File Identification in iOS

Michael Ogata
michael.ogata@nist.gov

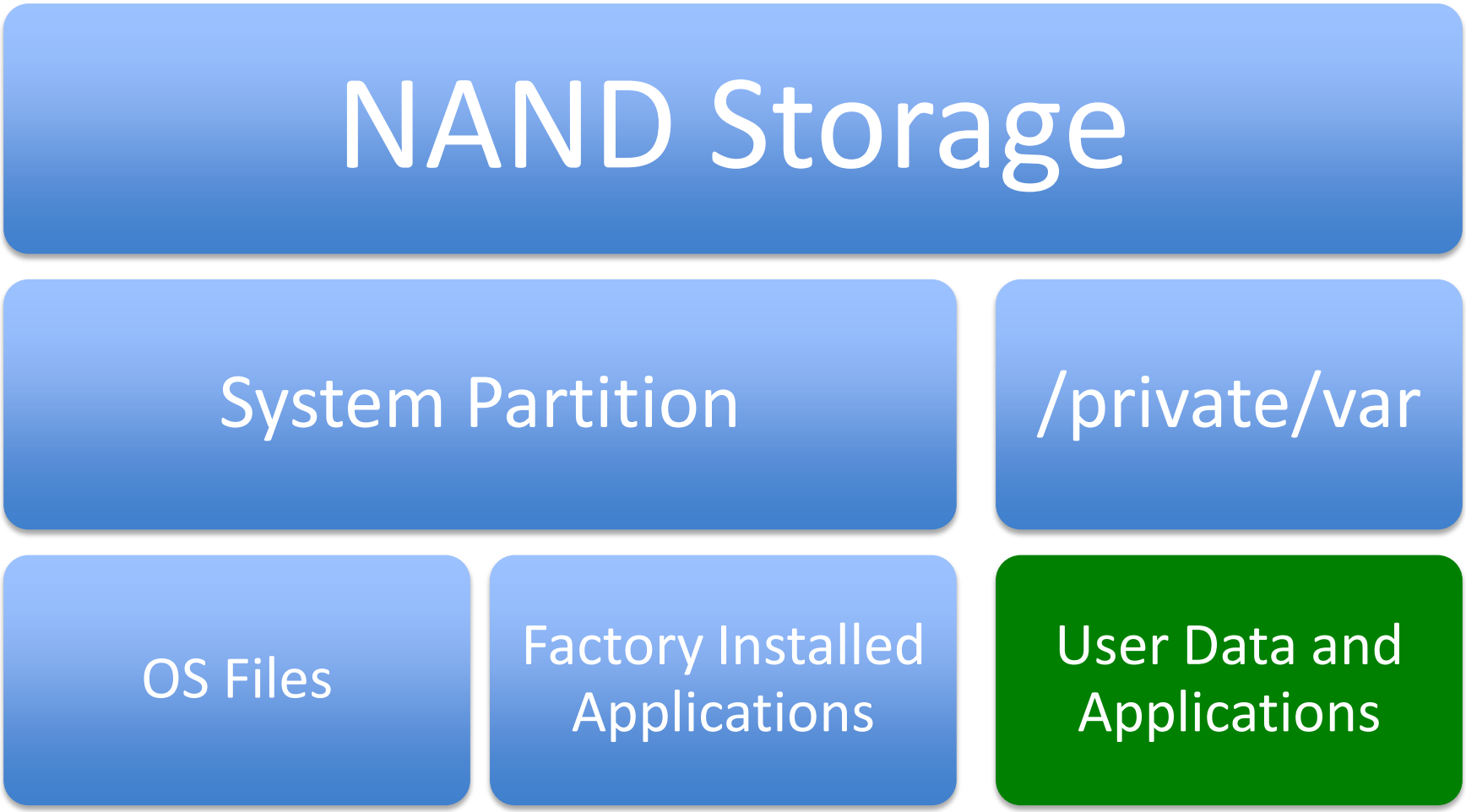
Questions:

- Can the NSRL method of file identification be used to identify files on a device running iOS?
- Once identified, can applications be automatically classified by their behavior?

