12bb9de7          {
7ffb12bb9dfb              _NSLog(&error_data, ((uint64_t)*(int32_t*)___error()));
7ffb12bb9deb          }
7ffb12bb9e0b          char* out;
7ffb12bb9e0b          _uuid_unparse(&id, &out);
7ffb12bb9e10          char var_34_1 = 0;
7ffb12bb9e33          _ourUUID = _objc_msgSend(_objc_alloc(__NSCFString), 0x2001aa1accd, &out);
7ffb12bb9e2a      }
7ffb12bb9e41      int64_t stack_guard_new = *(int64_t*)___stack_chk_guard;
7ffb12bb9e48      if (stack_guard_new != stack_guard_old)
7ffb12bb9e44      {
7ffb12bb9e51          ___stack_chk_fail();
7ffb12bb9e51          /* no return */
7ffb12bb9e51      }
7ffb12bb9e50      return stack_guard_new;
7ffb12bb9e50  }
```

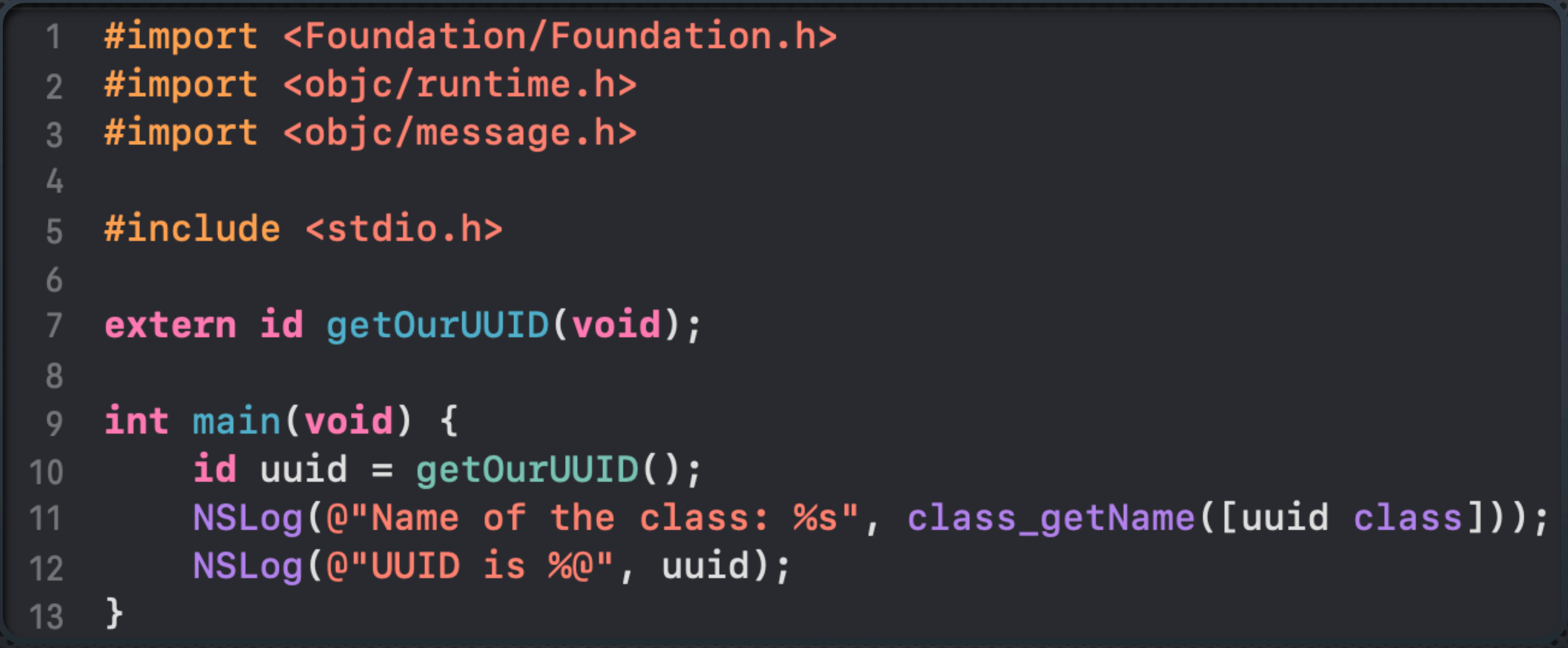
GENERATING HEADERS (.TBD)

- To successfully use and link against our target library, we’ll need to generate a .TBD file
- A .TBD file is a text-based file used by Apple Xcode, a macOS IDE used to develop iOS and macOS apps. It contains information about a .DYLIB library, the location of the .DYLIB library, and symbols.
