kpn

Play with
Mobile Applications

kpn

Mobile Application

iOS

Architecture ARM v6 v7

Language Objective C

Development Xcode (mainly)

Dev Platform: OSX (mainly)

Android

Architecture ARM v6 v7

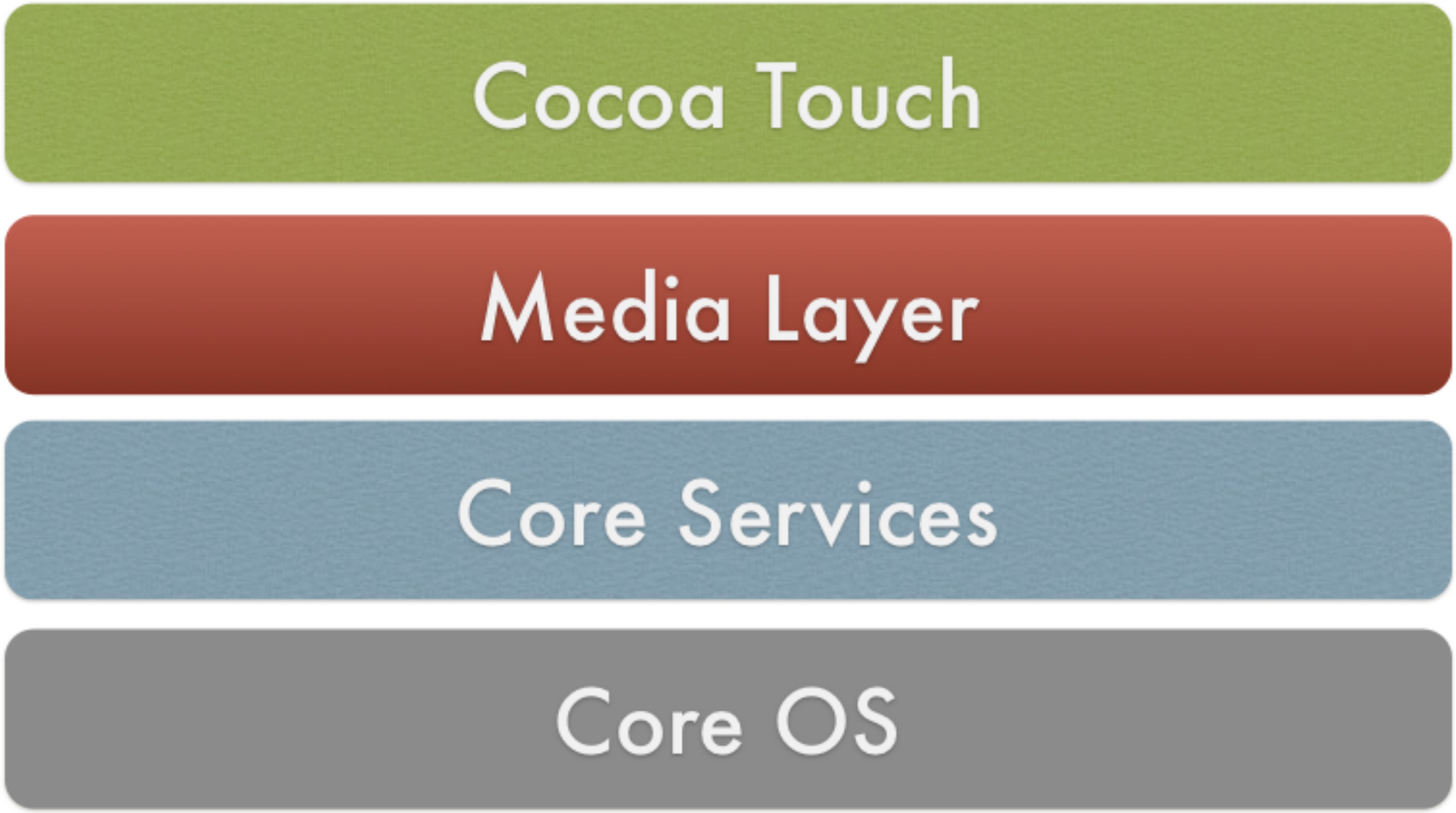
Language Java

Development Eclipse (mainly)

