Vaccinating APK’s

Milan Gabor & Danijel Grah

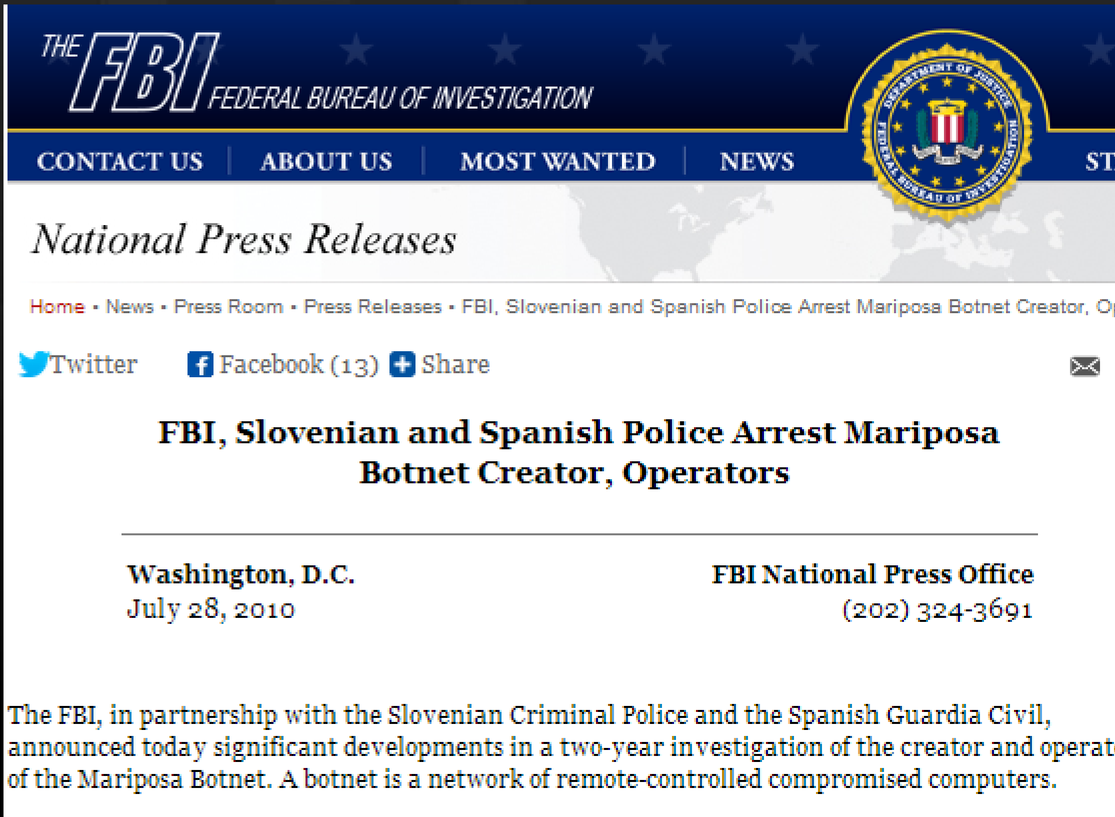
#/viris

Who_are_we?

- Slovenia
- Having fun
- Google us;)

POLAND
GERMANY
CZECH REPUBLIC
SLOVAKIA
FRANCE
AUSTRIA
HUNGARY
SWITZERLAND
CROATIA
BOSNIA & HERZEGOVINA
ITALY
SPAIN

Do you know him?



National Press Releases

Home • News • Press Room • Press Releases • FBI, Slovenian and Spanish Police Arrest Mariposa Botnet Creator, O

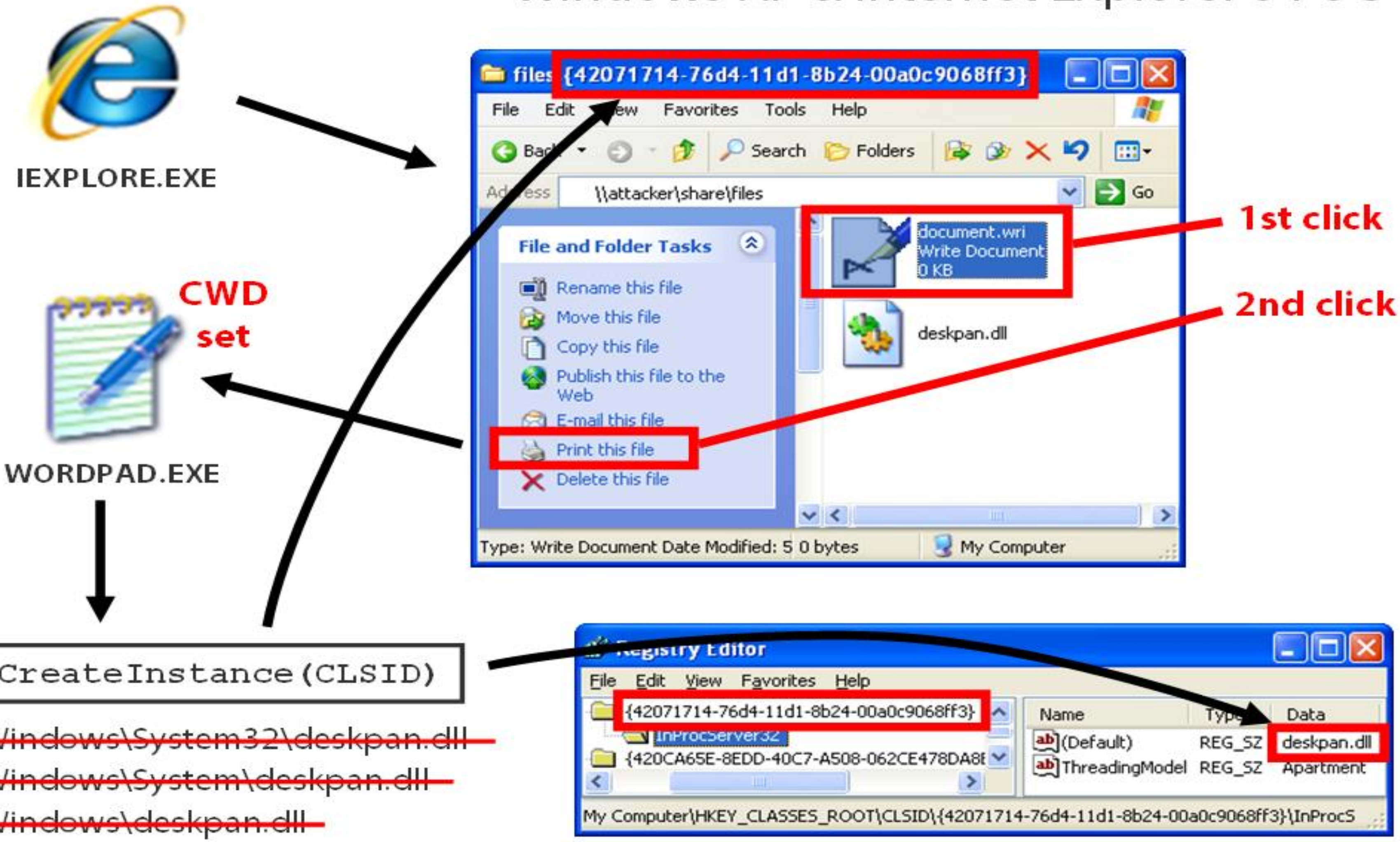
FBI, Slovenian and Spanish Police Arrest Mariposa Botnet Creator, Operators

Washington, D.C.
July 28, 2010

FBI National Press Office
(202) 324-3691

The FBI, in partnership with the Slovenian Criminal Police and the Spanish Guardia Civil, announced today significant developments in a two-year investigation of the creator and operat of the Mariposa Botnet. A botnet is a network of remote-controlled compromised computers.

Windows XP & Internet Explorer 8 PoC



files {42071714-76d4-11d1-8b24-00a0c9068ff3}

\\attacker\share\files

document.wri
Write Document
0 KB

deskpan.dll

Type: Write Document Date Modified: 5 0 bytes My Computer

CoCreateInstance(CLSID)

~~C:\Windows\System32\deskpan.dll~~

~~C:\Windows\System\deskpan.dll~~

~~C:\Windows\deskpan.dll~~

{42071714-76d4-11d1-8b24-00a0c9068ff3}
InProcServer32
{420CA65E-8EDD-40C7-A508-062CE478DA8E

Name	Type	Data
(Default)	REG_SZ	deskpan.dll
ThreadingModel	REG_SZ	Apartment

My Computer\HKEY_CLASSES_ROOT\CLSID\{42071714-76d4-11d1-8b24-00a0c9068ff3}\InProcS

WHERE
ARE
WE?
TODAY

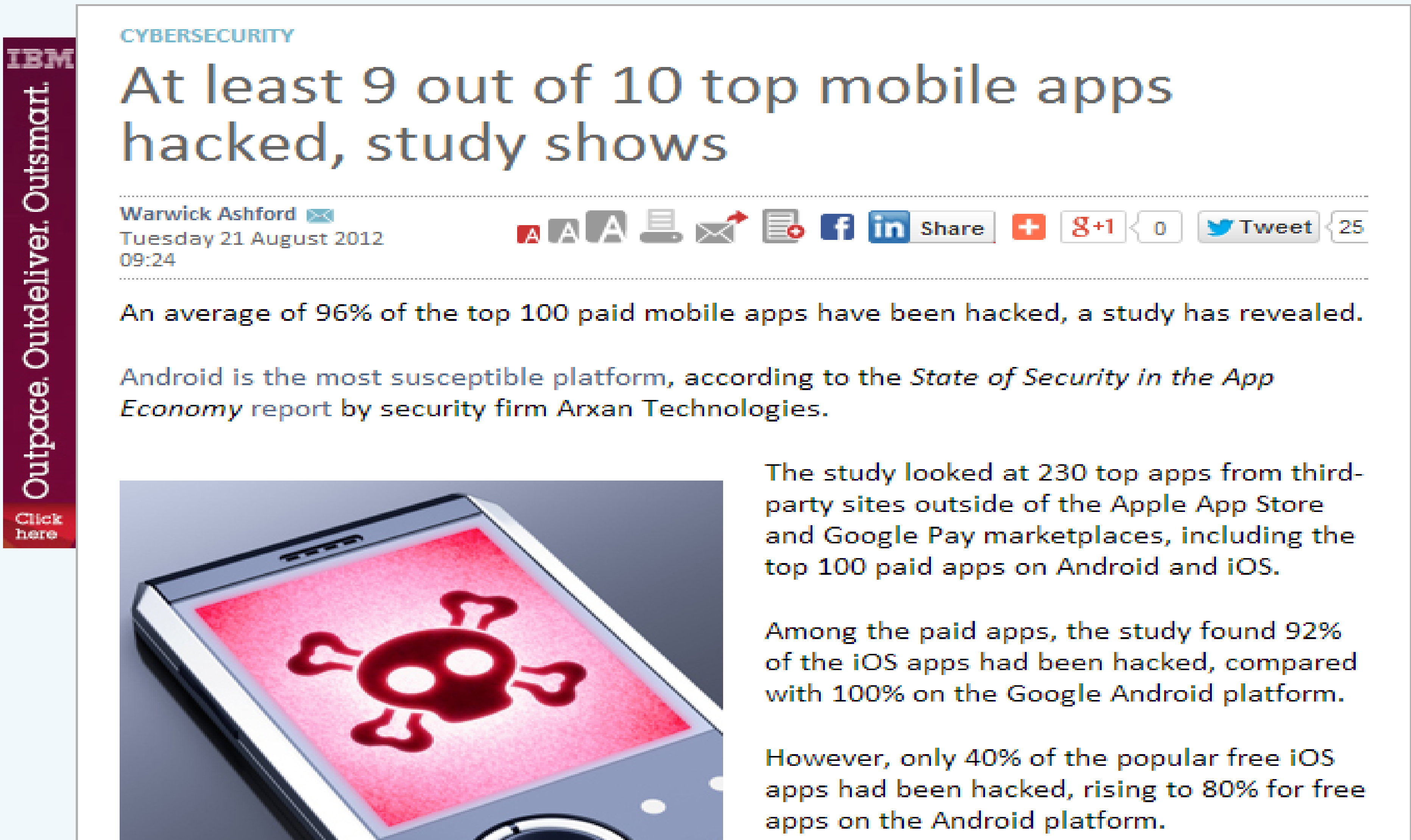
complexity
want
architects
Principle
just
Sounds
example
solution
shows
extra
drawbacks
working
help
one
looking
increasingly
handle
day
call
anymore
tools
really
capable
loose
still
like
layer
PC
box
top
oke
simple
scientific
Living
cleverly
ways
maybe
abstracting
work
also
oversight
day-to-day
article
used
getting
bother
higher
domain
understand
societal
left
abstraction
hide
possible
designers
start
new
scarce
need
Dutch
happening
simplify
PC's
complex
find
ecosystems
chaos
putting
favourite
way
accessed
certainly
society
total
ingewikkeld
whatever
little
People
things
interactions
questions
complicated
average
hidden
clever
internal
user
levels
splendid
complexitywill
diminish
yet
black-boxes
abstract
insane
order
inside
given
Consider
Emergence
trouble
picture
adding
boxes
rising
HW
comes
Take
inner
SW-wise
highly
tool
dirty
accept
interact
around
certain
black
details
HW/SW
life
Edge
social
device
virtual
science
fail

Client
Tester
Manager
Developer

~~WEB~~ DEVELOPERS

zach nicodemous

Status 2012



CYBERSECURITY

At least 9 out of 10 top mobile apps hacked, study shows

Warwick Ashford
Tuesday 21 August 2012
09:24

An average of 96% of the top 100 paid mobile apps have been hacked, a study has revealed.