- We will utilize https://github.com/inoahdev/tbd project to dump the .DYLIB and generate a .TBD from it

.TBD GENERATION AND LAYOUT

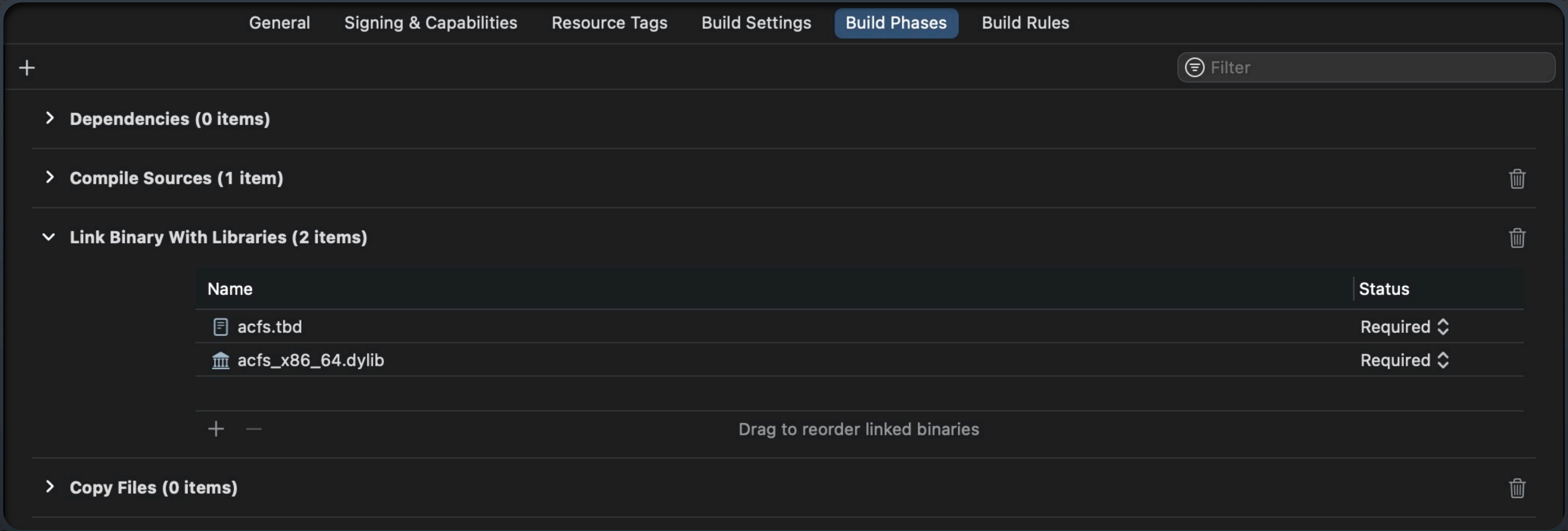


```
cr7pt0pl4gu3@Daniils-MacBook-Pro research % ./tbd-mac -p acfs_x86_64.dylib -o acfs.tbd
cr7pt0pl4gu3@Daniils-MacBook-Pro research % head -n 50 acfs.tbd
--- !tapi-tbd-v2
archs:                 [ x86_64 ]
uuids:                 [ 'x86_64: 3F6B2D2C-C9DD-3D4F-85D9-96A910E616E4' ]
platform:              macosx
flags:                 [ flat_namespace ]
install-name:          /System/Library/PrivateFrameworks/acfs.framework/Versions/A/acfs
current-version:       1
compatibility-version: 1
objc-constraint:       retain_release
exports:
  - archs:                [ x86_64 ]
    symbols:              [ _CFXsanErrorDomain, _GetXsanConfigEssentials,
                            _buildSanConfig, _buildSanConfigC, _buildSanConfigCF,
                            _buildXsanDirs, _changeXsanIPAddr,
                            _checkSanConfigChange,
                            _checkSanConfigChangeWithServer,
                            _clearXsanVolumeLockout, _configPlistIsController,
                            _configPlistIsMaster, _configPlistIsZombie,
                            _cullSanConfig, _destroySanConfig, _destroySanConfigC,
                            _destroySanConfigCF, _getOurUUID,
                            _ldapSanAccessNameForName, _ldapSanConfNameForName,
                            _ldapSanUserNameForName, _loadConfigPlist,
                            _loadControllerCerts, _loadLocalXsanConfig,
                            _read_xsan_cfg_file, _redactXsanSecrets,
                            _redactXsanSecretsWithHash, _requestSanConfig,