Dev Platform: OSX, Linux, Windows

Mobile Application

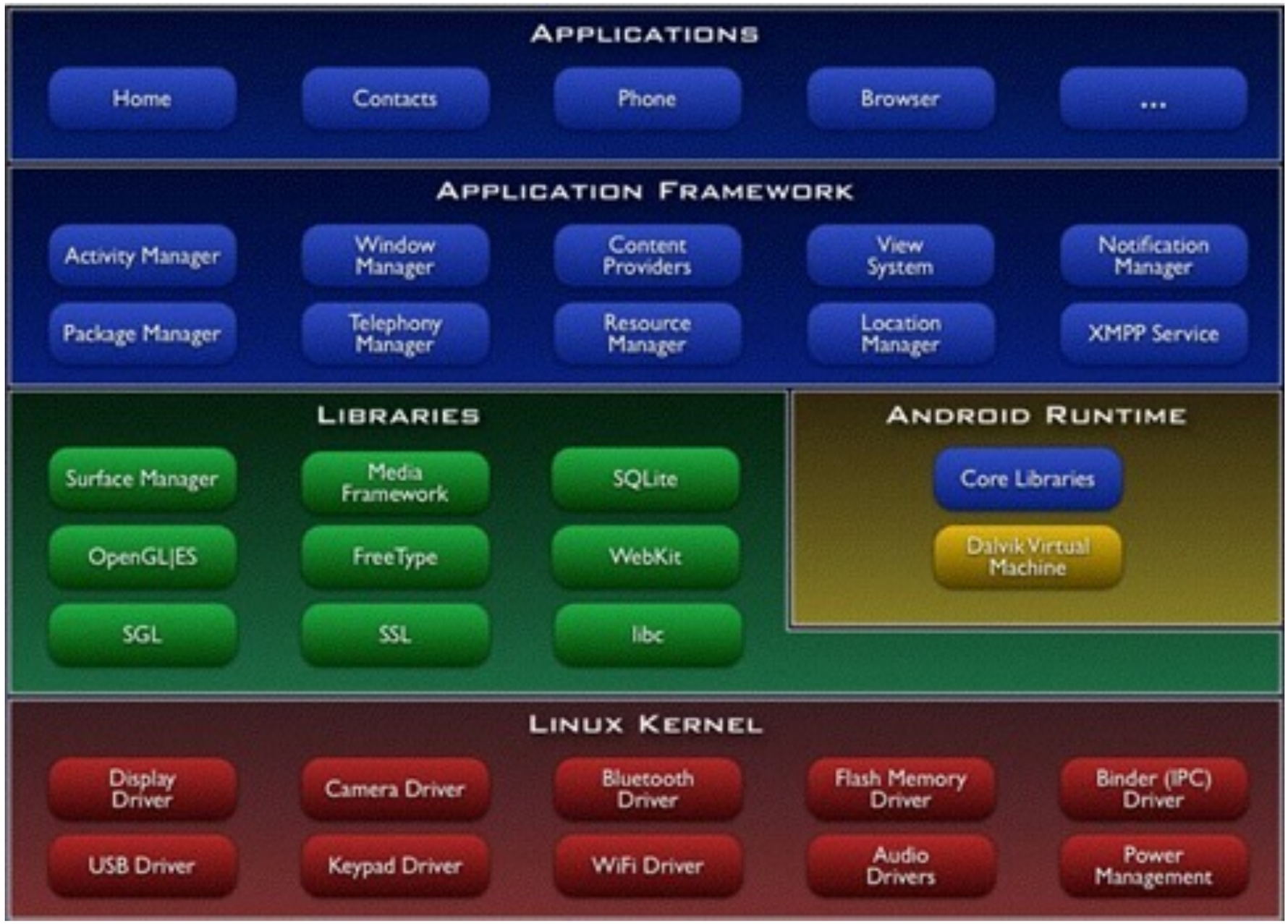
iOS



kpn

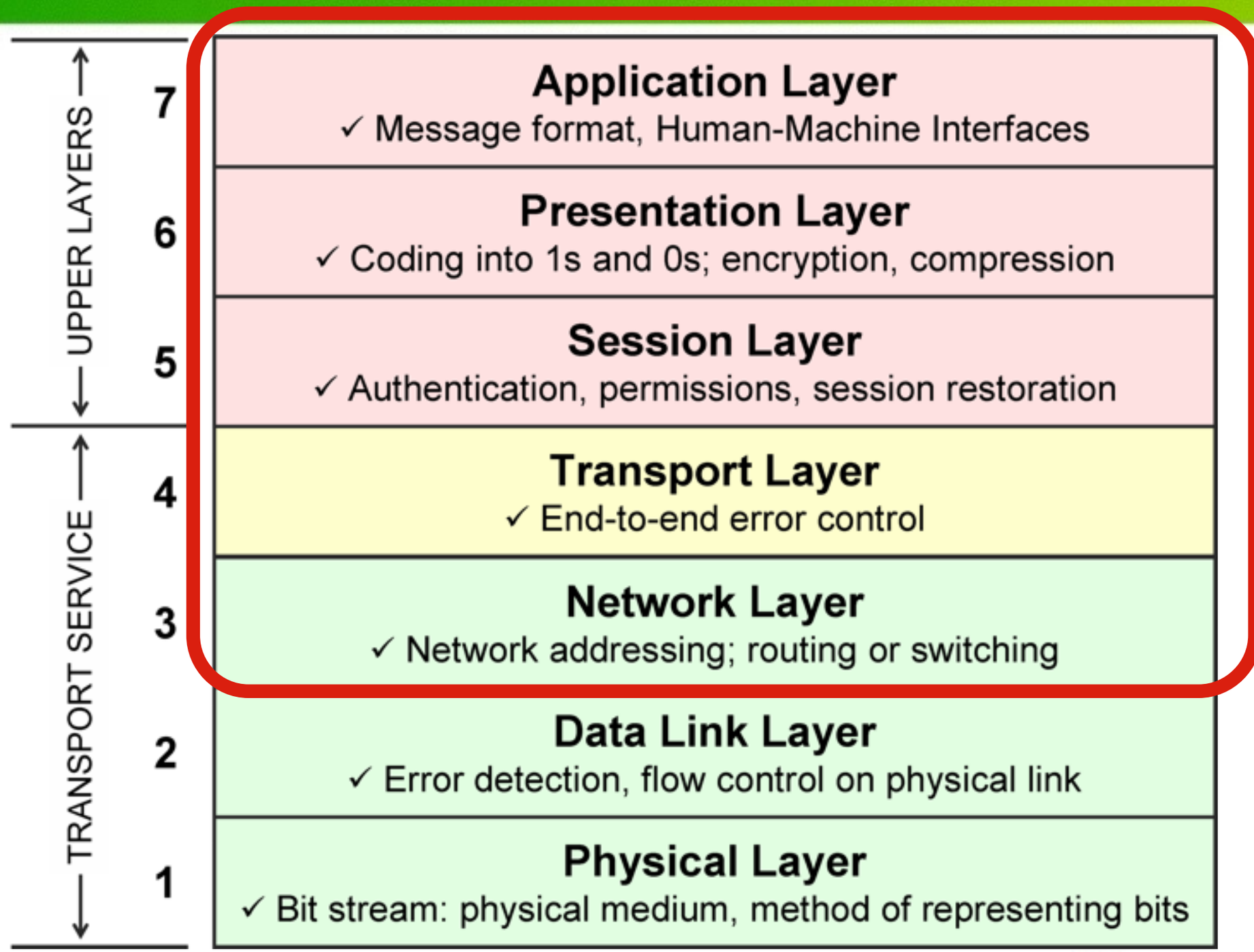
Mobile Application

Android



Mobile Application

Start point

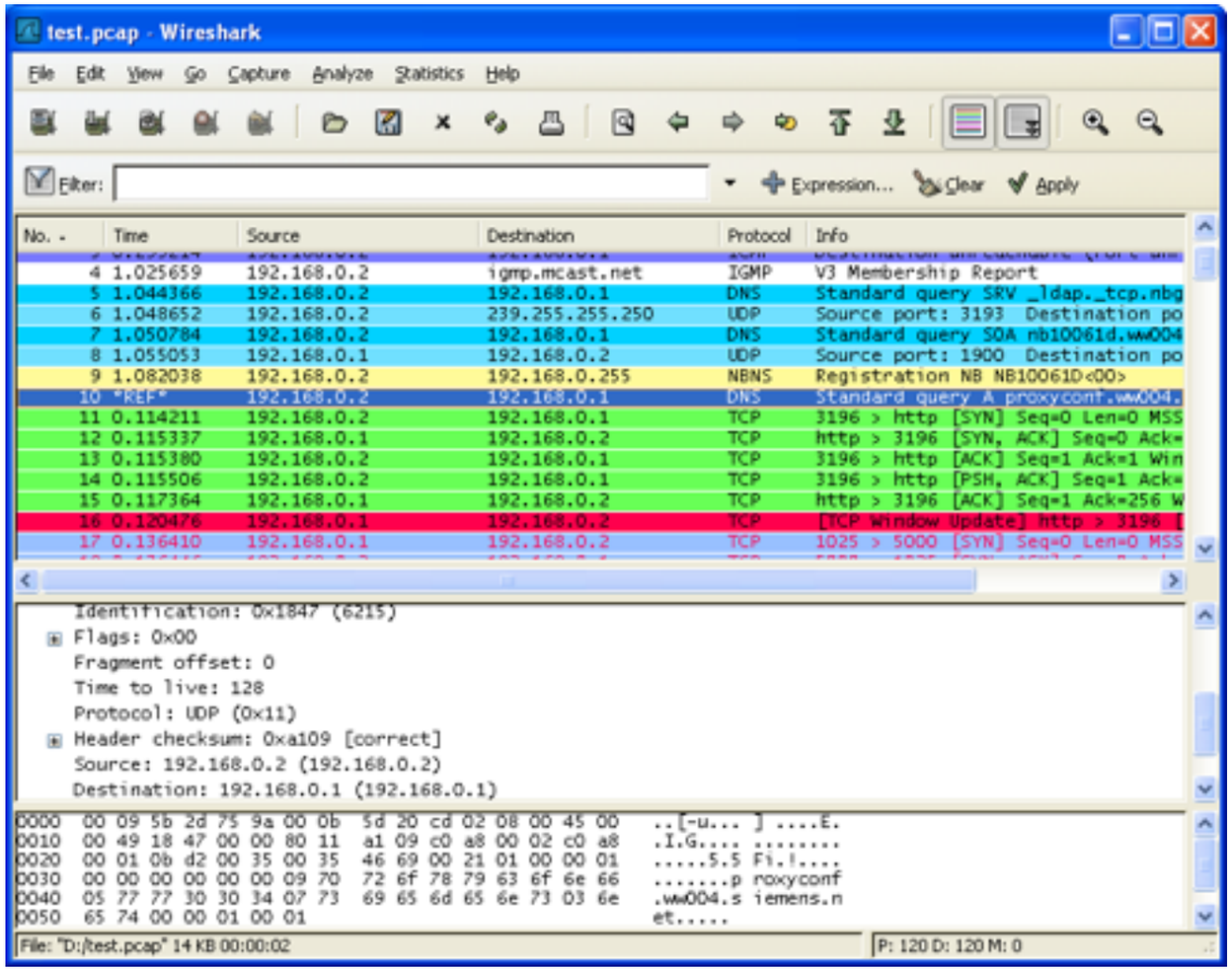


Mobile Application

Network traffic dump.

TCPdump

WireShark traffic dump



Mobile Application

iOS

HTTP Proxy BurpSuite
Configuration in mobile client

Android

HTTP Proxy BurpSuite

Network settings / Advanced.
Configuration in emulator.

Proxy Droid on the phone and BurpSuite

Mobile Application

Android

Mobile Application

Android

adb - access phone

strings - Getting strings from the binary

smali

dex2jar - for creating a jar file of an .apk

jd-gui - for decompiling

burp-suite and Wireshark for traffic interception and analyse.

Mobile Application

Android - adb

Getting apps from the phone

adb shell pm list packages

adb shell pm path com.example.someapp

adb pull /data/app/com.example.someapp-2.apk

Mobile Application

Android - adb logcat

```
D/dalvikvm(24579): VFY: replacing opcode 0x6e at 0x0042
D/Finsky  (22561): [2788] InAppBillingUtils.pickAccount: com.whatsapp: Account determined from installer data -
[g4W2-YZDoOL89AKIogbxnAowExo]
D/Finsky  (22561): [2811] InAppBillingUtils.pickAccount: com.whatsapp: Account determined from installer data -
[g4W2-YZDoOL89AKIogbxnAowExo]
D/Finsky  (22561): [2811] InAppBillingUtils.pickAccount: com.whatsapp: Account determined from installer data -
[g4W2-YZDoOL89AKIogbxnAowExo]
I/qtaguid (22561): Failed write_ctrl(u 74) res=-1 errno=22