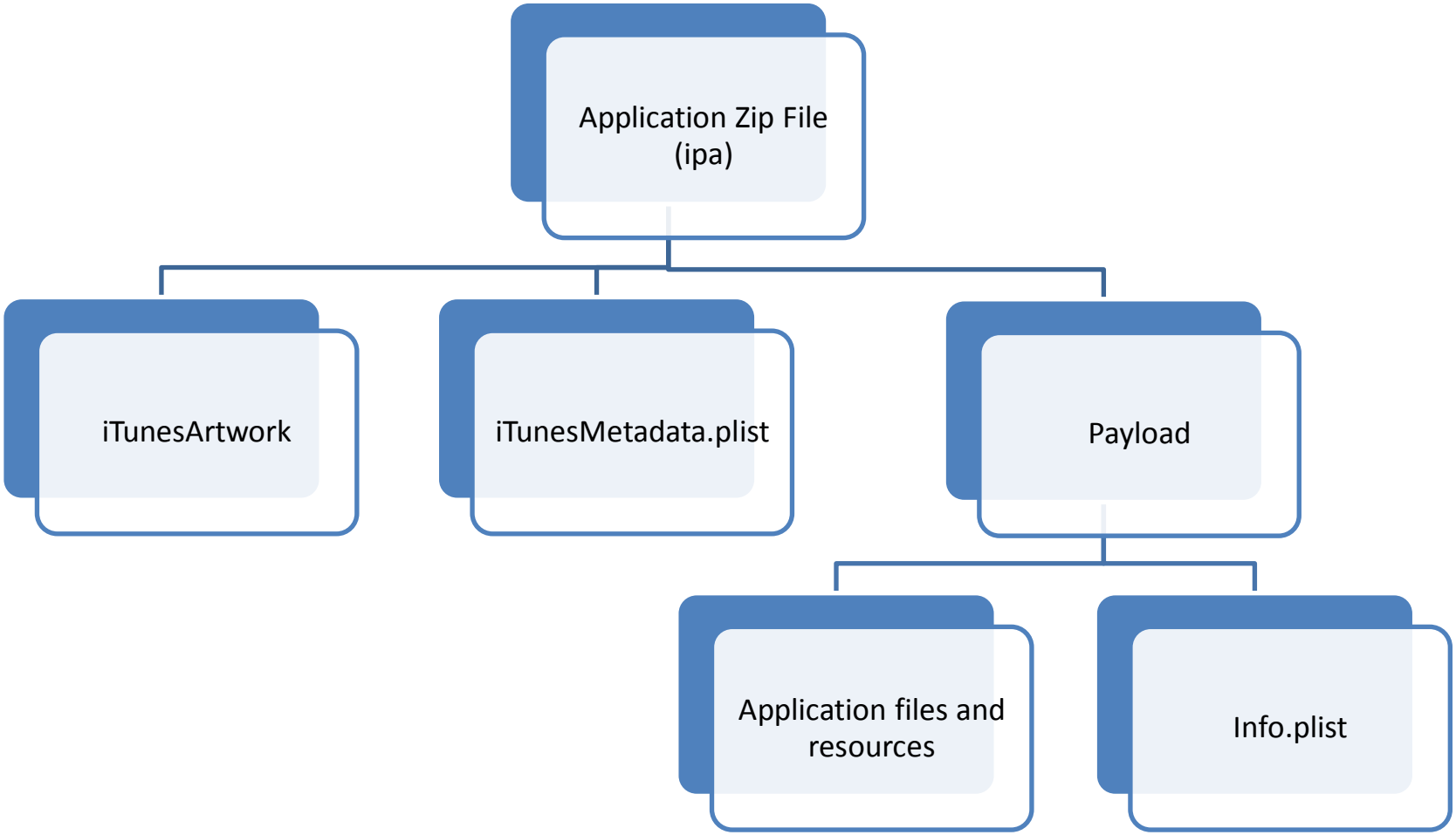
Presentation Overview

- Applying the NSRL methodology to iOS
  - Brief anatomy of iOS file system
  - Brief anatomy of iOS applications
  - File identification on an iPhone
- Methods for describing application functionality
  - Manifest files
  - Examining application binaries
- Benefits / Future Work