                            _requestSanConfig1, _requestSanConfigC,
                            _requestSanConfigCF, _resetSanController,
                            _saveConfigPlist, _saveLocalXsanConfig,
                            _saveRemoteXsanConfig, _send_xsand_request,
                            _send_xsand_requestCF, _xsanConfigProfileForPayload,
                            _xsanHostFromURL, _xsanProfileIsInstalled,
                            _xsan_controller_from_ip, _xsan_migrate_automount,
                            _xsan_upgrade, _xsand_make_mount_for_dict,
                            _xsand_wipe_configuration ]
undefineds:
  - archs:                [ x86_64 ]
    symbols:              [ _AuthorizationCreate, _AuthorizationMakeExternalForm,
                            _CC_SHA1, _CC_SHA1_Final, _CC_SHA1_Init, _CC_SHA1_Update,
                            _CFDataCreate, _CFDataCreateWithBytesNoCopy,
```



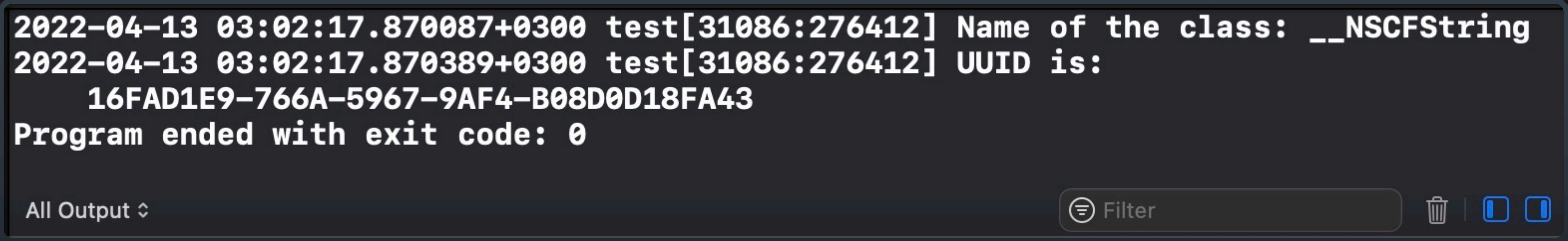
```
#import <Foundation/Foundation.h>
#import <objc/runtime.h>
#import <objc/message.h>

#include <stdio.h>

extern id getOurUUID(void);

int main(void) {
    id uuid = getOurUUID();
    NSLog(@"Name of the class: %s", class_getName([uuid class]));
    NSLog(@"UUID is %@", uuid);
}
```

CREATING XCODE PROJECT AND USING THE GETOURUUID() FUNCTION



Name	Status
acfs.tbd	Required
acfs_x86_64.dylib	Required

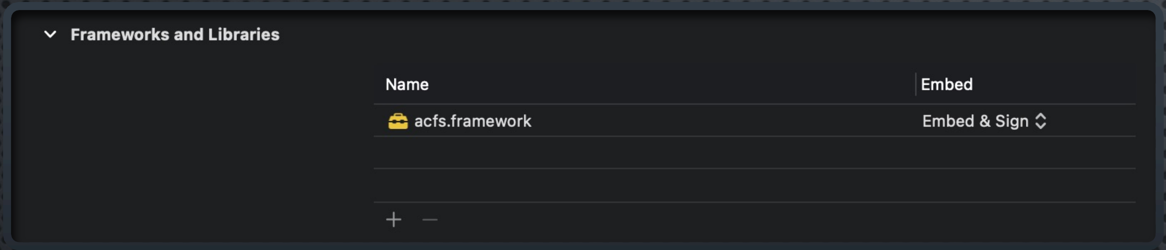
LINKING AND BUILDING



```
2022-04-13 03:02:17.870087+0300 test[31086:276412] Name of the class: __NSCFString
2022-04-13 03:02:17.870389+0300 test[31086:276412] UUID is:
    16FAD1E9-766A-5967-9AF4-B08D0D18FA43
Program ended with exit code: 0
```

RUNNING OUR PROJECT

EASIER LINKAGE?