I/qtaguid (22561): Untagging socket 74 failed errno=-22
W/NetworkManagementSocketTagger(22561): untagSocket(74) failed with errno -22
I/ElegantRequestDirector(22561): I/O exception (org.apache.http.NoHttpResponseException) caught when
processing request: The target server failed to respond
I/ElegantRequestDirector(22561): Retrying request
D/Volley  (22561): [2796] BasicNetwork.logSlowRequests: HTTP response for request=<[ ] https://
android.clients.google.com/fdfe/bulkDetails 0xe8d195d1 NORMAL 76> [lifetime=3198], [size=1624], [rc=200],
[retryCount=0]
```

Mobile Application

Android strings

cat app.binary | strings > output.txt or cat app.binary | strings | egrep '.{10,15}'

```
res/drawable/add_icon.png
{{{____RRRMMM
/ ($,,,$(
,-&.!)%-#+'
res/drawable/add_icon_pressed.png
rrrVVVBBB999666ppp
/ ($,,,$(
res/drawable/add_icon_selector.xmle
res/drawable/context_menu_bg.xmlm
res/drawable/context_menu_btn_normal.xmlu
res/drawable/context_menu_btn_pressed.xml]
res/drawable/context_menu_btn_selector.xmle
res/drawable/context_menu_header_bg.xmlu
res/drawable/gradient_btn_disabled.xml
res/drawable/gradient_btn_normal.xml
res/drawable/gradient_btn_pressed.xml
res/drawable/gradient_btn_selector.xml
res/drawable/gradient_cell_bg.xml
res/drawable/gradient_menu_bg.xml]
res/drawable/ic_launcher.png
res/drawable/ice_drive_logo.png
res/drawable/icn_audio.png
```

Mobile Application

smali

smali/baksmali is an assembler/disassembler for the dex format used by dalvik, Android's Java VM implementation.