Android is the most susceptible platform, according to the *State of Security in the App Economy* report by security firm Arxan Technologies.

The study looked at 230 top apps from third-party sites outside of the Apple App Store and Google Pay marketplaces, including the top 100 paid apps on Android and iOS.

Among the paid apps, the study found 92% of the iOS apps had been hacked, compared with 100% on the Google Android platform.

However, only 40% of the popular free iOS apps had been hacked, rising to 80% for free apps on the Android platform.

Status 2013(4)

HP research finds vulnerabilities in 9 of 10 mobile apps

Summary: Obvious security vulnerabilities are disturbingly common in corporate mobile apps. If HP can find them, so can malicious actors.

By Larry Seltzer for Zero Day | November 19, 2013 -- 13:15 GMT (05:15 PST)

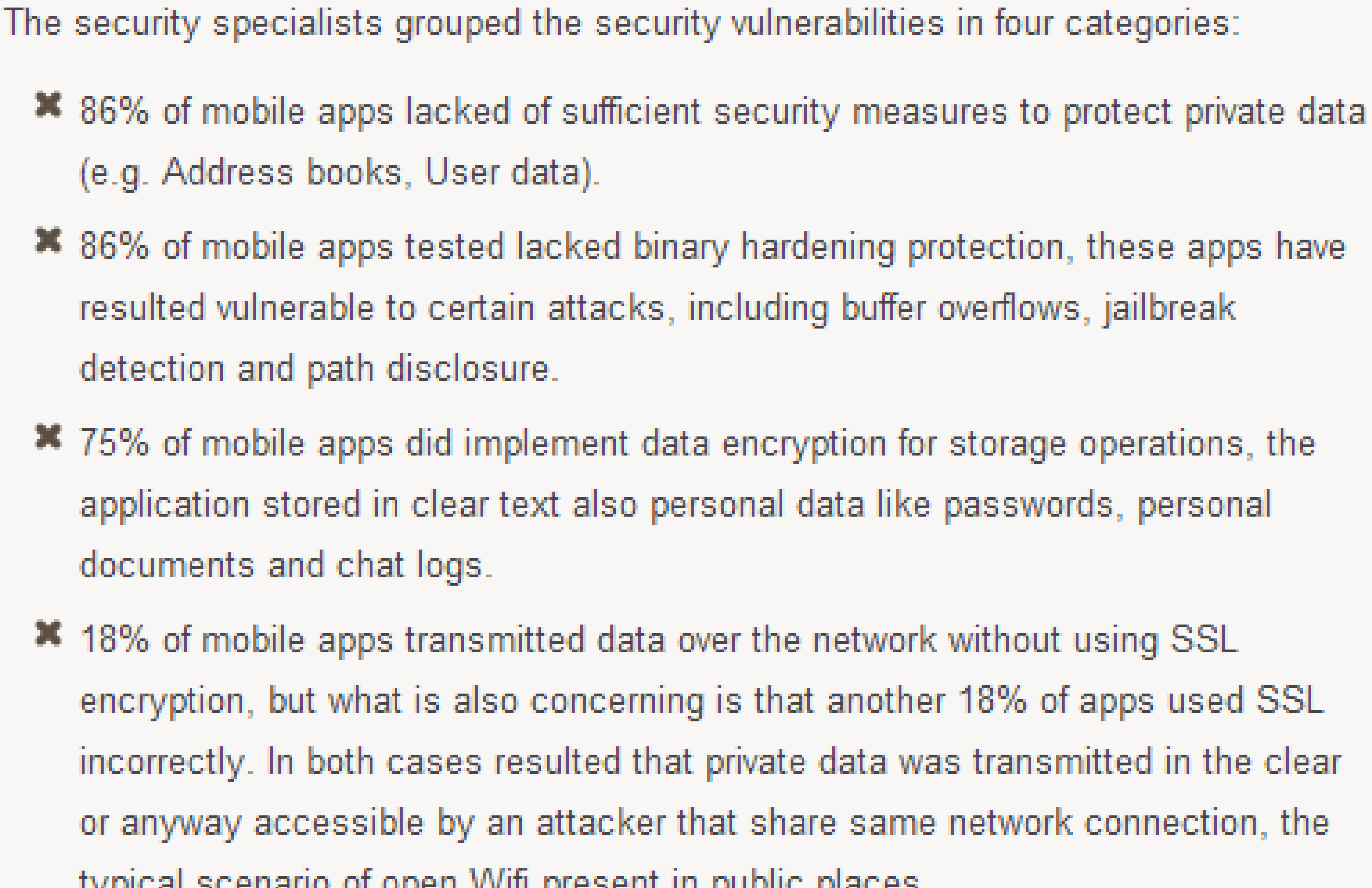
Tests run by HP Fortify, the company's enterprise security arm, indicate that 90% of mobile apps have at least one security vulnerability.

The company used their Fortify On Demand for Mobile product to test the security posture of 2,107 applications published by 601 companies on the Forbes Global 2000. Only iOS apps were tested, but HP says that there is good reason to believe the same problems exist in any Android counterparts.

Overall, the problems fell into one of four categories. The analysis showed that 86% of apps that accessed potentially private data sources, such as address books or Bluetooth connections, lacked sufficient security measures to protect the data from access.

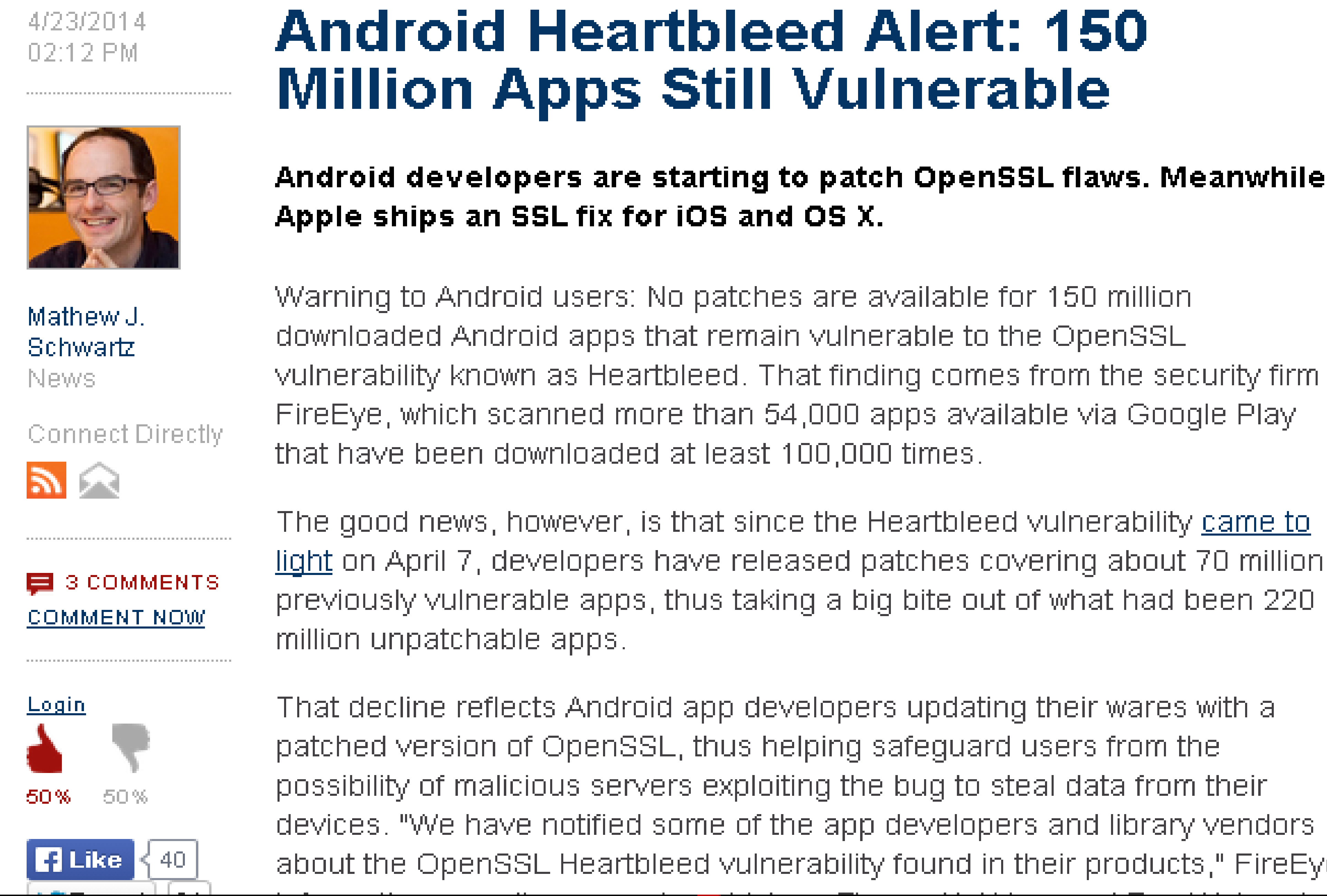
86% of apps tested lacked binary hardening protection. This refers to a group of techniques, many implemented simply with checkboxes at compile time, which protect against certain attacks, like buffer overflows, path disclosure and jailbreak detection.

Enough motivation?



The security specialists grouped the security vulnerabilities in four categories:

- 86% of mobile apps lacked of sufficient security measures to protect private data (e.g. Address books, User data).
- 86% of mobile apps tested lacked binary hardening protection, these apps have resulted vulnerable to certain attacks, including buffer overflows, jailbreak detection and path disclosure.
- 75% of mobile apps did implement data encryption for storage operations, the application stored in clear text also personal data like passwords, personal documents and chat logs.
- 18% of mobile apps transmitted data over the network without using SSL encryption, but what is also concerning is that another 18% of apps used SSL incorrectly. In both cases resulted that private data was transmitted in the clear or anyway accessible by an attacker that share same network connection, the typical scenario of open Wifi present in public places.



4/23/2014
02:12 PM

Mathew J. Schwartz
News

Android Heartbleed Alert: 150 Million Apps Still Vulnerable

Android developers are starting to patch OpenSSL flaws. Meanwhile Apple ships an SSL fix for iOS and OS X.

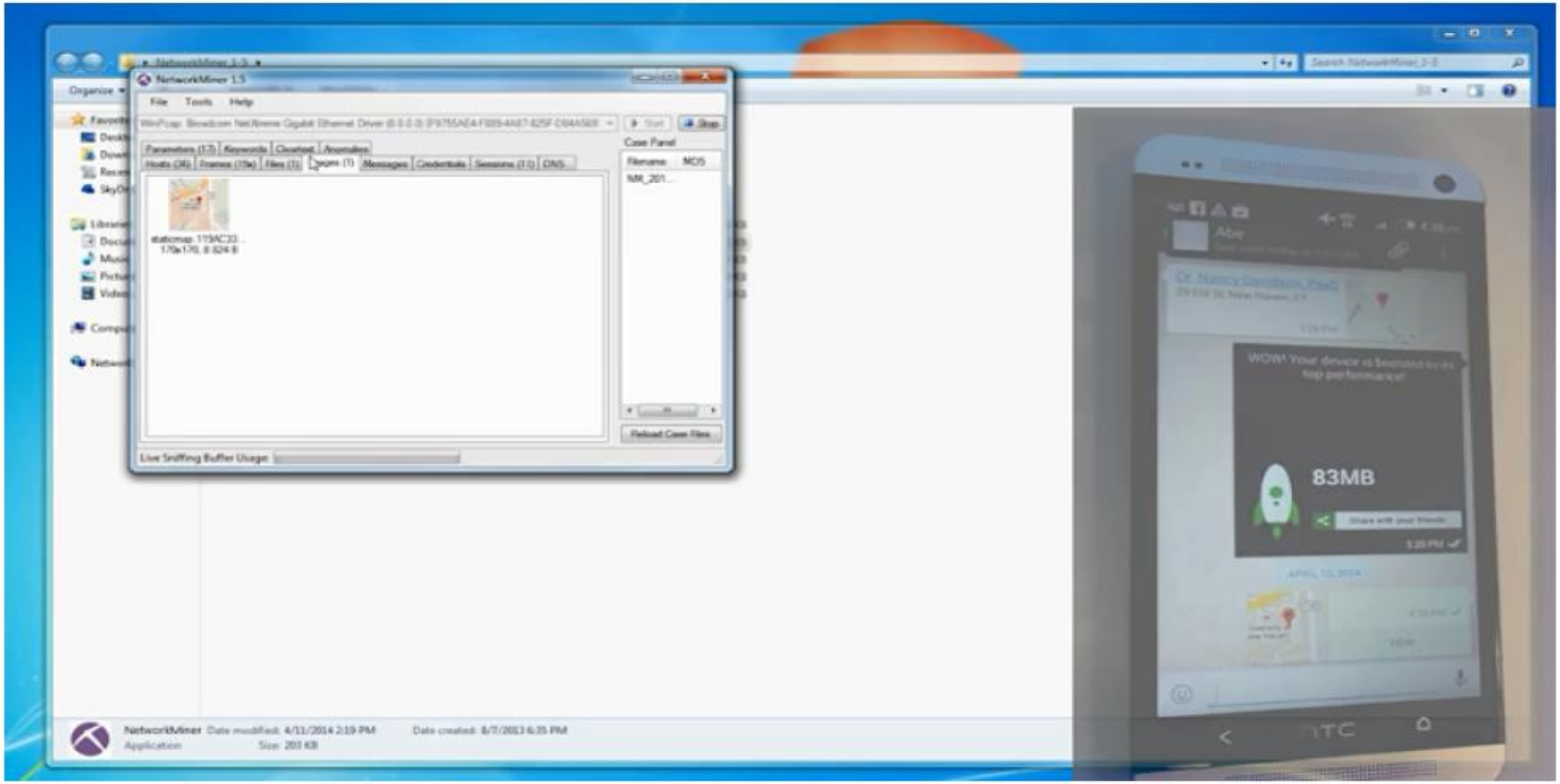
Warning to Android users: No patches are available for 150 million downloaded Android apps that remain vulnerable to the OpenSSL vulnerability known as Heartbleed. That finding comes from the security firm FireEye, which scanned more than 54,000 apps available via Google Play that have been downloaded at least 100,000 times.