Frameworks and Libraries

Name	Embed
acfs.framework	Embed & Sign

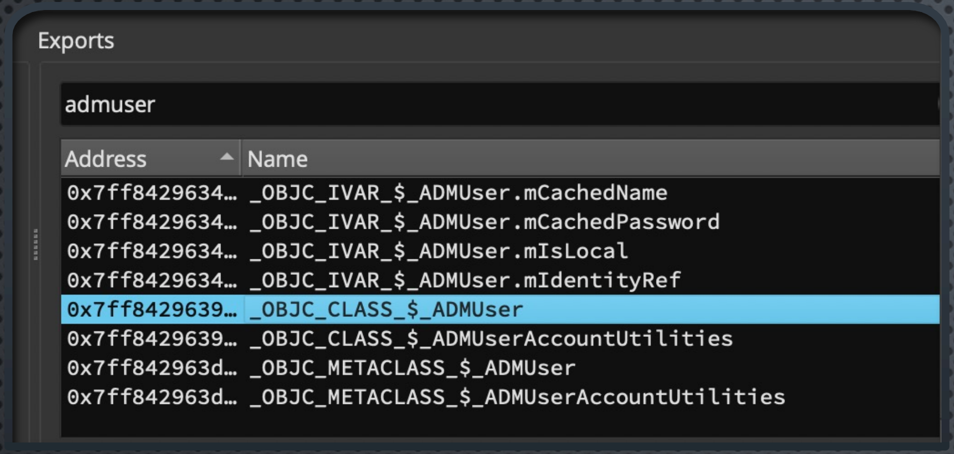
- We can also link framework from /System/Library/PrivateFrameworks folder directly, the result is the same

OBJECTIVE-C CLASSES

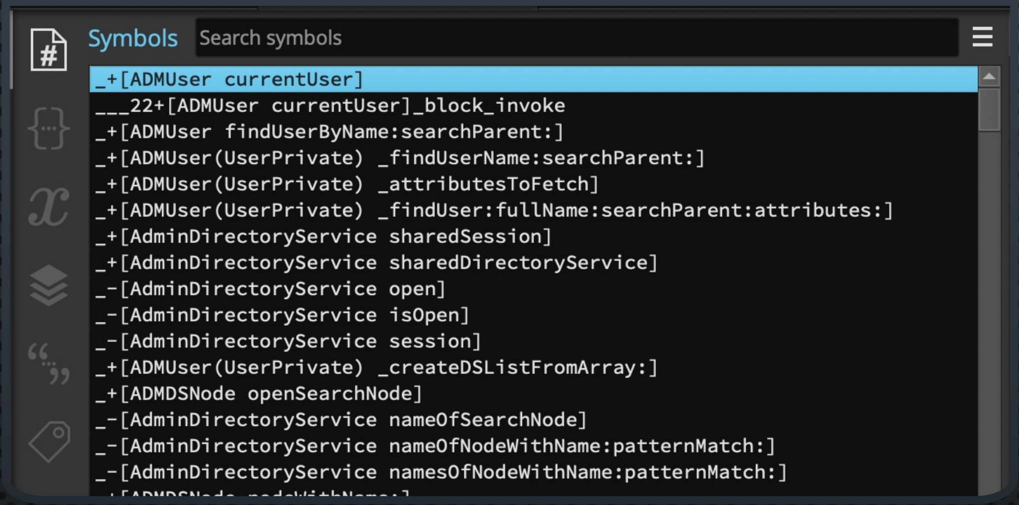
We now know how to utilize C/Objective-C functions, but what if we want to use a class?