Mobile Application

smali sample

Example 1 java code
Code:

```
if (flagx == 1)
    flagx = 2
else
    flagx = 3
```

When flagx variable is referenced as v0
Equivalent Example 1 smali code
Code:

```
const/4 v1, 0x1
if-ne v0, v1, :cond_0
const/4 v2, 0x2
move v0,v2
goto :goto_0
```

Mobile Application

Android dex2jar

```
root@Xeno /Users/Jack/Desktop/mobile-presentation
# /opt/android/dex2jar/dex2jar.sh  myandroid.apk
dex2jar version: translator-0.0.9.8
dex2jar myandroid.apk -> myandroid_dex2jar.jar
Done.
```

Mobile Application

Android JD-GUI

Java Decompiler – a.class

myandroid_dex2jar.jar

- c
- d
- e
- model
  - Domain
  - a
  - b
  - c
  - d
  - e
- receiver
  - CameraPhotoReceiver
- service
  - CameraPhotosSyncService
  - MediaSyncService
  - a
  - b
  - c
- view
  - BoundedRelativeLayout
- wrapper
  - DomainCellWrapper
  - a
- ICEDriveApplication
  - ICEDriveApplication
    - a : ICEDriveApplication
    - b : byte[]
    - ICEDriveApplication()
    - a() : Context
    - a(byte[]) : void
    - b() : byte[]
- a
  - a
    - a() : boolean
    - a(Context) : boolean

e.class | ICEDriveApplication.class | a.class

```
    localAlertDialog.setMessage(paramString2);
    localAlertDialog.setButton(paramContext.getString(2131034143), new b());
    localAlertDialog.show();
  }

  public static boolean a()
  {
    String str = Environment.getExternalStorageState();
    if ((!"mounted".equals(str)) && (!"mounted_ro".equals(str)));
    for (boolean bool = false; ; bool = true)
      return bool;
  }

  public static boolean a(Context paramContext)
  {
    NetworkInfo localNetworkInfo = ((ConnectivityManager)paramContext.getSystemService("connectivity")).getActiveN
    if ((localNetworkInfo != null) && (localNetworkInfo.isConnectedOrConnecting()));
    for (boolean bool = true; ; bool = false)
      return bool;
  }

  private static byte[] a(String paramString)
  {
    int i = paramString.length();
    if (i % 2 == 1)
      throw new Exception("Invalid hex string");
    byte[] arrayOfByte = new byte[i / 2];
    for (int j = 0; ; j += 2)
    {
      if (j >= i)
        return arrayOfByte;
      arrayOfByte[(j / 2)] = ((byte)((Character.digit(paramString.charAt(j), 16) << 4) + Character.digit(paramStri
    }
  }

  public static String b(Context paramContext, String paramString)
  {
```

Voor intern gebruik

kpn

Mobile Application

Android Burp

Burp Suite Professional

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Options | Alerts

Intercept | History | Options

Request to https://0b7bd624bab7.mdseclabs.net:443 [67.202.9.175]

Forward | Drop | Intercept is on | Action | Comment this item

Raw | Params | Headers | Hex

```
POST /auth/319/Default.ashx HTTP/1.1
Host: 0b7bd624bab7.mdseclabs.net
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: https://0b7bd624bab7.mdseclabs.net/auth/319/Default.ashx
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

username=admin&password=fme69
```

password — 1 match

Mobile Application

iOS

Mobile Application

iOS

tree - Directory Tree

iExplorder - file downloader from iPhone/iPad

strings - Getting strings from the binary

otool - Determine the binary. use -L for list the used library

class-dump-z - display the uses classes.

Cycript - runtime modification

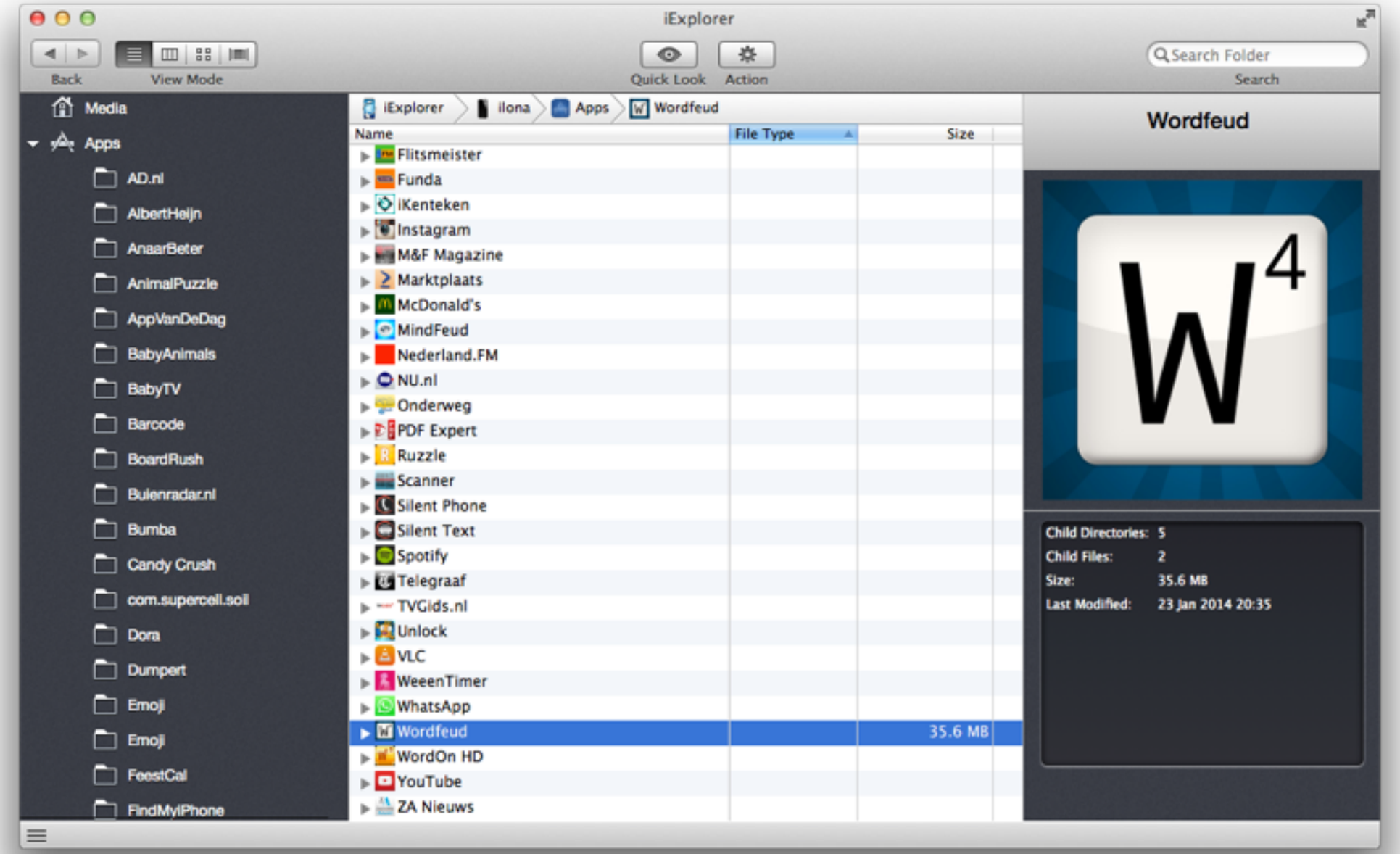
snoop-it - combination of all above.