The good news, however, is that since the Heartbleed vulnerability came to light on April 7, developers have released patches covering about 70 million previously vulnerable apps, thus taking a big bite out of what had been 220 million unpatchable apps.

That decline reflects Android app developers updating their wares with a patched version of OpenSSL, thus helping safeguard users from the possibility of malicious servers exploiting the bug to steal data from their devices. "We have notified some of the app developers and library vendors about the OpenSSL Heartbleed vulnerability found in their products," FireEy

WhatsApp Flaw leaves User Location Vulnerable to Hackers and Spy Agencies

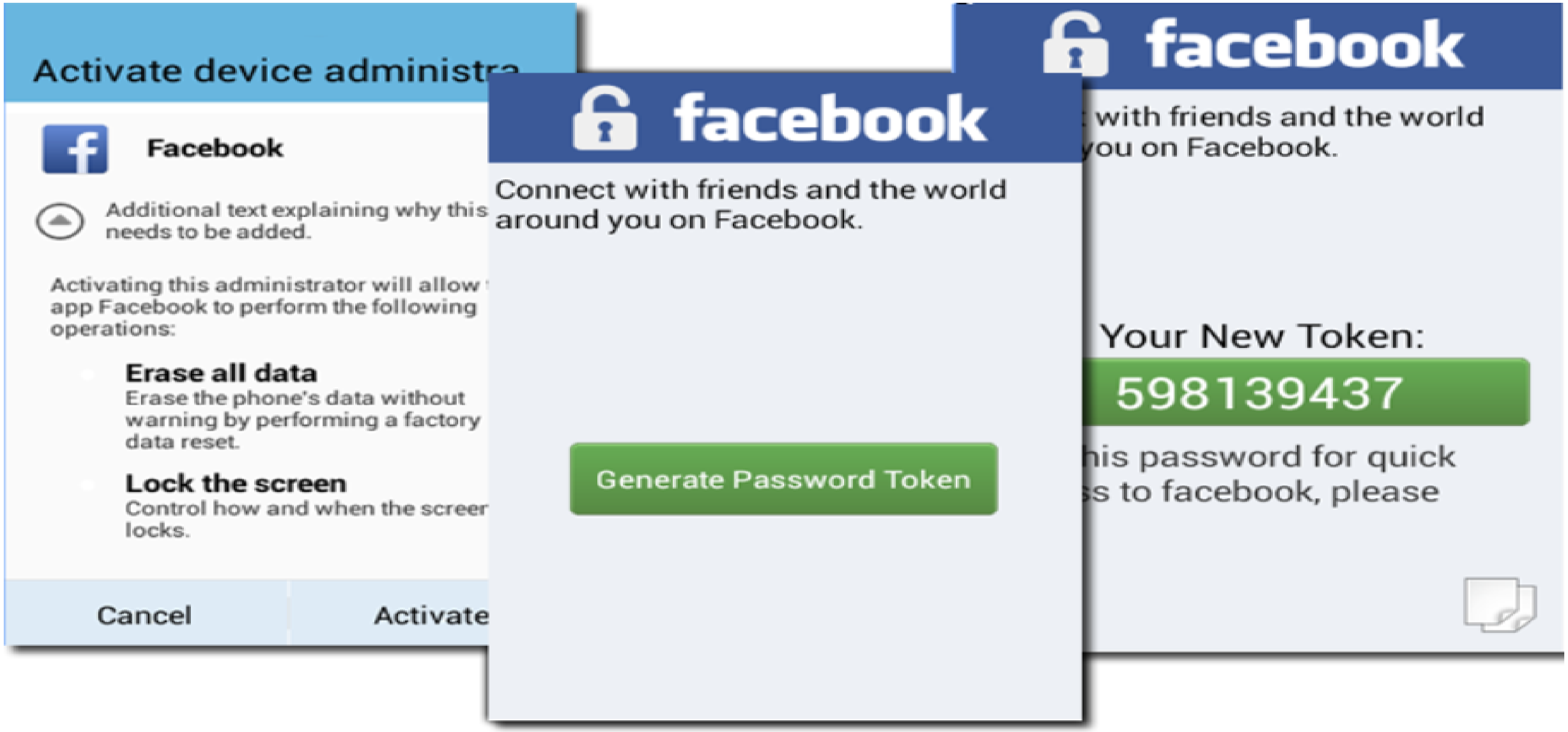
Tuesday, April 15, 2014 by Swati Khandelwal


NetworkMiner 1.5
File Tools Help
Case Panel
Live Sniffing Buffer Usage:
Reload Case Files
WOW! Your device is boosted to its top performance!
83MB
NetworkMiner Date modified: 4/11/2014 2:19 PM
Date created: 8/7/2013 6:35 PM
Application
Size: 203 KB

If you are using WhatsApp to chit-chat with your friends or relatives, then you should be careful about sharing your location with them using WhatsApp 'Location Share' feature.

iBanking Android Malware targeting Facebook Users with Web Injection techniques

Wednesday, April 16, 2014 by Swati Khandelwal



Activate device administra

Facebook

Additional text explaining why this needs to be added.

Activating this administrator will allow t app Facebook to perform the following operations:

Erase all data
Erase the phone's data without warning by performing a factory data reset.

Lock the screen
Control how and when the screen locks.

Cancel | Activate

facebook

Connect with friends and the world around you on Facebook.

Generate Password Token

facebook

t with friends and the world you on Facebook.

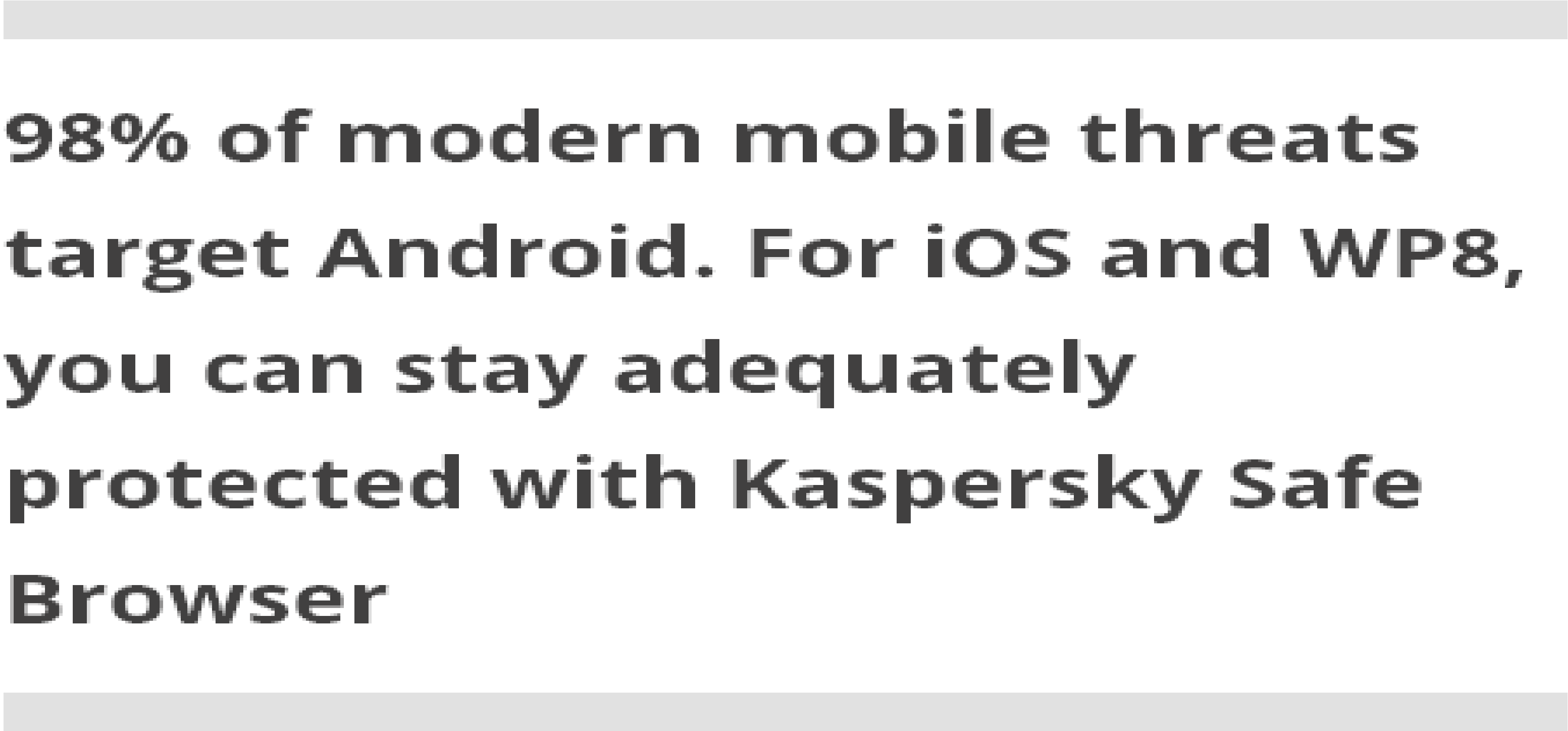
Your New Token:

598139437

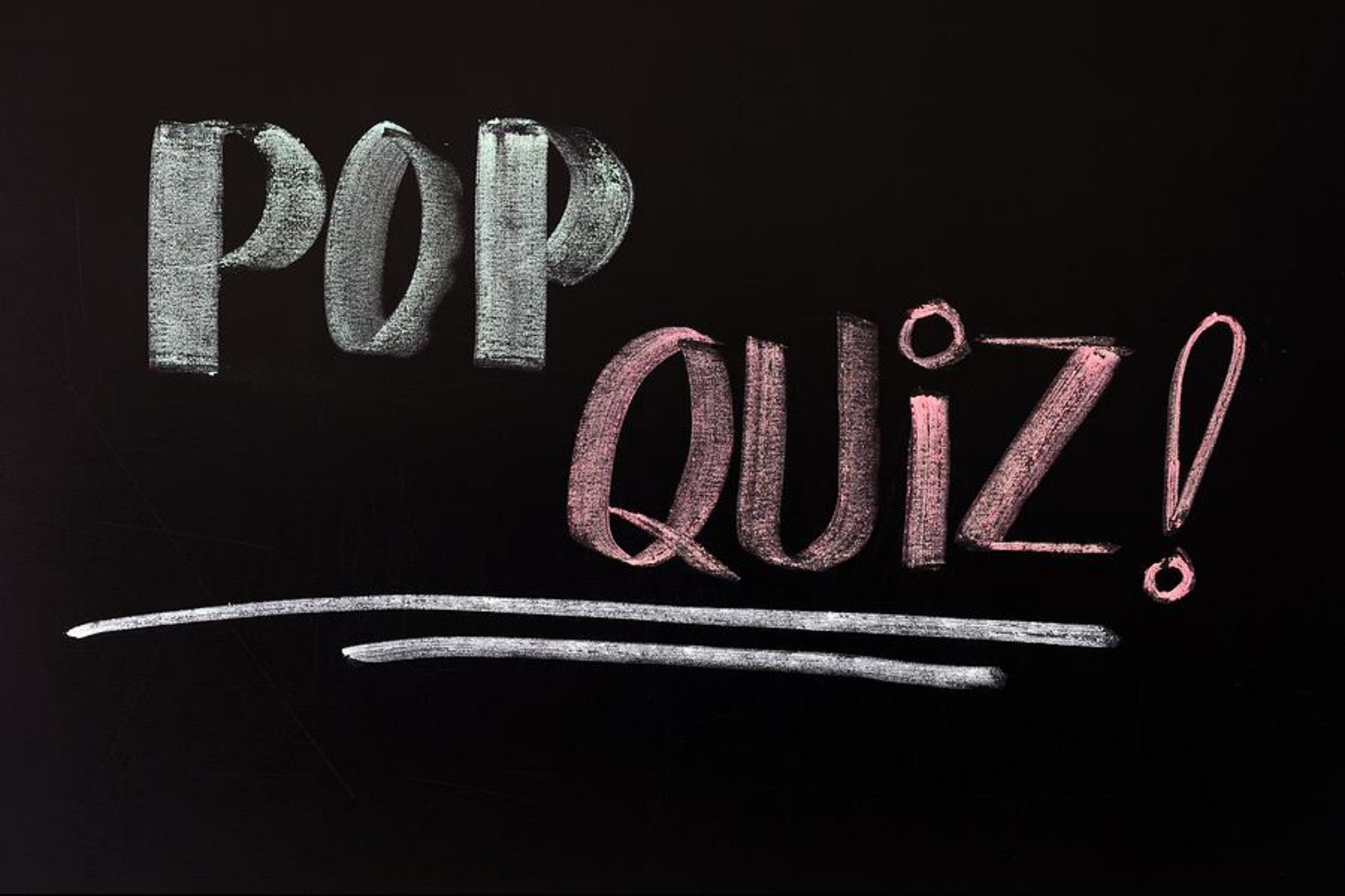
his password for quick s to facebook, please

iBanking is nothing but a mobile banking Trojan app which impersonates itself as a so-called '*Security App*' for Android devices and distributed through HTML injection attacks on banking sites, in order to deceive its victims.