Anatomy of the iOS File System



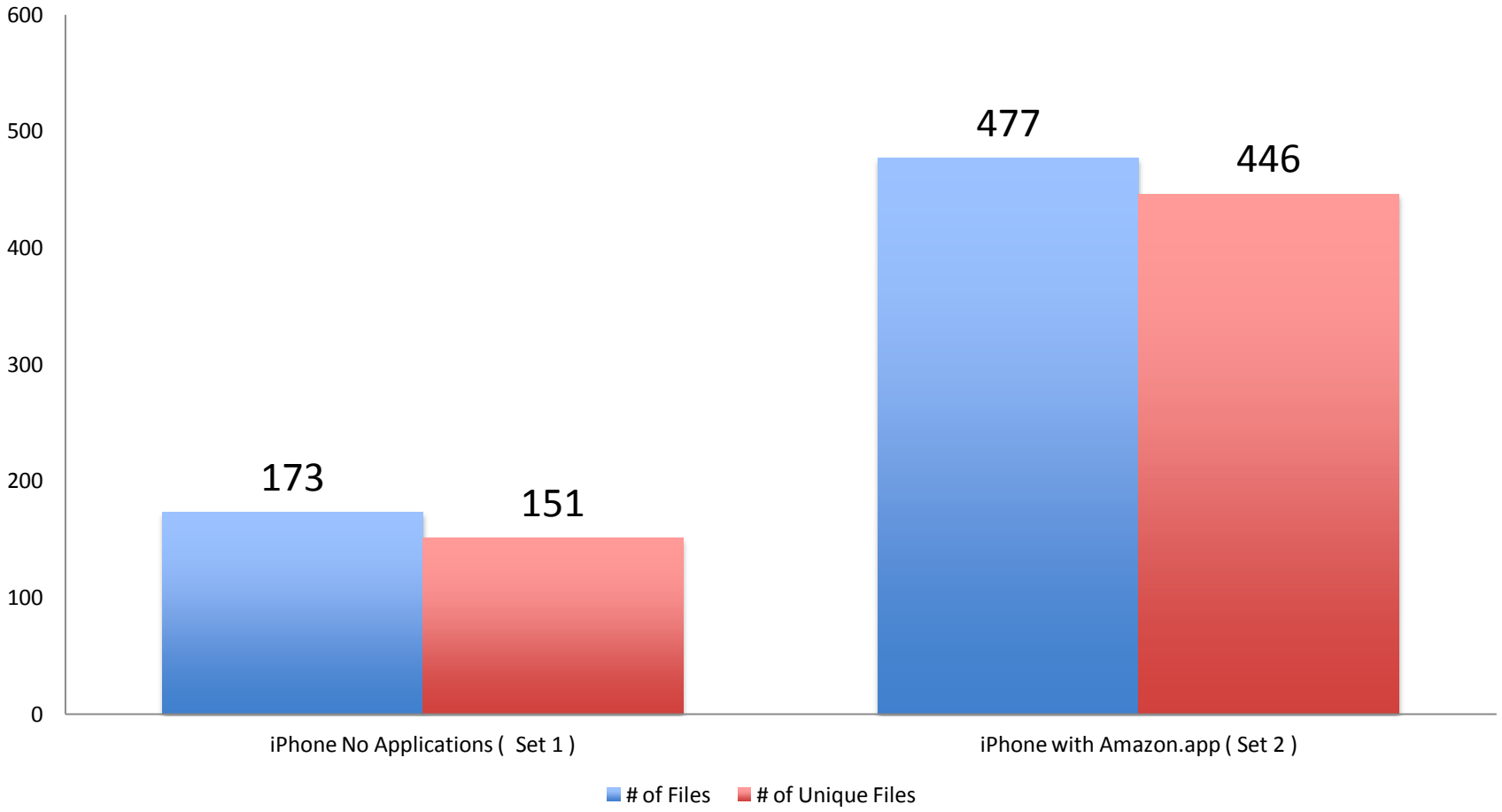
Anatomy of an iOS Application



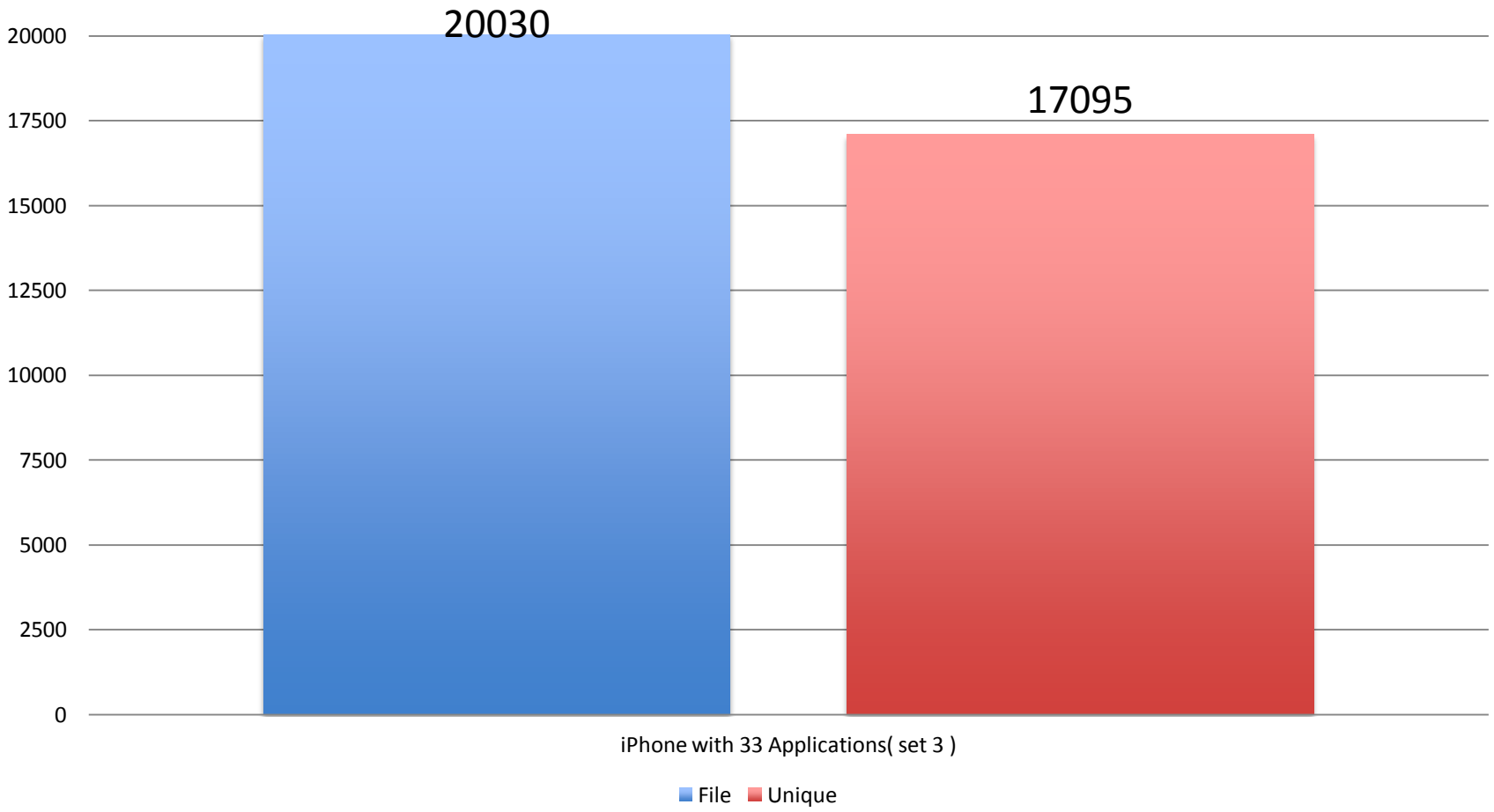
iPhone File Identification

- Application corpus of 91 applications
  - 49,403 files
  - 43,462 unique files
- File sets extracted from 1st generation iPhone
  - Set 1: No applications (used as baseline)
  - Set 2: One application synced to phone
  - Set 3: 33 (all compatible) corpus applications synced to phone