burp-suite and Wireshark for traffic interception and analyse.

hopper - Disassemble

Mobile Application

iOS iExplorer



Voor intern gebruik

kpn

Mobile Application

iOS .app location

```
find /var/mobile/Applications/ -iname *.app

/var/mobile/Applications/793E0A43-06B5-4836-9BAA-5A7193F48E78/rws.app
/var/mobile/Applications/85E58F55-0010-4382-AF3A-BA49ECD719D4/WebViewService.app
/var/mobile/Applications/89F9DEE0-03C6-467D-AADE-835A0503A2B1/Instagram.app
/var/mobile/Applications/920F3035-0901-4E4C-8CAD-8D339F2D1D6C/NederlandFM.app
/var/mobile/Applications/956F49DF-91B1-42E0-8624-89F1FA529DE7/BoardRush.app
/var/mobile/Applications/A0FAF4FD-60BA-4FCE-8F7D-D46D0AEDE751/DDActionsService.app
/var/mobile/Applications/A9BC54FF-581B-40EB-968F-F3977DBD2957/Funda.app
/var/mobile/Applications/AF790D74-D2D7-4725-997B-6DD24366FCB3/FindMyiPhone.app
/var/mobile/Applications/B644E678-6813-43E9-B224-E9658D9F74EB/AlbertHeijn.app
/var/mobile/Applications/BB7735F5-978D-46A3-8D06-96FEE6E33865/PDFExpertIPhone.app
/var/mobile/Applications/C07D122A-E50B-4422-ADF8-CBC2485BBD60/AppVanDeDag.app
/var/mobile/Applications/C3D00B8A-55EA-4BDC-B518-BEA0D1456479/com.mcpeppergames.AmazingAnimalPuzzleFKAT.app
/var/mobile/Applications/C7187557-83BE-4697-874A-2FD8D6E740DA/BarcodeReader.app
/var/mobile/Applications/D057B088-06AA-4B84-BA8E-AEFC559914A0/iKenteken.app
/var/mobile/Applications/D2BC8039-3493-4B78-A939-CFB1AF04BCA4/Telegraaf.app
/var/mobile/Applications/D2E22B3A-8FD6-45FA-BDB8-3754FF4B35B5/Spotify.app
/var/mobile/Applications/D43706C0-4AA5-4B47-875D-4E3CC9A53E15/StoreKitUIService.app
/var/mobile/Applications/DF7E3FAE-C1F8-4A30-A6C5-91967595495A/dumpert.app
/var/mobile/Applications/ECCCF0FF-CCEE-41DE-93E8-426E7C526FF8/Wordfeud.app
/var/mobile/Applications/ED80E78C-6D39-45D4-A8DB-D04B52695647/MindFeud.app
/var/mobile/Applications/F445A651-43FE-4239-82E1-87D7D242EA4D/Library/Caches/nl.tvgids.app
/var/mobile/Applications/F445A651-43FE-4239-82E1-87D7D242EA4D/TVGids.nl.app
/var/mobile/Applications/F692221C-028C-4E36-9F79-F0F432CBEDB4/AD.nl.app
```

Mobile Application

iOS .ipa file tree

```
# tree -d -L 2
.
|-- Documents
|-- Library
|   |-- Application\ Support
|   |-- Caches
|   |-- Cookies
|   |-- FlurryFiles
|   |-- Preferences
|   `-- SyncedPreferences
|-- StoreKit
|-- Wordfeud.app
|   |-- FinishedGameViewController.nib
|   |-- FinishedGameViewController~ipad.nib
|   |-- FinishedGamesPageViewController.nib
|   |-- FriendStatsViewController.nib
|   |-- NewGameViewController.nib
|   |-- SC_Info
|   |-- SelectRulesetViewController.nib
|   |-- SettingsViewController.nib
|   |-- _CodeSignature
|   |-- de.lproj
|   |-- en.lproj
|   `-- nb.lproj
`-- tmp
```

Mobile Application

iOS otool

Wordfeud.app root#

```
# file Wordfeud
Wordfeud: Mach-O arm_v7 executable
root@Xeno /Users/mark/Desktop/onderzoek
# otool -arch armv7 -l Wordfeud | grep crypt
    cryptoff  16384
    cryptsize 3833856
    cryptid   1
```