Kaspersky says …



98% of modern mobile threats target Android. For iOS and WP8, you can stay adequately protected with Kaspersky Safe Browser


POP
QUIZ!

Lock it and don't use it?

WHAT'S YOUR STORY?

It started …

> That shall

> not be named?

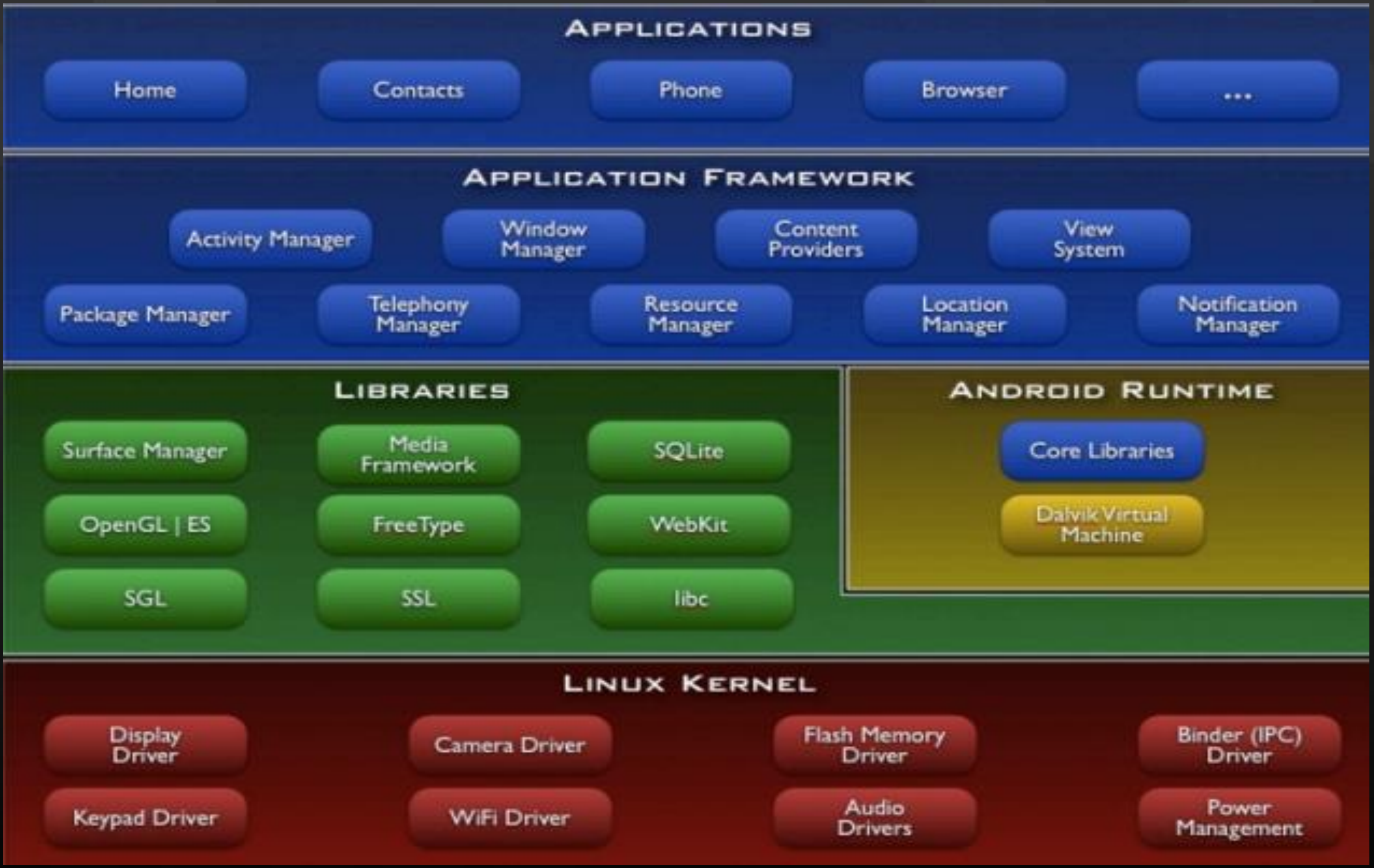
Things

- Need for testing mobile apps
- Mobile app development feels like late 90's development
- Our own analysis

Why?

- Developers focused on features not security
- Developers not aware of underlying platform
- Users don't care about security

Complicated!



APPLICATIONS

Home | Contacts | Phone | Browser | ...

APPLICATION FRAMEWORK

Activity Manager | Window Manager | Content Providers | View System

Package Manager | Telephony Manager | Resource Manager | Location Manager | Notification Manager

LIBRARIES

Surface Manager | Media Framework | SQLite

OpenGL | ES | FreeType | WebKit

SGL | SSL | libc

ANDROID RUNTIME

Core Libraries

Dalvik Virtual Machine

LINUX KERNEL

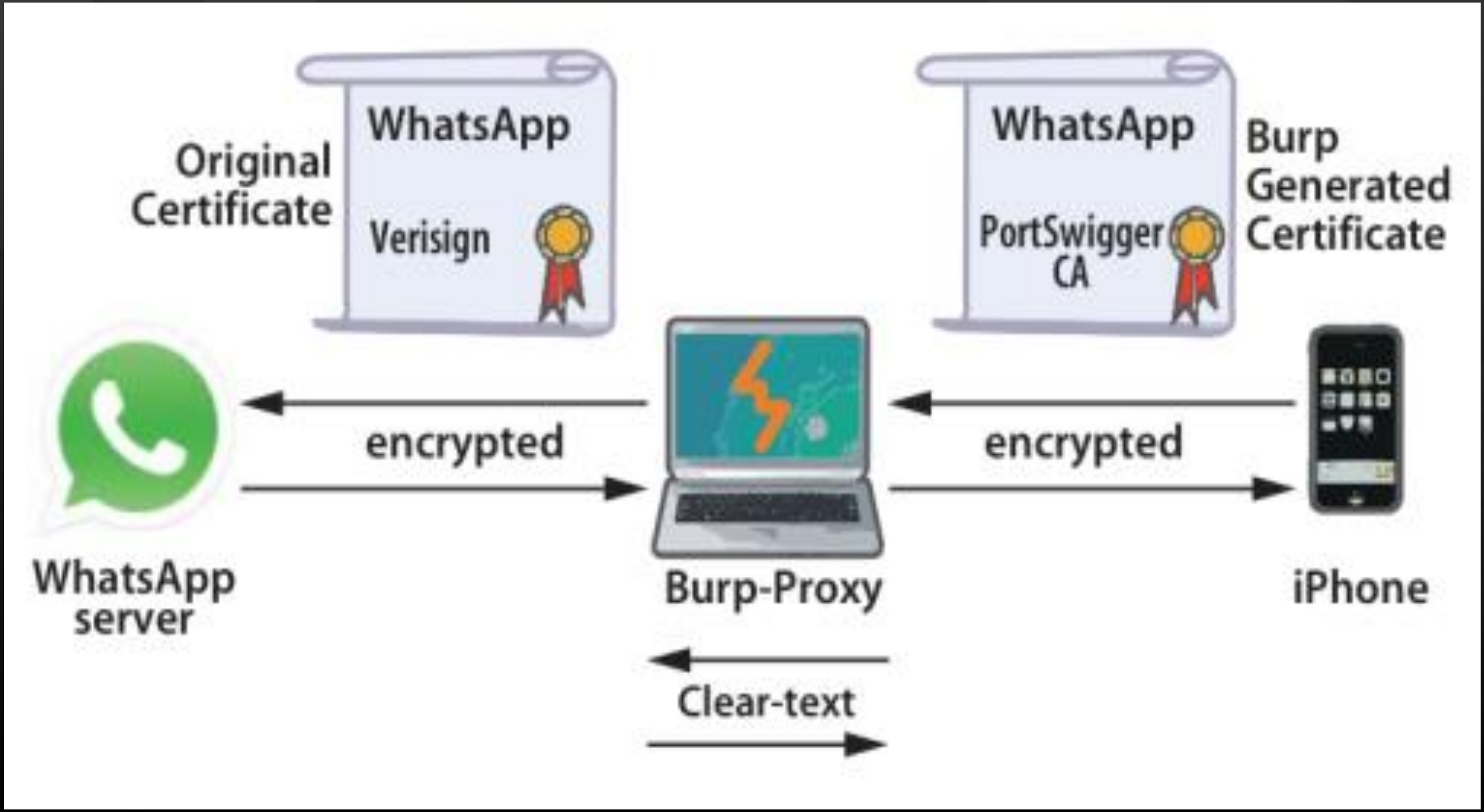
Display Driver | Camera Driver | Flash Memory Driver | Binder (IPC) Driver

Keypad Driver | WiFi Driver | Audio Drivers | Power Management

Mobile App pentest

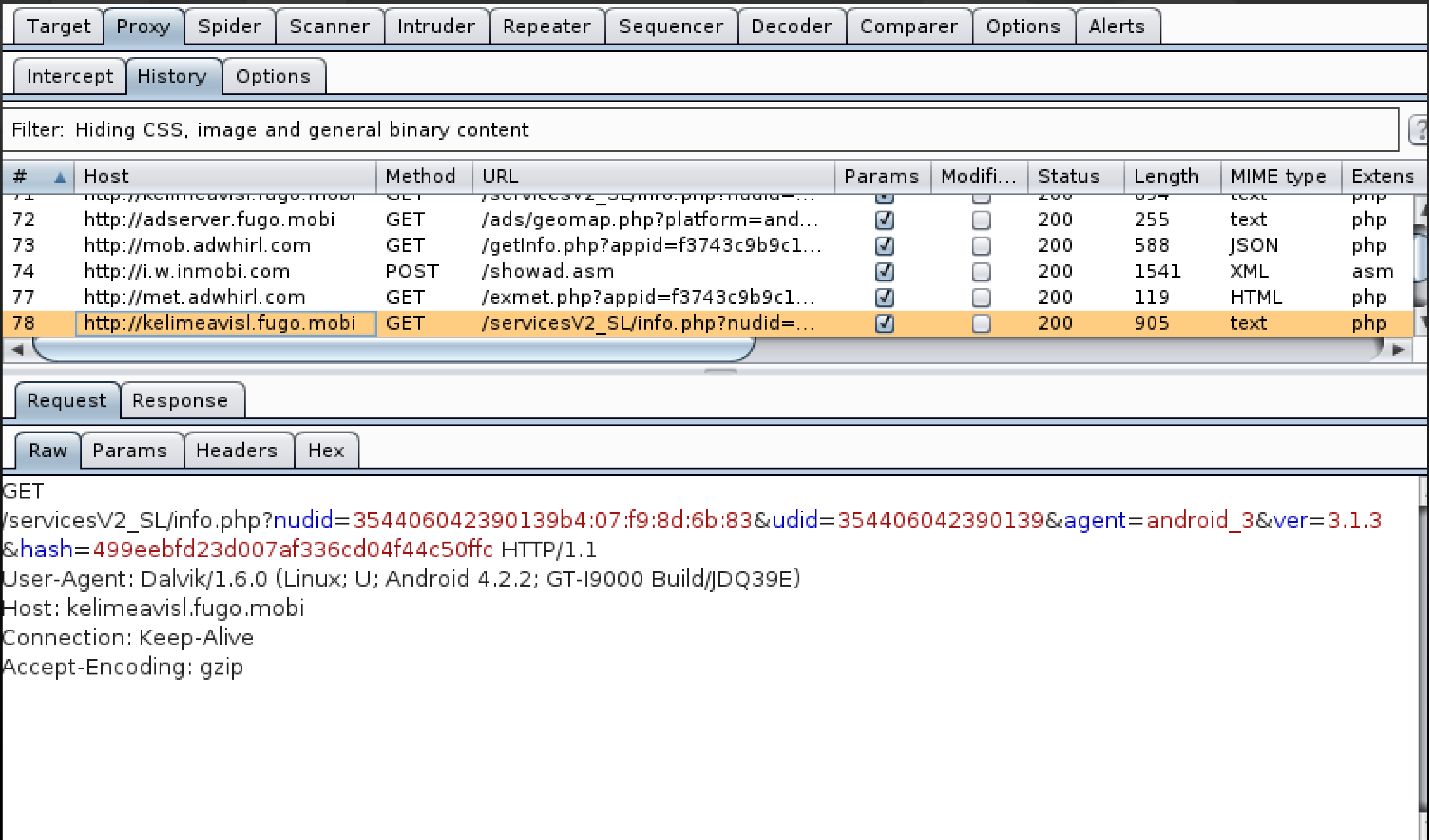
- Start emulator with proxy
- Install app in emulator
- Use Wireshark, Fiddler &/|| Burp to monitor network traffic
- Run app, see logs, dumps