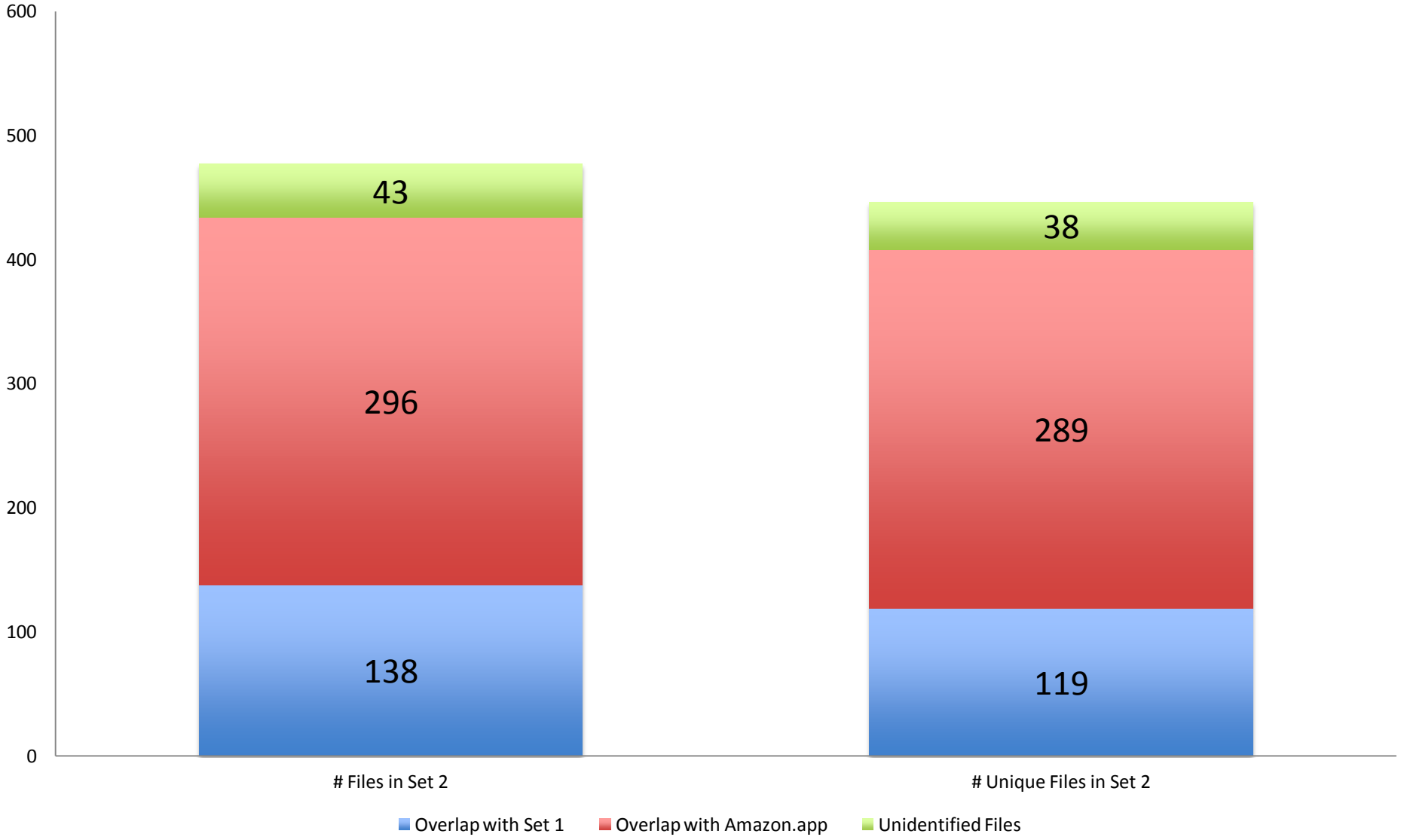
Uniqueness of Files



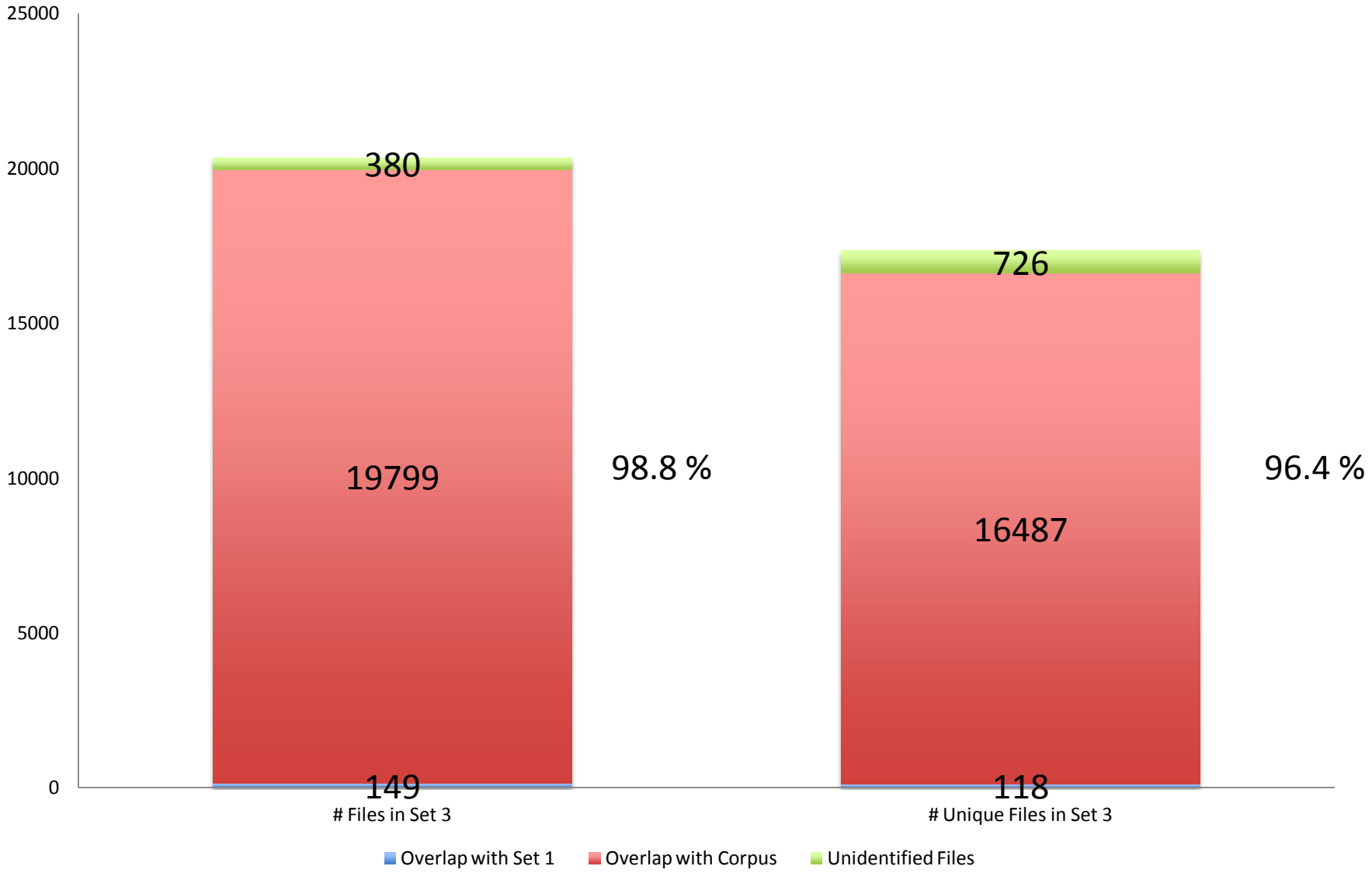
Uniqueness of Files in Set 3



File Identification in Set 2



File Identification in Set 3



Describing Application Functionality

- Info.plist
- Examining application binary files

Info.plist

Localization native development re	English
Bundle display name	MapQuest
▼ Document types	(0 items)
Executable file	MapQuest
Bundle identifier	com.aol.mapquest
InfoDictionary version	6.0
Bundle name	MapQuest
Bundle OS Type code	APPL
CFBundleResourceSpecification	ResourceRules.plist
Bundle versions string, short	2.5.7
Bundle creator OS Type code	????
▶ CFBundleSupportedPlatforms	(1 item)
▶ URL types	(1 item)
Bundle version	2.5.7.1
DTCompiler	4.2
DTPlatformBuild	8C134
DTPlatformName	iphoneos
DTPlatformVersion	4.2 Seed 2
DTSDKName	iphoneos4.2
DTXcode	0400
DTXcodeBuild	4A278b
LSRequiresIPhoneOS	☑
MinimumOSVersion	3.1.3
Main nib file base name	MainWindow
SBUsesNetwork	☑
▼ UIBackgroundModes	(2 items)
Item 0	location
Item 1	audio
▼ UIDeviceFamily	(1 item)
Item 0	1
UIPrerenderedIcon	☑

Info.plist

- Dictionary of key-value pairs
  - UIDeviceFamily / MinimumOSVersion
  - UIRequiresPersistantWifi
  - UIBackgroundModes
    - Describes how the application functions when backgrounded

*http://developer.apple.com/library/ios/#documentation/General/Reference/InfoPlistKeyReference/Articles/iPhoneOSKeys.html

Info.plist Continued…

- UIRequiredDeviceCapabilities
  - Specifies hardware requirements:
    - GPS and location services
    - Accelerometer
    - Front or rear facing cameras
    - Bluetooth
    - SMS
  - Requirements not declared are still permitted