Objective-C runtime & messaging comes to our aid!

We will also explore how to utilize Objective-C runtime,
eliminating the need for the Objective-C class/method declarations!



```
admuser
Address          Name
0x7ff8429634…  _OBJC_IVAR_$_ADMUser.mCachedName
0x7ff8429634…  _OBJC_IVAR_$_ADMUser.mCachedPassword
0x7ff8429634…  _OBJC_IVAR_$_ADMUser.mIsLocal
0x7ff8429634…  _OBJC_IVAR_$_ADMUser.mIdentityRef
0x7ff8429639…  _OBJC_CLASS_$_ADMUser
0x7ff8429639…  _OBJC_CLASS_$_ADMUserAccountUtilities
0x7ff842963d…  _OBJC_METACLASS_$_ADMUser
0x7ff842963d…  _OBJC_METACLASS_$_ADMUserAccountUtilities
```

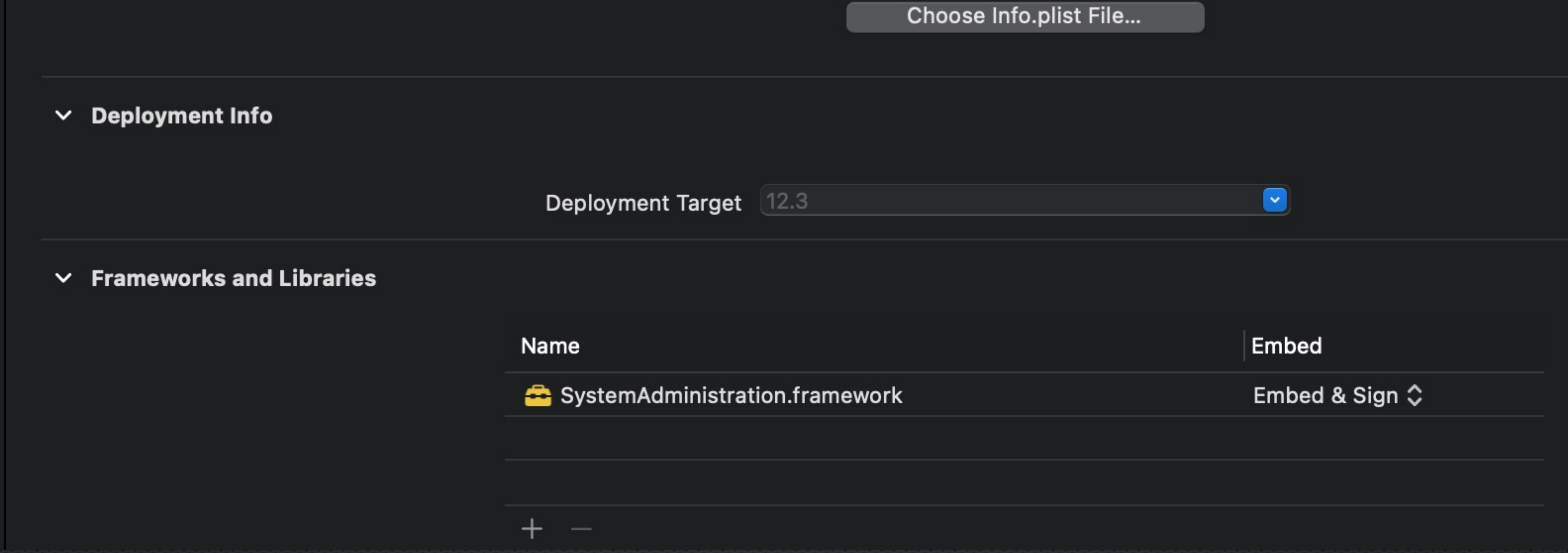


```
_+[ADMUser currentUser]
___22+[ADMUser currentUser]_block_invoke
_+[ADMUser findUserByName:searchParent:]
_+[ADMUser(UserPrivate) _findUserName:searchParent:]
_+[ADMUser(UserPrivate) _attributesToFetch]
_+[ADMUser(UserPrivate) _findUser:fullName:searchParent:attributes:]
_+[AdminDirectoryService sharedSession]
_+[AdminDirectoryService sharedDirectoryService]
_-[AdminDirectoryService open]
_-[AdminDirectoryService isOpen]
_-[AdminDirectoryService session]
_+[ADMUser(UserPrivate) _createDSListFromArray:]
_+[ADMDSNode openSearchNode]
_-[AdminDirectoryService nameOfSearchNode]
_-[AdminDirectoryService nameOfNodeWithName:patternMatch:]
_-[AdminDirectoryService namesOfNodeWithName:patternMatch:]
```

SYSTEMADMINISTRATION.FRAMEWORK EXPORT TABLE

We notice that “ADMUser” Objective-C class is being exported, which means that every method of the class is exported as well (for example, the “currentUser” selector is available).