Classics



Original Certificate
WhatsApp
Verisign
WhatsApp
PortSwigger CA
Burp Generated Certificate
encrypted
encrypted
WhatsApp server
Burp-Proxy
iPhone
Clear-text

Request

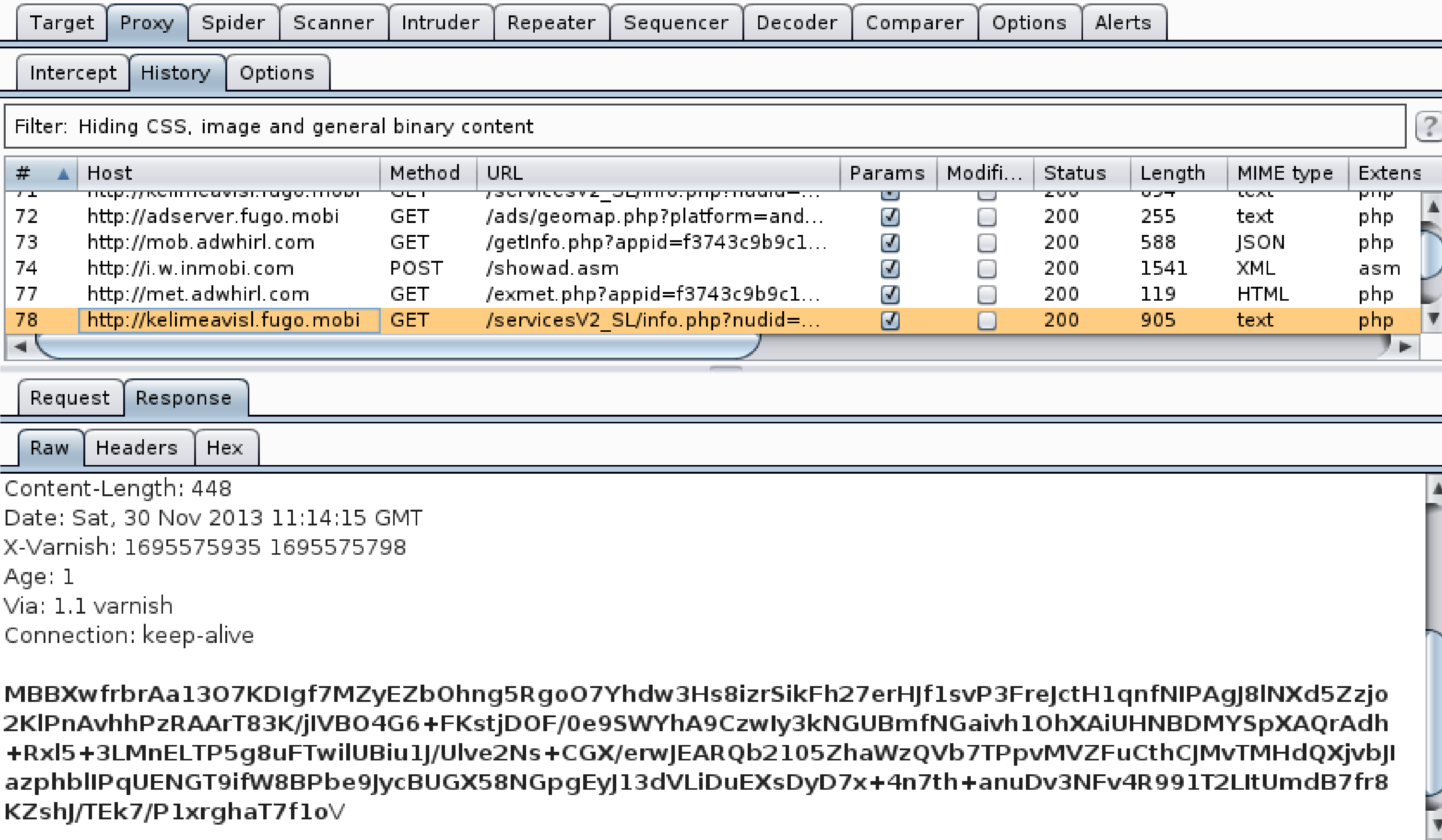


Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params	Modifi...	Status	Length	MIME type	Extens
71	http://kelimeavisl.fugo.mobi	GET	/servicesV2_SL/info.php?nudid=...	☑	☐	200	894	text	php
72	http://adserver.fugo.mobi	GET	/ads/geomap.php?platform=and...	☑	☐	200	255	text	php
73	http://mob.adwhirl.com	GET	/getInfo.php?appid=f3743c9b9c1...	☑	☐	200	588	JSON	php
74	http://i.w.inmobi.com	POST	/showad.asm	☑	☐	200	1541	XML	asm
77	http://met.adwhirl.com	GET	/exmet.php?appid=f3743c9b9c1...	☑	☐	200	119	HTML	php
78	http://kelimeavisl.fugo.mobi	GET	/servicesV2_SL/info.php?nudid=...	☑	☐	200	905	text	php

```
GET
/servicesV2_SL/info.php?nudid=354406042390139b4:07:f9:8d:6b:83&udid=354406042390139&agent=android_3&ver=3.1.3
&hash=499eebfd23d007af336cd04f44c50ffc HTTP/1.1
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.2.2; GT-I9000 Build/JDQ39E)
Host: kelimeavisl.fugo.mobi
Connection: Keep-Alive
Accept-Encoding: gzip
```

Reply



Filter: Hiding CSS, image and general binary content

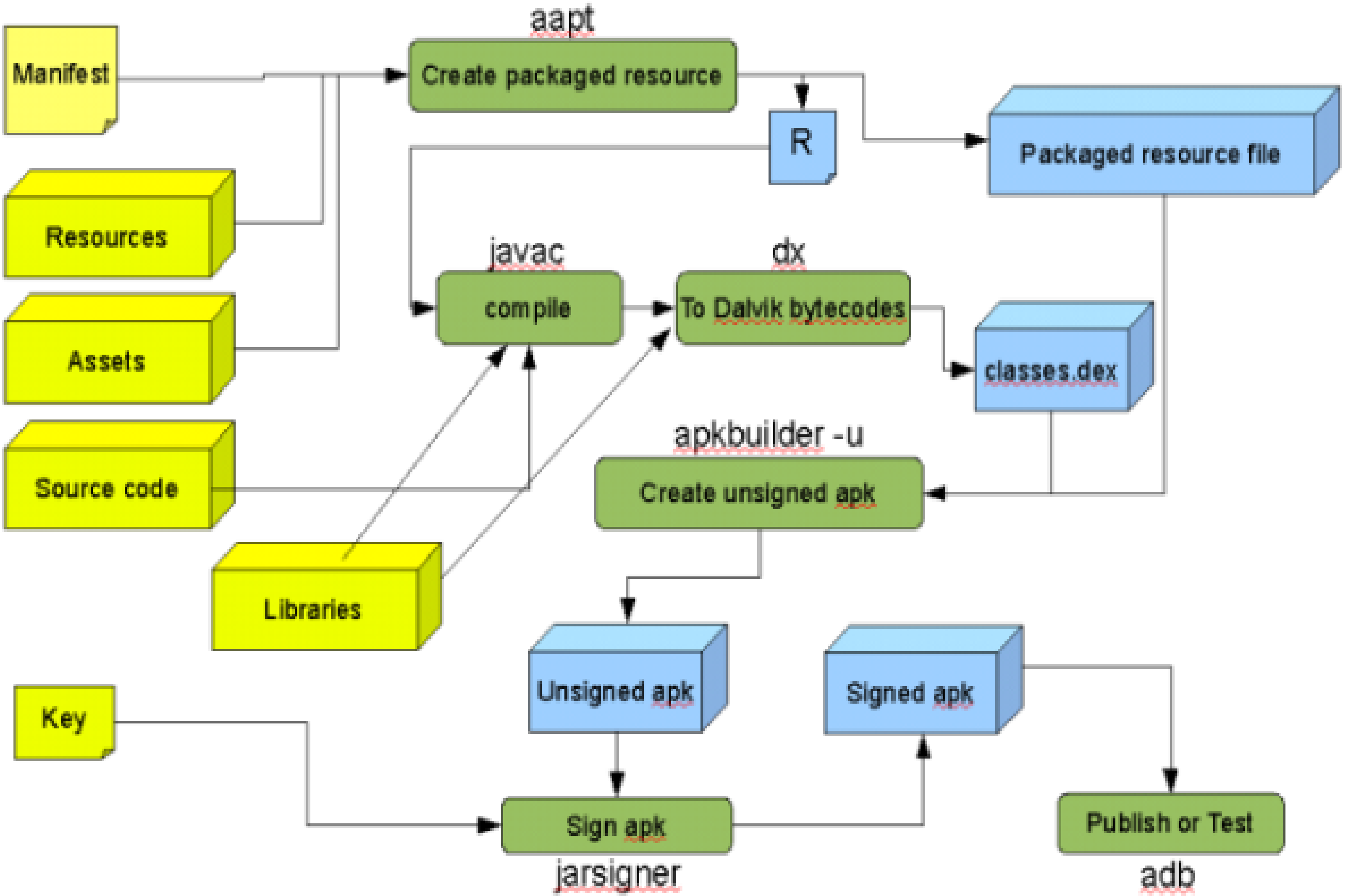
#	Host	Method	URL	Params	Modifi...	Status	Length	MIME type	Extens
71	http://kelimeavisl.fugo.mobi	GET	/servicesV2_SL/info.php?nudid=...	☑	□	200	[illegible]	text	php
72	http://adserver.fugo.mobi	GET	/ads/geomap.php?platform=and...	☑	□	200	255	text	php
73	http://mob.adwhirl.com	GET	/getInfo.php?appid=f3743c9b9c1...	☑	□	200	588	JSON	php
74	http://i.w.inmobi.com	POST	/showad.asm	☑	□	200	1541	XML	asm
77	http://met.adwhirl.com	GET	/exmet.php?appid=f3743c9b9c1...	☑	□	200	119	HTML	php
78	http://kelimeavisl.fugo.mobi	GET	/servicesV2_SL/info.php?nudid=...	☑	□	200	905	text	php

```
Content-Length: 448
Date: Sat, 30 Nov 2013 11:14:15 GMT
X-Varnish: 1695575935 1695575798
Age: 1
Via: 1.1 varnish
Connection: keep-alive
```

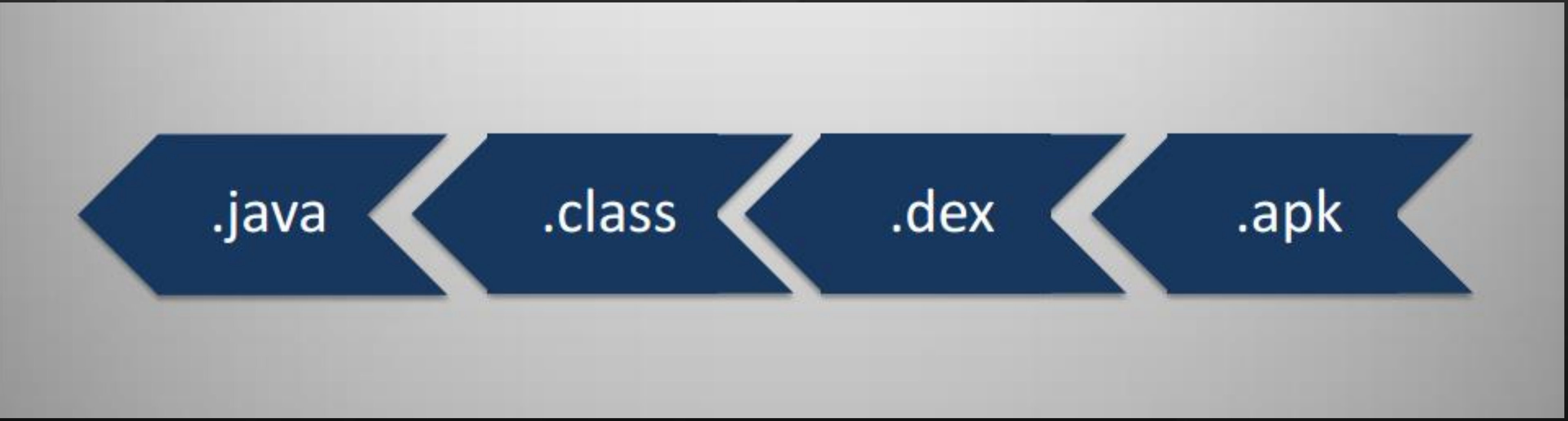
MBBXwfrbrAa13O7KDIgf7MZyEZbOhng5RgoO7Yhdw3Hs8izrSikFh27erHJf1svP3FreJctH1qnfNIPAgJ8lNXd5Zzjo
2KlPnAvhhPzRAArT83K/jIVBO4G6+FKstjDOF/0e9SWYhA9CzwIy3kNGUBmfNGaivh1OhXAiUHNBDMYSpXAQrAdh
+Rxl5+3LMnELTP5g8uFTwilUBiu1J/Ulve2Ns+CGX/erwJEARQb2105ZhaWzQVb7TPpvMVZFuCthCJMvTMHdQXjvbJI
azphblIPqUENGT9ifW8BPbe9JycBUGX58NGpgEyJ13dVLiDuEXsDyD7x+4n7th+anuDv3NFv4R991T2LItUmdB7fr8
KZshJ/TEk7/P1xrghaT7f1oV