Normal With GDB

- Load application
- Init application
- read memory offsets
- dump memory to file
- dd memory part into application
- set Cryptid to 0

```
ilona:~/bin root# clutch
usage: clutch [application name] [...]
Applications available: AD.nl AlbertHeijn AppVanDeDag BabyTVHQME
iPhone BarcodeReader BoardRush Buienradar Bumba candycrushsaga
ColorLEDFlashlightPro com.mcpeppergames.AmazingAnimalPuzzleFKAT
com.mcpeppergames.BabyAnimalsPuzzleFKAT DoraCrystalKingdom
dumpert Emoji Browser EmojiFree FindMyiPhone Flitsmeister Funda
Hay Day iKenteken Instagram Marktplaats McDonalds MindFeud
NederlandFM NU-Universal Onderweg PDFExpertIPhone Rumble
rws SchedJoules Spotify StreepjescodeScanner Telegraaf
TVGids.nl Unlock VLC for iOS VoipPhone WhatsApp
Wordfeud WordOn HD

ilona:~/bin root# clutch MindFeud
Cracking MindFeud...
    /var/root/Documents/Cracked/MindFeud-v5.4.0.ipa
ilona:~/bin root#
```

Mobile Application

iOS strings

cat app.binary | strings > output.txt or cat app.binary | strings | egrep '.{10,15}'

```
Wordfeud.app root# cat Wordfeud | strings | egrep '.{10,15}' | grep "System"
/System/Library/Frameworks/Security.framework/Security
/System/Library/Frameworks/Twitter.framework/Twitter
/System/Library/Frameworks/PassKit.framework/PassKit
/System/Library/Frameworks/AdSupport.framework/AdSupport
/System/Library/Frameworks/Social.framework/Social
/System/Library/Frameworks/Accounts.framework/Accounts
/System/Library/Frameworks/CoreMedia.framework/CoreMedia
/System/Library/Frameworks/AssetsLibrary.framework/AssetsLibrary
/System/Library/Frameworks/EventKitUI.framework/EventKitUI
/System/Library/Frameworks/CoreLocation.framework/CoreLocation
/System/Library/Frameworks/iAd.framework/iAd
/System/Library/Frameworks/StoreKit.framework/StoreKit
/System/Library/Frameworks/OpenAL.framework/OpenAL
/System/Library/Frameworks/AddressBook.framework/AddressBook
/System/Library/Frameworks/AddressBookUI.framework/AddressBookUI
```

Mobile Application

iOS otool

Wordfeud.app root# otool -L Wordfeud

```
Wordfeud:
	/System/Library/Frameworks/Security.framework/Security (compatibility version 1.0.0, current version 1.0.0)
	/System/Library/Frameworks/Twitter.framework/Twitter (compatibility version 1.0.0, current version 164.0.0)
	/System/Library/Frameworks/PassKit.framework/PassKit (compatibility version 1.0.0, current version 1.0.0)
	/System/Library/Frameworks/AdSupport.framework/AdSupport (compatibility version 1.0.0, current version 1.0.0)
	/System/Library/Frameworks/Social.framework/Social (compatibility version 1.0.0, current version 87.0.0)
	/System/Library/Frameworks/Accounts.framework/Accounts (compatibility version 1.0.0, current version 113.0.0)
	/System/Library/Frameworks/CoreMedia.framework/CoreMedia (compatibility version 1.0.0, current version 1.0.0)
	/System/Library/Frameworks/AssetsLibrary.framework/AssetsLibrary (compatibility version 1.0.0, current version 1.0.0)
	/System/Library/Frameworks/EventKitUI.framework/EventKitUI (compatibility version 1.0.0, current version 1.0.0)
	/System/Library/Frameworks/CoreLocation.framework/CoreLocation (compatibility version 1.0.0, current version
1613.5.2)
	/System/Library/Frameworks/iAd.framework/iAd (compatibility version 1.0.0, current version 1.0.0)
```

Mobile Application

iOS otool dissasemble

Wordfeud.app root# otool -tV Wordfeud

```
Wordfeud:
(__TEXT,__text) section
0000bad0    f1e2c293    strnvb  ip, [r2, #35]!
0000bad4    d922ddb9    stmledb r2!, {r0, r3, r4, r5, r7, r8, r10, r11, ip, lr, pc}
0000bad8    788495c6    stmvcia r4, {r1, r2, r6, r7, r8, r10, ip, pc}
0000badc    e709bdbc    undefined
0000bae0    df61fc60    swile   0x0061fc60
0000bae4    e8c461b8    stmia   r4, {r3, r4, r5, r7, r8, sp, lr}^
0000bae8    88c1a83d    stmhiia r1, {r0, r2, r3, r4, r5, r11, sp, pc}^
0000baec    86125f94    undefined
0000baf0    542d734b    strplt  r7, [sp], #-843
0000baf4    fdc0f477    stcnvl  4, cr15, [r0, #476]
0000baf8    f2c39caf    sbcnv   r9, r3, #44800  ; 0xaf00
0000bafc    7d4f82c5    stcvcl  2, cr8, [pc, #-788]
0000bb00    051d430c    ldreq   r4, [sp, #-780]
0000bb04    34cd5e20    strccb  r5, [sp], #3616
0000bb08    8eb1db74    mrchi   11, 5, sp, cr1, cr4, {3}
0000bb0c    45bfe95f    ldrmi   lr, [pc, #2399]!        ; 0xc473
0000bb10    79945d00    ldmvcib r4, {r8, r10, r11, ip, lr}
0000bb14    9929f457    stmlsdb r9!, {r0, r1, r2, r4, r6, r10, ip, sp, lr, pc}
0000bb18    94765d1d    ldrlsbt r5, [r6], #-3357
0000bb1c    ad8d9e91    stcge   14, cr9, [sp, #580]
```


Mobile Application

iOS class-dump-z

Wordfeud.app root#

```
class-dump-z -u armv7 Wordfeud
@interface DTPinLockController : XXUnknownSuperclass <UITextFieldDelegate> {
int mode;
NSArray* pins;
NSArray* pins2;
UITextField* hiddenTextField;
UILabel* message;
UILabel* message2;
UILabel* subMessage;
UINavigationBar* navBar;
BOOL first;
NSString* pin;
id delegate;
UIViewController* baseViewController;
unsigned numberOfDigits;
}
@property(assign, nonatomic) id delegate;
@property(retain, nonatomic) NSString* pin;
@property(assign, nonatomic) unsigned numberOfDigits;
-(id)initWithMode:(int)mode;
-(void)viewWillAppear:(BOOL)view;
-(BOOL)shouldAutorotateToInterfaceOrientation:(int)interfaceOrientation;
```