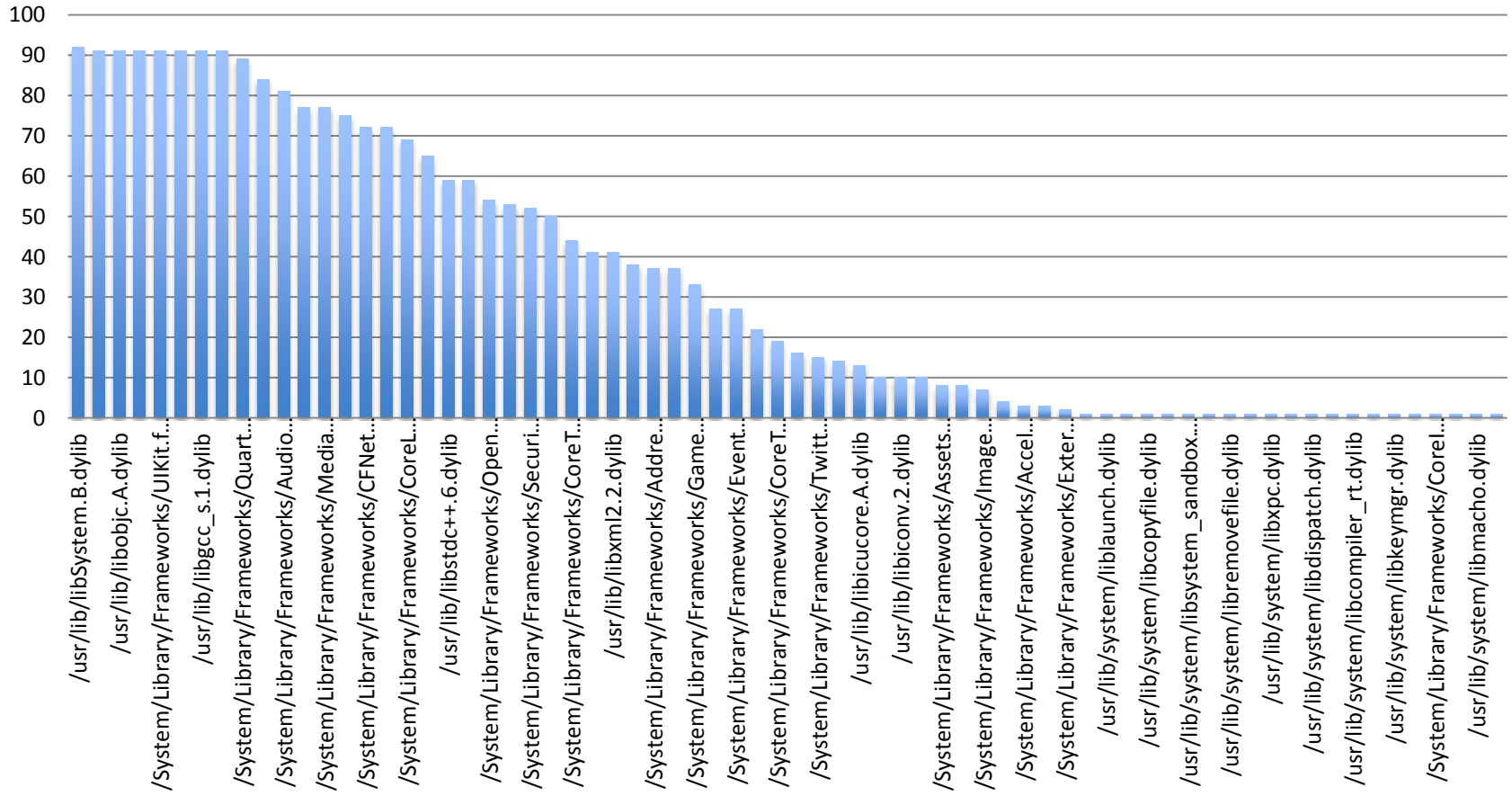
Examining Application Binary Files

- String Search of binary files
- Apple Developer Libraries embedded in plain text
- Identified 70 unique library names

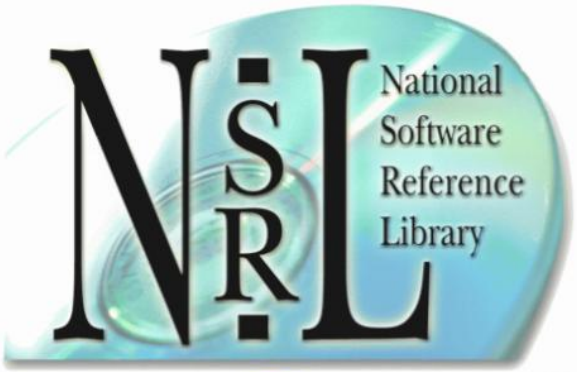
Notable Observed Libraries

Library Name	# Times Observed
CoreLocation.framework/CoreLocation	69
libsqlite3.dylib	65
AddressBook.framework/AddressBook	53
CoreTelephony.framework/CoreTelephony	44
GameKit.framework/GameKit	33
Twitter.framework/Twitter	15
ExternalAccessory.framework/ExternalAccessory	2

Frequencies of Observed Libraries



NIST Special Database #28



Reference Data Set
Version 2.38 10-01-2012

NIST

Potential Benefits

- Augment the RDS
- Identify files on iOS devices
- Build iOS application behavior profiles
- Build iOS device capability profiles

Future Work

- Incorporate iOS application acquisition into NSRL acquisition chain ✓
- Build iOS Library Data Dictionary
- Build DFXML iOS data set
- Determine applicability to iPhone backup files
  - File fragments and fuzzy hashing
- Determine applicability to iCloud
- Expanding into the Android platform

Acknowledgements

- Zdziarski, J. (2003). iPhone Forensics. Sebastopol, CA: O'Reilly Media Inc.