The [ADMUser currentUser] call is rather self-explanatory. We will try to use it without reverse engineering its inner workings to save time.



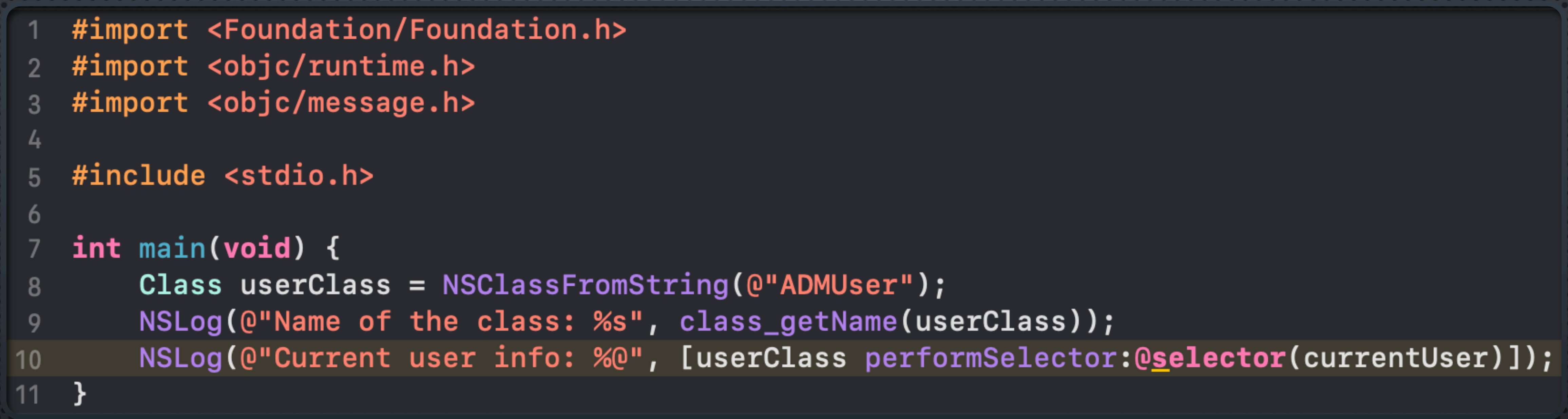
Deployment Info

Deployment Target 12.3

Frameworks and Libraries

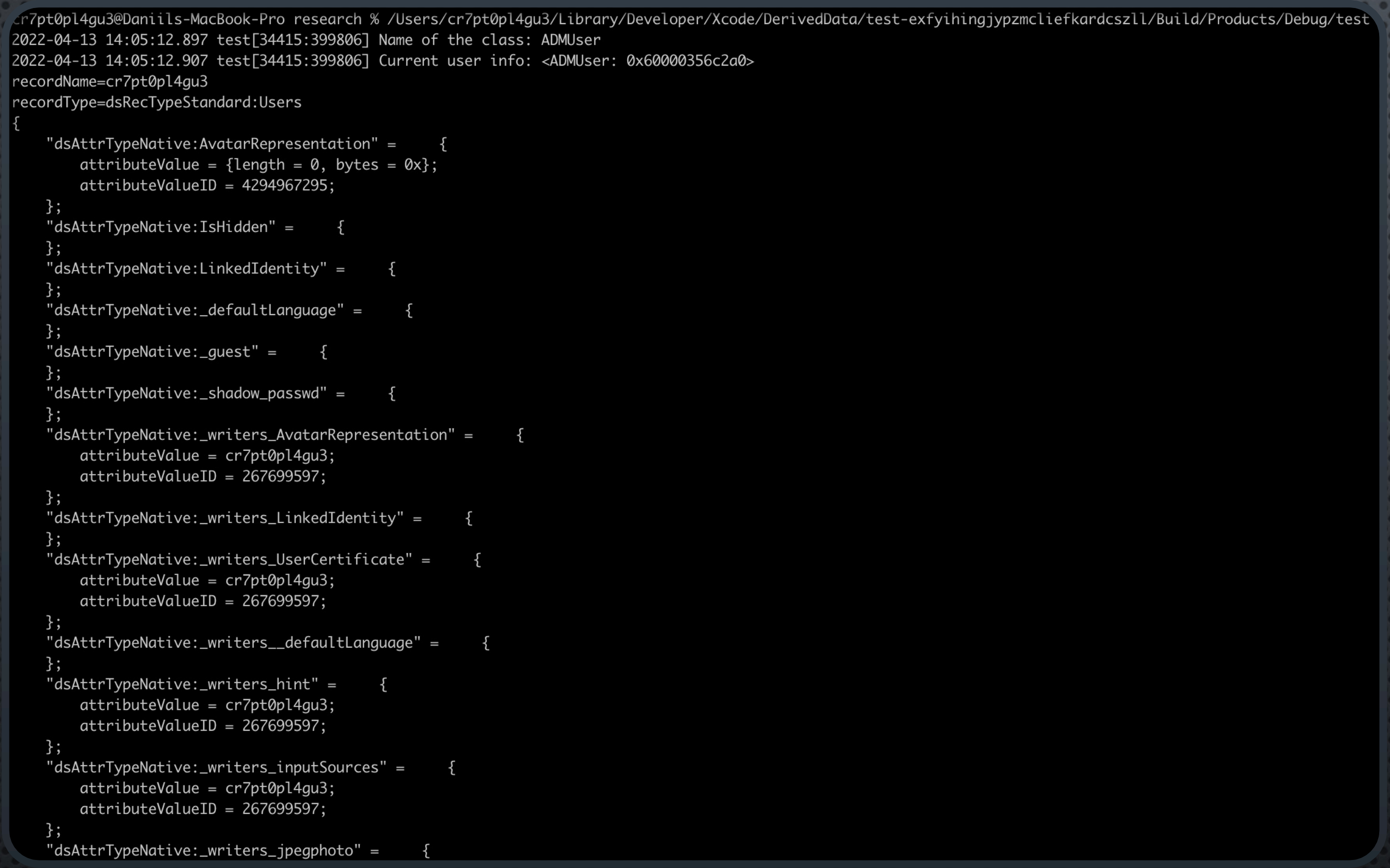
Name	Embed
SystemAdministration.framework	Embed & Sign

LINKING AGAINST THE FRAMEWORK



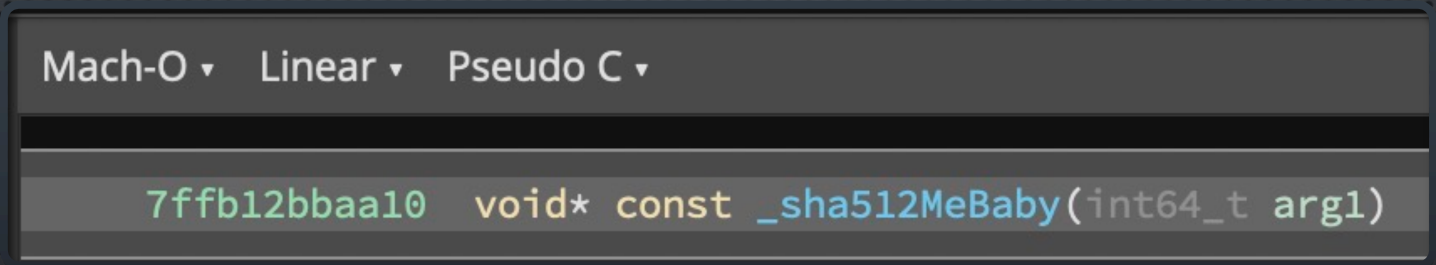
```
#import <Foundation/Foundation.h>
#import <objc/runtime.h>
#import <objc/message.h>

#include <stdio.h>

int main(void) {
    Class userClass = NSClassFromString(@"ADMUser");
    NSLog(@"Name of the class: %s", class_getName(userClass));
    NSLog(@"Current user info: %@", [userClass performSelector:@selector(currentUser)]);
}
```

(NSCLASSFROMSTRING && PERFORMSELECTOR) TRICK



```
cr7pt0pl4gu3@Daniils-MacBook-Pro research % /Users/cr7pt0pl4gu3/Library/Developer/Xcode/DerivedData/test-exfyihingjypzmcliefkardcszll/Build/Products/Debug/test