Android Applications

- .apk (Android Package) format
- Nothing more than a zip
- Written exclusively in Java, with native libraries in C/C++.
- Composed of components like Activities, Services, Broadcast Receivers, etc.


aapt
Create packaged resource
Manifest
R
Packaged resource file
Resources
javac
compile
dx
To Dalvik bytecodes
Assets
classes.dex
apkbuilder -u
Source code
Create unsigned apk
Libraries
Unsigned apk
Signed apk
Key
Sign apk
jarsigner
Publish or Test
adb

Reversing APK



Reversing APK

- > Dex2Jar
- > JD-GUI
- > (Bak) smali
- > APKTool

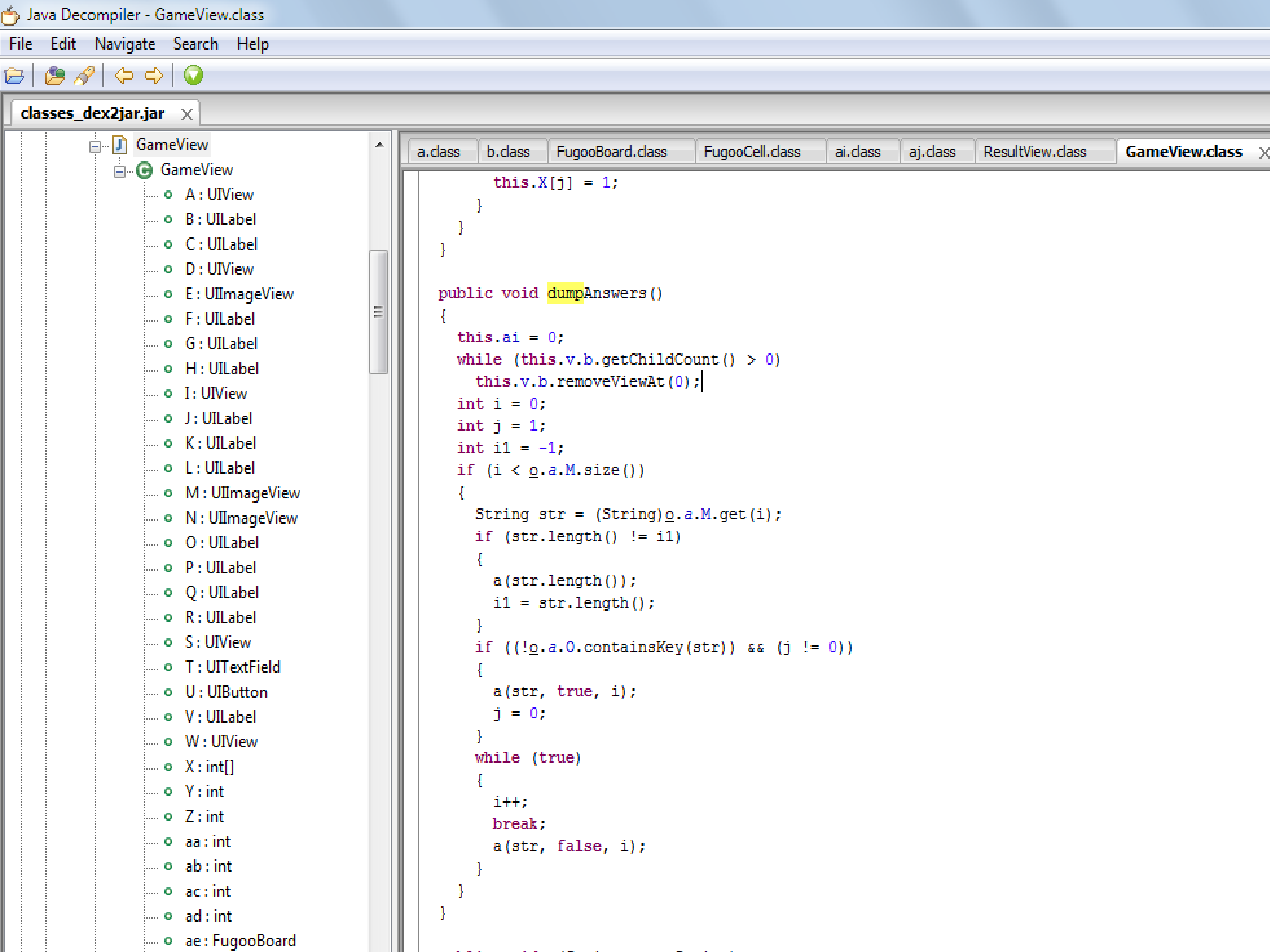
Procedure

> Pull from phone.

```
adb pull /data/app(or app-private)/app1.apk
unzip app1.apk
dex2jar classes.dex
jdgui classes2jar.jar
```

or convert to smali and then analyse the code

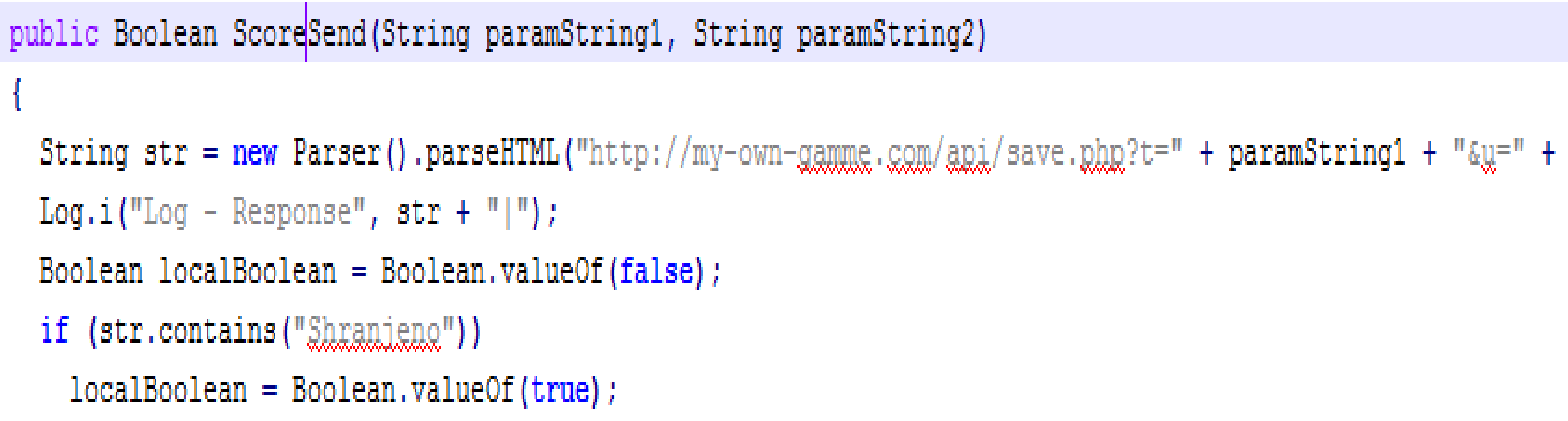
```
adb pull /data/app/app1.apk
unzip app1.apk
java -jar baksmali.jar -o C:\pentest\app\classes.dex
```



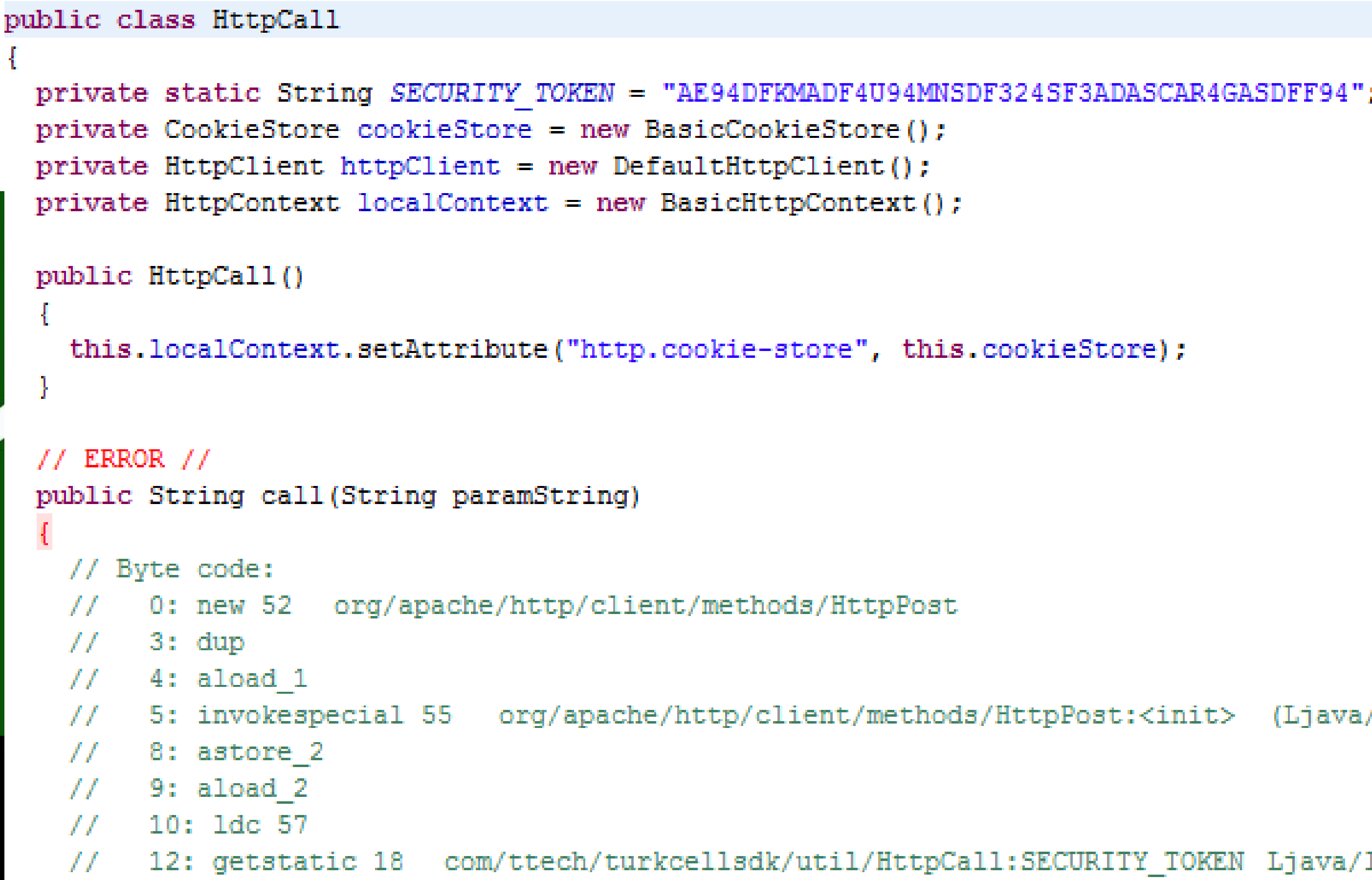
```
GameView
  GameView
    A : UIView
    B : UILabel
    C : UILabel
    D : UIView
    E : UIImageView
    F : UILabel
    G : UILabel
    H : UILabel
    I : UIView
    J : UILabel
    K : UILabel
    L : UILabel
    M : UIImageView
    N : UIImageView
    O : UILabel
    P : UILabel
    Q : UILabel
    R : UILabel
    S : UIView
    T : UITextField
    U : UIButton
    V : UILabel
    W : UIView
    X : int[]
    Y : int
    Z : int
    aa : int
    ab : int
    ac : int
    ad : int
    ae : FugooBoard
```

```
          this.X[j] = 1;
        }
      }
    }

    public void dumpAnswers()
    {
      this.ai = 0;
      while (this.v.b.getChildCount() > 0)
        this.v.b.removeViewAt(0);
      int i = 0;
      int j = 1;
      int i1 = -1;
      if (i < o.a.M.size())
      {
        String str = (String)o.a.M.get(i);
        if (str.length() != i1)
        {
          a(str.length());
          i1 = str.length();
        }
        if ((!o.a.O.containsKey(str)) && (j != 0))
        {
          a(str, true, i);
          j = 0;
        }
        while (true)
        {
          i++;
          break;
          a(str, false, i);
        }
      }
    }
```