Mobile Application

iOS cycript

Wordfeud.app root#

```
cycript -p APPname
cy# var myString = [ [ NSString alloc ] initWithString:
cy> @"Hello, world!" ];
"Hello, world!”

cy# *UIApp

cy# [i for (i in *UIApp)]

cy#NSObject.messages
{“cy$toCYON:":0x6c9d5f4,cy$JSType:0x6c9d5ec,"cy$hasProperty:":0x6c9d644,"cy$getProperty:":0x6c9d64c,"cy$getProperty:inContext:":
0x6c9d654,"cy$getPropertyNames:inContext:":0x6c9d7f4,cy$box:0x6c9d5c0,"cy$setProperty:to:":0x6c9d7e4,"cy$deleteProperty:":0x6c9d7ec,"cy
$valueOfInContext:":0x6c9d5e4,"cy$toJSON:inContext:":0x6c9d5c4,"__setSnoopiWatchDog:":0x4bdf99,"matchesATVPredicate:error:":
0x107cc5,"replacementObjectForPortCoder:":0x30838091,classForPortCoder:
0x30838081,"performSelector:onThread:withObject:waitUntilDone:modes:":
0x306d9a85,"performSelectorOnMainThread:withObject:waitUntilDone:modes:":0x307029c9,"performSelectorInBackground:withObject:":
```


Mobile Application

iOS cycript

Wordfeud.app root#

```
cy# function printMethods(className) {
cy>   var count = new new Type("I");
cy>   var methods = class_copyMethodList(objc_getClass(className), count);
cy>   var methodsArray = [];
cy>   for(var i = 0; i < *count; i++) {
cy>     var method = methods[i];
cy>     methodsArray.push({selector:method_getName(method), implementation:method_getImplementation(method)});
cy>   }
cy>   free(methods);
cy>   free(count);
cy>   return methodsArray;
cy> }

cy# UIApp.keyWindow.rootViewController
#"<AppViewController: 0x16d660f0>”

cy# rootVC = UIApp.keyWindow.rootViewController
#"<AppViewController: 0x16d660f0>"

cy# rootVC.visibleViewController
cy# printMethods(AppViewController)
[{selector:@selector(prefersStatusBarhidden),implementation:0x113d3d},{selector:@selector(setPrefersStatusBarhidden:),implementation:0x113d4d},
{selector:@selector(dealloc),implementation:0x113499},{selector:@selector(nextResponder),implementation:0x113505},
{selector:@selector(preferredStatusBarStyle),implementation:0x1134f5},{selector:@selector(prefersStatusBarHidden),implementation:0x1134e5},
{selector:@selector(shouldAutorotate),implementation:0x113729},{selector:@selector(supportedInterfaceOrientations),implementation:0x11372d},
{selector:@selector(viewWillLayoutSubviews),implementation:0x113581},
```


Mobile Application

iOS cycript

```
cy# AppDelegate->isa.messages
{cy$hasImplicitProperties:0x6c9d7f8,"replacementObjectForPortCoder:":0x308380c5,"cancelPreviousPerformRequestsWithTarget:selector:object:":
0x306bcde5,"cancelPreviousPerformRequestsWithTarget:":0x306cf6c1,"implementsSelector:":0x307756c9,"instancesImplementSelector:":
0x3077565d,load:0x306ef761,"setVersion:":0x306f2511,version:0x307757a9,classForKeyedUnarchiver:0x30722161,classFallbacksForKeyedArchiver:
0x30720db5,"_shouldAddObservationForwardersForKey:":0x306f62c9,"setKeys:triggerChangeNotificationsForDependentKey:":
0x3076a849,"_keysForValuesAffectingValueForKey:":0x306f1b59,"automaticallyNotifiesObserversForKey:":
0x306f3655,"keyPathsForValuesAffectingValueForKey:":0x306f1a55,"_createValueGetterWithContainerClassID:key:":
0x306ec585,"_createValueSetterWithContainerClassID:key:":0x306f40f5,"_createValuePrimitiveGetterWithContainerClassID:key:":
0x306ecc2d,"_createValuePrimitiveSetterWithContainerClassID:key:":
0x306f42ed,"_createMutableOrderedSetValueGetterWithContainerClassID:key:"{selector:@selector(shouldAutorotateToInterfaceOrientation:),implem
entation:0x11361d},{selector:@selector(initWithNibName:bundle:),implementation:0x113459},
{selector:@selector(willRotateToInterfaceOrientation:duration:),implementation:0x1135d9},
{selector:@selector(didRotateFromInterfaceOrientation:),implementation:0x113619},{selector:@selector(setPreferredStatusBarStyle:),implementation:
0x113d5d},{selector:@selector(setNextResponder:),implementation:0x113545}]
```

Mobile Application

iOS snoop-it

Marktplaats.app root#

Snoop-it

Marktplaats | Connection Status:

- Monitoring
  - Filesystem
  - Keychain
  - Network
  - Sensitive API
  - Common Crypto
- Analysis
  - Objective-C Classes
  - View Controller
  - URL Schemes
- Runtime Manipulation
  - Hardware Identifier
  - Fake Location
  - Method Tracing

Home | Filesystem | Keychain | Network

Network Access (HTTP requests using NSURLConnection)