2022-04-13 14:05:12.897 test[34415:399806] Name of the class: ADMUser
2022-04-13 14:05:12.907 test[34415:399806] Current user info: <ADMUser: 0x60000356c2a0>
recordName=cr7pt0pl4gu3
recordType=dsRecTypeStandard:Users
{
    "dsAttrTypeNative:AvatarRepresentation" =     {
        attributeValue = {length = 0, bytes = 0x};
        attributeValueID = 4294967295;
    };
    "dsAttrTypeNative:IsHidden" =     {
    };
    "dsAttrTypeNative:LinkedIdentity" =     {
    };
    "dsAttrTypeNative:_defaultLanguage" =     {
    };
    "dsAttrTypeNative:_guest" =     {
    };
    "dsAttrTypeNative:_shadow_passwd" =     {
    };
    "dsAttrTypeNative:_writers_AvatarRepresentation" =     {
        attributeValue = cr7pt0pl4gu3;
        attributeValueID = 267699597;
    };
    "dsAttrTypeNative:_writers_LinkedIdentity" =     {
    };
    "dsAttrTypeNative:_writers_UserCertificate" =     {
        attributeValue = cr7pt0pl4gu3;
        attributeValueID = 267699597;
    };
    "dsAttrTypeNative:_writers__defaultLanguage" =     {
    };
    "dsAttrTypeNative:_writers_hint" =     {
        attributeValue = cr7pt0pl4gu3;
        attributeValueID = 267699597;
    };
    "dsAttrTypeNative:_writers_inputSources" =     {
        attributeValue = cr7pt0pl4gu3;
        attributeValueID = 267699597;
    };
    "dsAttrTypeNative:_writers_jpegphoto" =     {
```

SUCCESS!



```
7ffb12bbaa10  void* const _sha512MeBaby(int64_t arg1)
```

P.S. WHAT THE... (HAPPILY TAKEN FROM ACFS.FRAMEWORK)

THANK YOU FOR LISTENING, HAPPY HACKING ;)
QUESTIONS?

RESOURCES

- HTTPS://DEVELOPER.APPLE.COM/FORUMS/THREAD/692383
- HTTPS://BINARY.NINJA
- HTTPS://GITHUB.COM/KEITH/DYLD-SHARED-CACHE-EXTRACTOR
- HTTPS://GITHUB.COM/INOAHDEV/TBD
- HTTP://NEWOSXBOOK.COM/INDEX.PHP (VOLUME I - USER MODE)
- HTTPS://OPENSOURCE.APPLE.COM
- HTTPS://DEVELOPER.APPLE.COM/SECURITY-BOUNTY/
- HTTPS://WOJCIECHREGULA.BLOG/POST/PLAY-THE-MUSIC-AND-BYPASS-TCC-AKA-CVE-2020-29621/