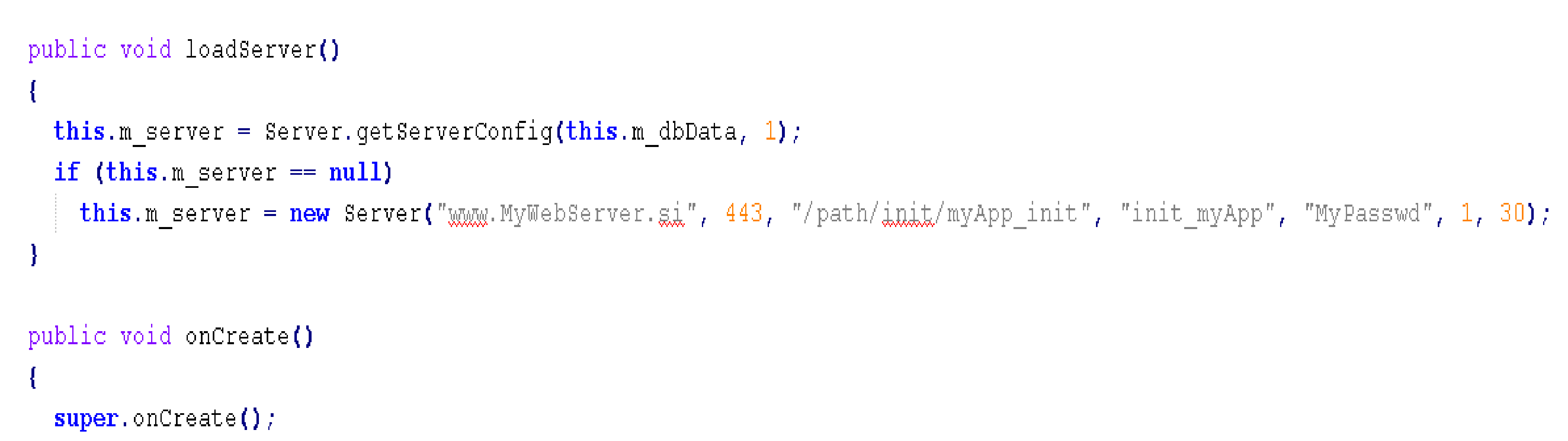
```
public Boolean ScoreSend(String paramString1, String paramString2)
{
  String str = new Parser().parseHTML("http://my-own-gamme.com/api/save.php?t=" + paramString1 + "&u=" +
  Log.i("Log - Response", str + "|");
  Boolean localBoolean = Boolean.valueOf(false);
  if (str.contains("Shranjeno"))
    localBoolean = Boolean.valueOf(true);
  return localBoolean;
}
```



```
public class HttpCall
{
  private static String SECURITY_TOKEN = "AE94DFKMADF4U94MNSDF324SF3ADASCAR4GASDFF94";
  private CookieStore cookieStore = new BasicCookieStore();
  private HttpClient httpClient = new DefaultHttpClient();
  private HttpContext localContext = new BasicHttpContext();

  public HttpCall()
  {
    this.localContext.setAttribute("http.cookie-store", this.cookieStore);
  }

  // ERROR //
  public String call(String paramString)
  {
    // Byte code:
    //   0: new 52   org/apache/http/client/methods/HttpPost
    //   3: dup
    //   4: aload_1
    //   5: invokespecial 55   org/apache/http/client/methods/HttpPost:<init>   (Ljava/
    //   8: astore_2
    //   9: aload_2
    //   10: ldc 57
    //   12: getstatic 18   com/ttech/turkcellsdk/util/HttpCall:SECURITY_TOKEN  Ljava/l
```



```
public void loadServer()
{
  this.m_server = Server.getServerConfig(this.m_dbData, 1);
  if (this.m_server == null)
    this.m_server = new Server("www.MyWebServer.si", 443, "/path/init/myApp_init", "init_myApp", "MyPasswd", 1, 30);
}

public void onCreate()
{
  super.onCreate();
```

YOU CAN
EXPECT
THE
UNEXPECTED
IAMRIDICULOUS.COM

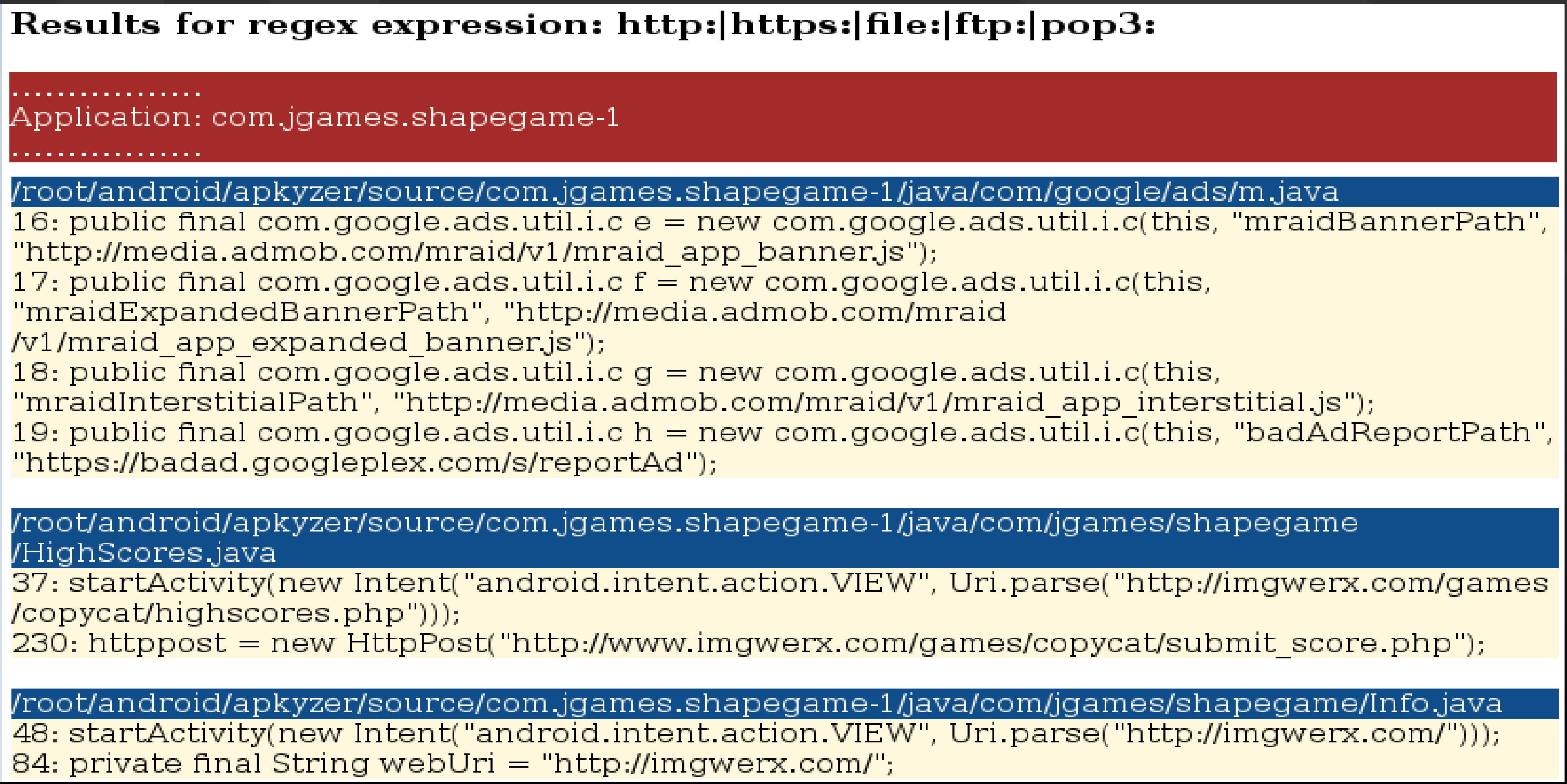
Static

- Able to read Java code
- Cannot see all runtime replies
- Obfuscated?
- Identify important segments in code

Static

- Apkyzer
  - Unzip, dex2jar, jad, bash, html
- More apk‘s at once
- WebView addJavascriptInterface Remote Code Execution (September 24, 2013, https://labs.mwrinfosecurity.com/blog/2013/09/24/webview-addjavascriptinterface-remote-code-execution/)
  - grep -r -n -i --include=*.java addJavascriptInterface *
- Result.html

apkyzer



Results for regex expression: http:|https:|file:|ftp:|pop3:

```
.................
Application: com.jgames.shapegame-1
.................

/root/android/apkyzer/source/com.jgames.shapegame-1/java/com/google/ads/m.java
16: public final com.google.ads.util.i.c e = new com.google.ads.util.i.c(this, "mraidBannerPath",
"http://media.admob.com/mraid/v1/mraid_app_banner.js");
17: public final com.google.ads.util.i.c f = new com.google.ads.util.i.c(this,
"mraidExpandedBannerPath", "http://media.admob.com/mraid
/v1/mraid_app_expanded_banner.js");
18: public final com.google.ads.util.i.c g = new com.google.ads.util.i.c(this,
"mraidInterstitialPath", "http://media.admob.com/mraid/v1/mraid_app_interstitial.js");
19: public final com.google.ads.util.i.c h = new com.google.ads.util.i.c(this, "badAdReportPath",
"https://badad.googleplex.com/s/reportAd");

/root/android/apkyzer/source/com.jgames.shapegame-1/java/com/jgames/shapegame
/HighScores.java
37: startActivity(new Intent("android.intent.action.VIEW", Uri.parse("http://imgwerx.com/games
/copycat/highscores.php")));
230: httppost = new HttpPost("http://www.imgwerx.com/games/copycat/submit_score.php");

/root/android/apkyzer/source/com.jgames.shapegame-1/java/com/jgames/shapegame/Info.java
48: startActivity(new Intent("android.intent.action.VIEW", Uri.parse("http://imgwerx.com/")));
84: private final String webUri = "http://imgwerx.com/";
```

Dynamical analysis

- Monitoring/changing traffic with proxy
- Debugging
- Remoting

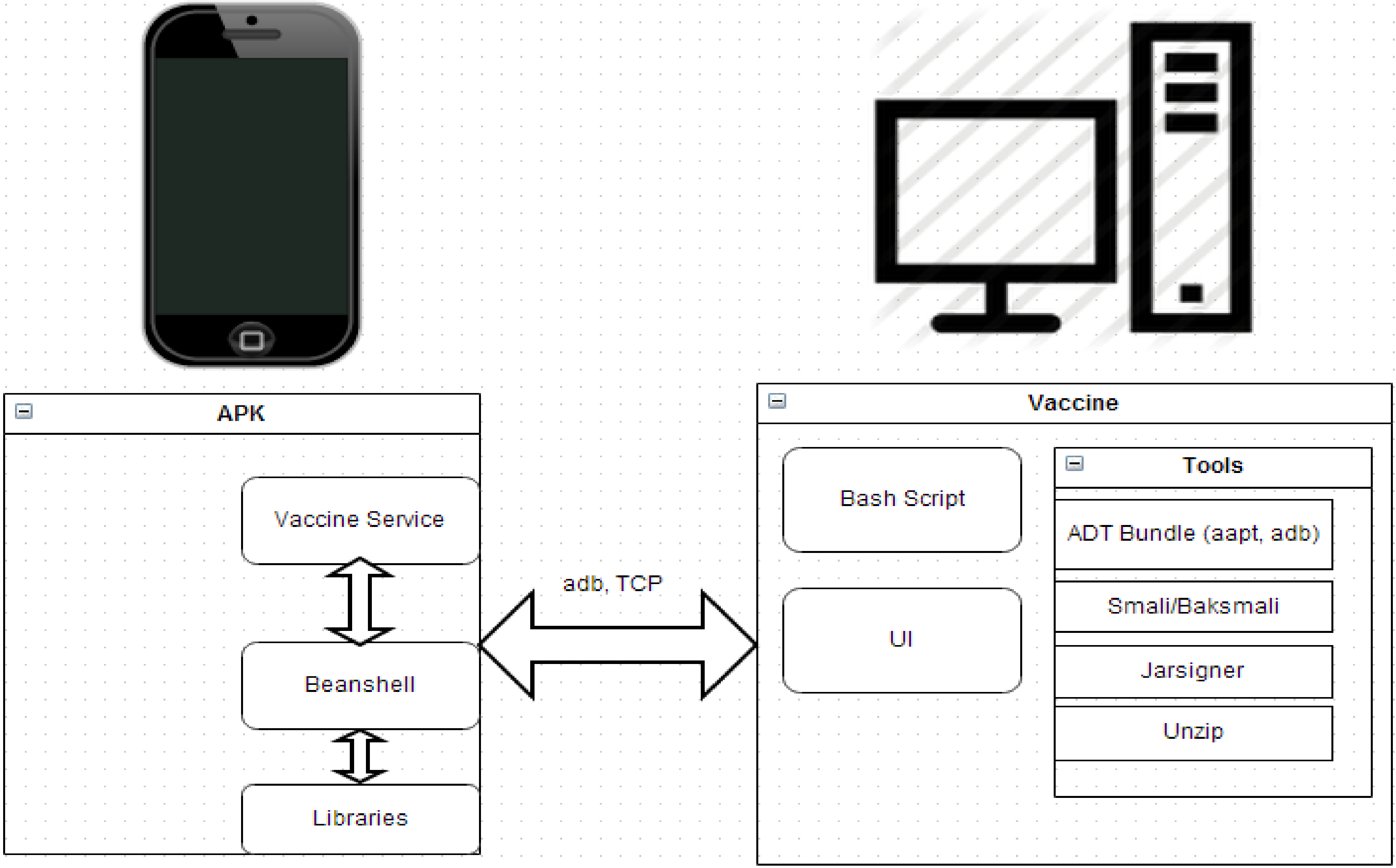
Debugging vs remoting

- Higher level view
- Better idea how application works
- Java like access to objects, methods, variables
- Interaction with application