Network Summary

Display MIME Types: Text : ☑ Images : ☑ Others : ☑

Display http/https: Http : ☑ Https : ☑

ID	Timestamp	Protocol	URL	Query String
1	23.01.14 21:57:06	https://	settings.crashlytics.com	/spi/v1/platforms/ios/apps/com.marktplaats.iphone/settings?build_version=3.0&display_version=3.0&instance=8656acae3db108b0daa7a8e865b99c9135da7b02&source=4&icon_hash=3816e1fdb9ce28d4da3573fc437b39ea46f33012
2	23.01.14 21:57:09	http://	statisch.marktplaats.com	/html/mobile/version.html
4	23.01.14 21:57:10	https://	api.marktplaats.nl	/api3/config.json?api_ver=3.3&oauth_token=3va7c0phkrtq2v1j76f8v1eu9l&session=670AC3E7-40AF-4737-9AEF-4D7FCC5FC77B&app_ver=3.0&screenWidth=50&screenHeight=75
6	23.01.14 21:57:25	https://	api.marktplaats.nl	/api3/categories.json?api_ver=3.3&oauth_token=3va7c0phkrtq2v1j76f8v1eu9l&session=670AC3E7-40AF-4737-9AEF-4D7FCC5FC77B&app_ver=3.0&screenWidth=50&screenHeight=75
9	23.01.14 21:57:35	https://	ssl.google-analytics.com	/collect?_v=mi3.0.0&cd1=Homepage&av=3.0&cd=%2FHP&cd8=WiFi&t=appview&cd18=Portrait&ul=nl&cd7=iOS7.0&cid=8c594647-13a5-41ae-9e17-11ef34e7ec80&_u=.tnoKoKoKoKoKoKoK-L&tid=UA-39872321-2&sr=320x480&v=1&cd6=iOS3.0&an=Marktplaats&cd9=iPhone+4S&ht=1390510647249&qt=8131&z=18068840164158659837

Details

Debug Report | Search :

JSD OFF

Mobile Application

iOS Burp

Burp Suite Professional

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Options | Alerts

Intercept | History | Options

Request to https://0b7bd624bab7.mdseclabs.net:443 [67.202.9.175]

Forward | Drop | Intercept is on | Action | Comment this item

Raw | Params | Headers | Hex

```
POST /auth/319/Default.ashx HTTP/1.1
Host: 0b7bd624bab7.mdseclabs.net
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: https://0b7bd624bab7.mdseclabs.net/auth/319/Default.ashx
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

username=admin&password=fme69
```

password — 1 match

kpn

Mobile Application

iOS Hopper

[redacted].hop

Read Executable | Back | Follow | D Mark As Data | A Mark As ASCII | C Mark As Code | P Mark As Procedure | S Segments | X Cross References | Show CFG | Pseudo Code | G GDB

Labels | Strings

aes

AES256EncryptedDataUsingKey:error:
AES256EncryptedDataUsingKey:iv:error:
decryptedAES256DataUsingKey:error:
decryptedAES256WithIVDataUsingKey:error:
applicationWillResignActive:
application:willChangeStatusBarOrientation:d...
application:didChangeStatusBarOrientation:
application:willChangeStatusBarFrame:
application:didChangeStatusBarFrame:
application:shouldRestoreApplicationState:
setShouldProcessNamespaces:
connection:didSendBodyData:totalBytesWritte...
absoluteString
nodesForXPath:namespaceMappings:error:
setDavnamespace:
davnamespace
parsesStrictly
weekDateStringForDate:timeZone:
setParsesStrictly:
reachabilityWithAddress:
lowercaseString
namespaceWithName:stringValue:
dataWithBytes:length:
namespaceForPrefix:
attributes
namespaces
resolveNamespaceForName:
resolvePrefixForNamespaceURI:

```
========== B E G I N   O F   P R O C E D U R E ================

                        ; Basic Block Input Regs: r1 r2 r7 sp lr pc -  Killed Regs: r1 r2 r3 r7 r9 sp
                    sub_9710:
10 80B5                 push    {r7, lr}                        ; XREF=0x1c054

========== B E G I N   O F   P R O C E D U R E ================

                        ; Basic Block Input Regs: r1 r2 r7 sp lr pc -  Killed Regs: r1 r2 r3 r7 r9 sp
                    sub_9710:
10 80B5                 push    {r7, lr}                        ; XREF=0x1c054
24 0093                 str     r3, [sp, #0x4 + var_0]
26 7944                 add     r1, pc                          ; 0x3a688
28 4B46                 mov     r3, r9
2a 0968                 ldr     r1, [r1]                        ; @selector(AES256EncryptedDataUsingKey:iv:e
2c 27F00AEC             blx     imp___symbolstub1__objc_msgSend
30 01B0                 add     sp, #0x4
32 80BD                 pop     {r7, pc}
                ; endp

========== B E G I N   O F   P R O C E D U R E ================

                        ; Basic Block Input Regs: r0 r1 r4 r5 r6 r7 sp lr pc -  Killed Regs: r0 r1 r2 r3 r4 r5 r6 r7
                    sub_9734:
34 F0B5                 push    {r4, r5, r6, r7, lr}            ; XREF=0xe62e, 0xe65a, 0xe686, 0xe6b2, 0xe6d
36 0646                 mov     r6, r0
38 40F61C30             movw    r0, #0xb1c
3c C0F20300             movt    r0, #0x3
40 41F27272             movw    r2, #0x1772
44 C0F20302             movt    r2, #0x3
48 7844                 add     r0, pc                          ; 0x3a268
4a 7A44                 add     r2, pc                          ; 0x3aec0
4c 0C46                 mov     r4, r1
4e 0168                 ldr     r1, [r0]                        ; @selector(alloc)
50 03AF                 add     r7, sp, #0xc
52 1068                 ldr     r0, [r2]                        ; @bind__OBJC_CLASS_$_NSString
54 27F0F6EB             blx     imp___symbolstub1__objc_msgSend
```

Analysis segment __objc_catlist
Analysis segment __objc_protolist
Analysis segment __objc_imageinfo
Analysis segment __objc_const
Analysis segment __objc_selrefs
Analysis segment __objc_protorefs
Analysis segment __objc_classrefs
Analysis segment __objc_superrefs
Analysis segment __objc_data
Analysis segment __objc_ivar
Analysis segment __cfstring

Address 0x9704, Segment __text, sub_96e0 + 36, file offset 0x8704

kpn

Mobile Application

Resources list

Snoop-it - https://code.google.com/p/snoop-it/wiki/GettingStarted

Cycript - http://www.andreas-kurtz.de/2013/07/how-to-easily-spot-broken-cryptography.html

Dex2Jar - http://code.google.com/p/dex2jar/

JD-GUI - http://jd.benow.ca/

otool - https://github.com/gdbinit/otool-ng

clutch - https://github.com/KJCracks/Clutch/releases