Vaccine

- Fino (https://github.com/sysdream/fino)
- Repackaging
- Service injection
- Injecting Beanshell
- Connection and Dynamical analysis

APK



APK

Vaccine Service

Beanshell

Libraries

adb, TCP

Vaccine

Bash Script

UI

Tools

ADT Bundle (aapt, adb)

Smali/Baksmali

Jarsigner

Unzip

Features

- Access all variables
- Change values of variables
- Call functions
- Use variables and scripts
- Use full beanshell
- Write Java code

Features

- Access all variables
- Change values of variables
- Call functions
- Use variables and scripts
- Use full beanshell
- Write Java code

Disclaimer

This presentation was created for educational purposes. We will not take any responsibility for any action you cause using the information shown in this presentation. Please do not contact us with blackhat type hacking requests.

Thanks!

Original taken from: http://www.lo0.ro/

Let‘s play game(s)

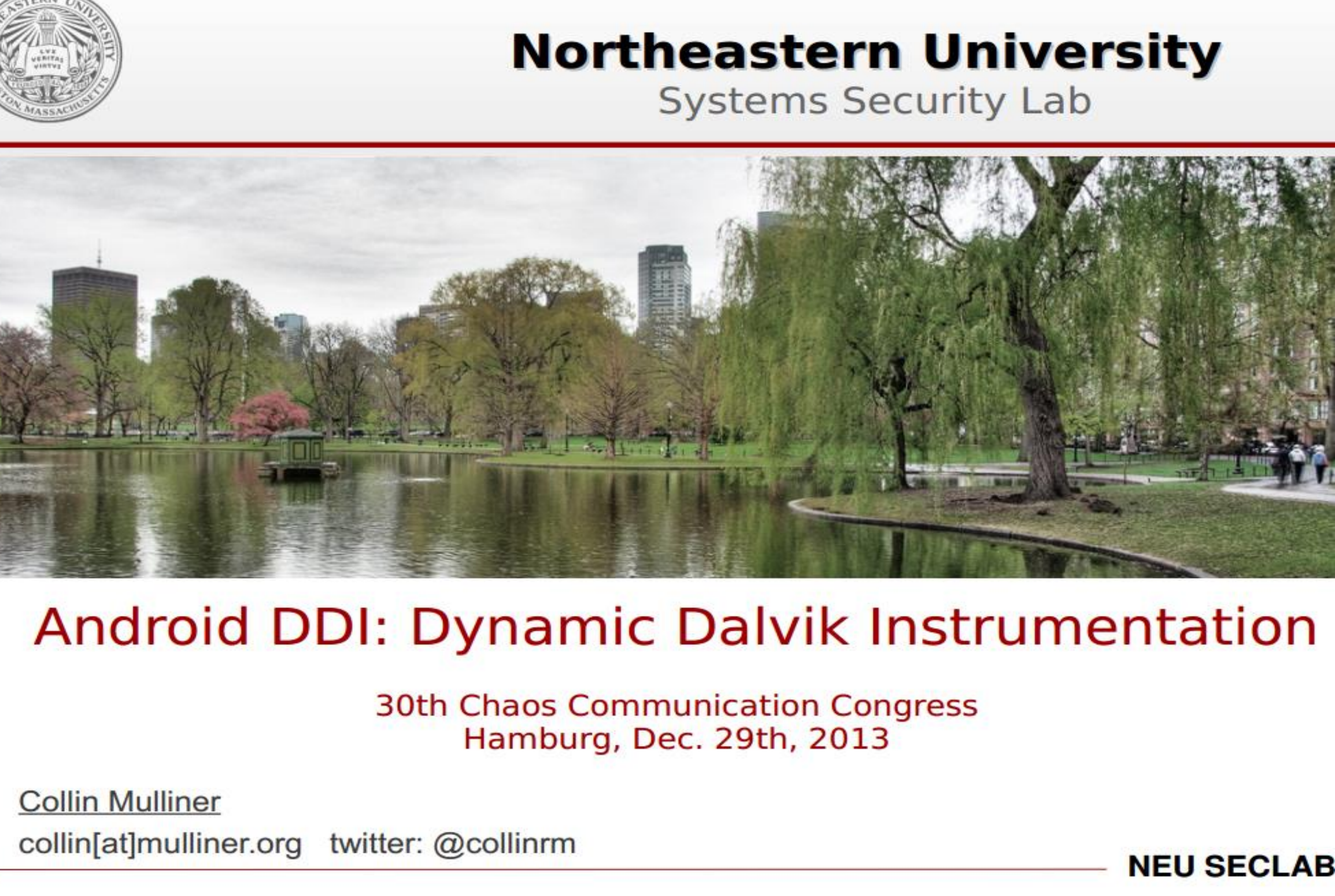
```
./vaccine.sh -i android.apk -p 8888
```

And pray to the DEMO gods ;)

CHALLENGES
AHEAD

Possibbilites

- Many apks:
  - gmail, dropbox, playstore, games...
  - Messaging, settings, browser...
- Getting Phone instance
- Using phone as framework(Quick SMS)
- Sending class 0 sms
- Extending by writting beanshell scripts



Northeastern University
Systems Security Lab

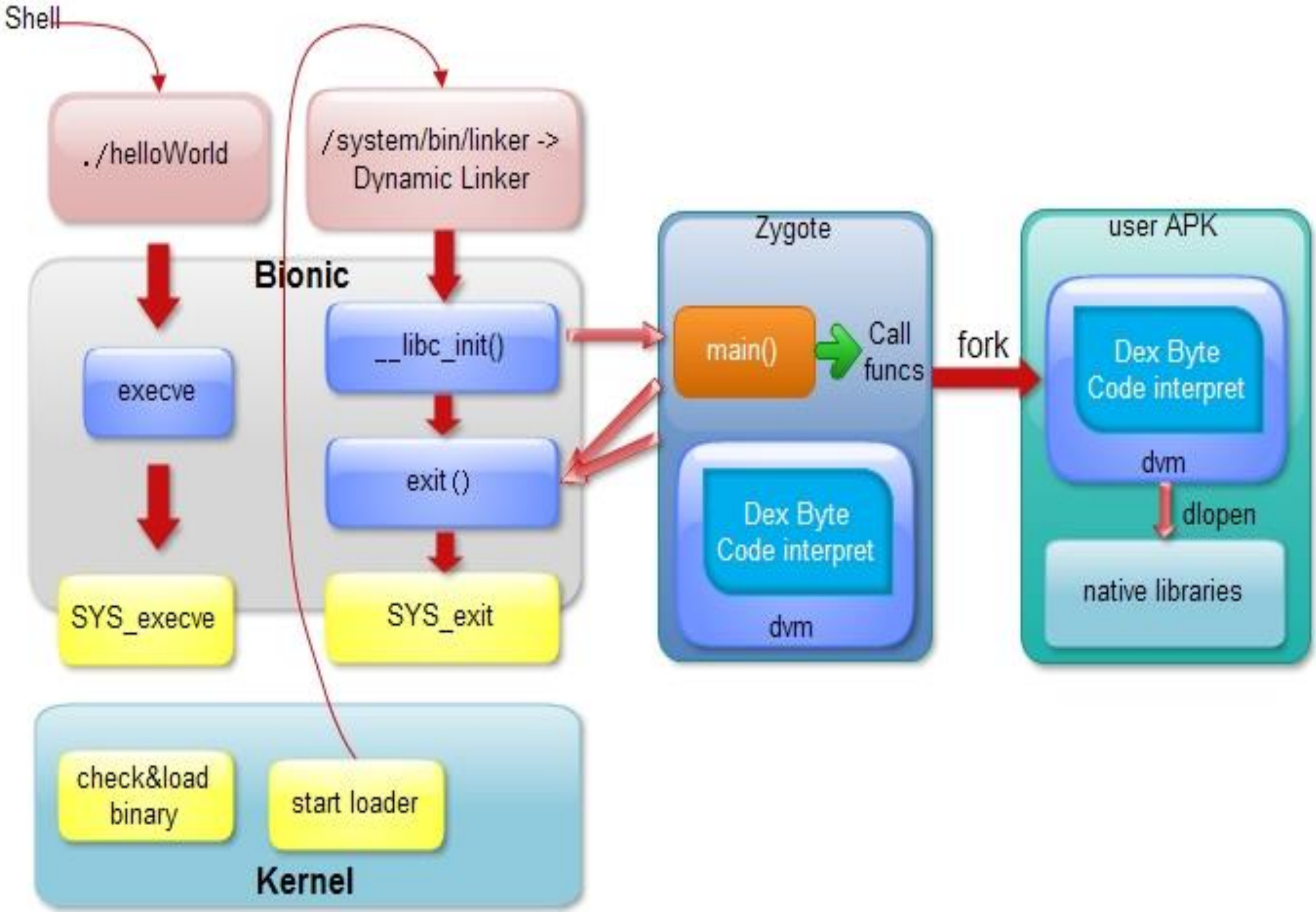
Android DDI: Dynamic Dalvik Instrumentation

30th Chaos Communication Congress
Hamburg, Dec. 29th, 2013

Collin Mulliner
collin[at]mulliner.org twitter: @collinrm

NEU SECLAB

#/viris


Shell
./helloWorld
/system/bin/linker -> Dynamic Linker
Bionic
execve
__libc_init()
exit ()
SYS_execve
SYS_exit
Kernel
check&load binary
start loader
Zygote
main()
Call funcs
Dex Byte Code interpret
dvm
fork
user APK
Dex Byte Code interpret
dvm
dlopen
native libraries

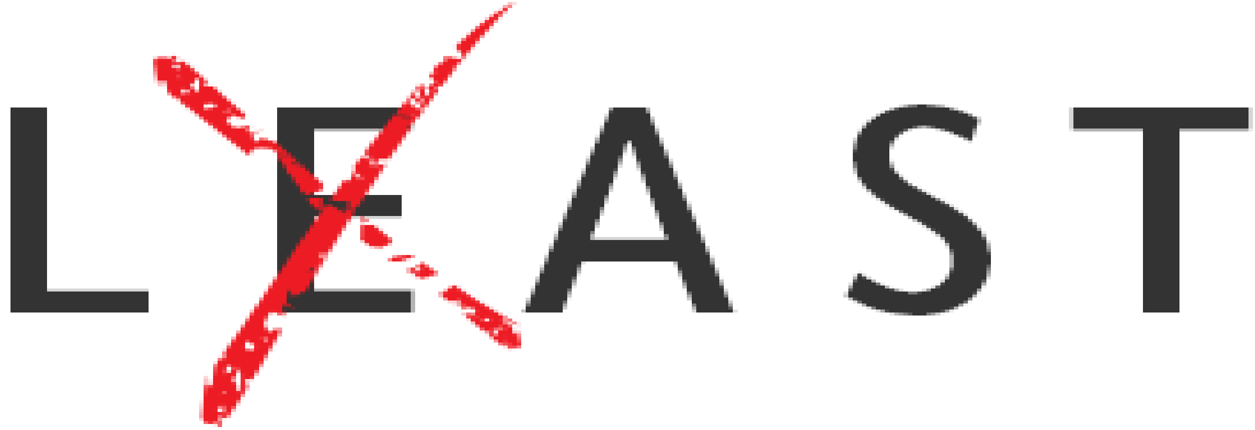
Next presentation title?

Final thoughts

- One script, one tool (never be finished)
- Help testers, researchers, (hackers, cheaters)
- Open for suggestions, improvements, comments

Tips

- Know your platform (this means read at least 1 more book different then iOS/Android in 10 minutes)
- Know how things are made off
- Know where thing are stored (save, conf, cache, logs)


L~~E~~AST

Share
ideas
Start
something
good

Questions?

www.github.com/viris

@MilanGabor

@alm8i

Thank You!!