RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: MBS-R02

How to Analyze an Android Bot

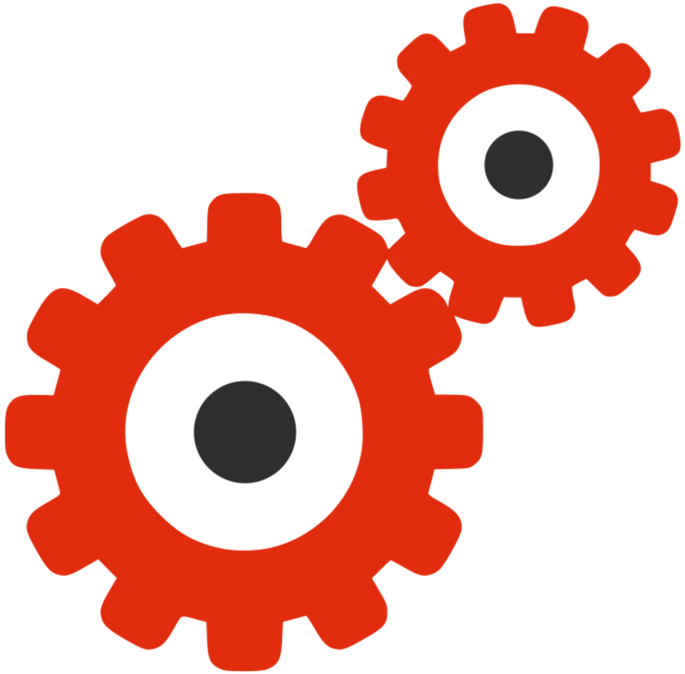
Kevin McNamee

Nokia Threat Intelligence Lab
@KevMcNamee

#RSAC

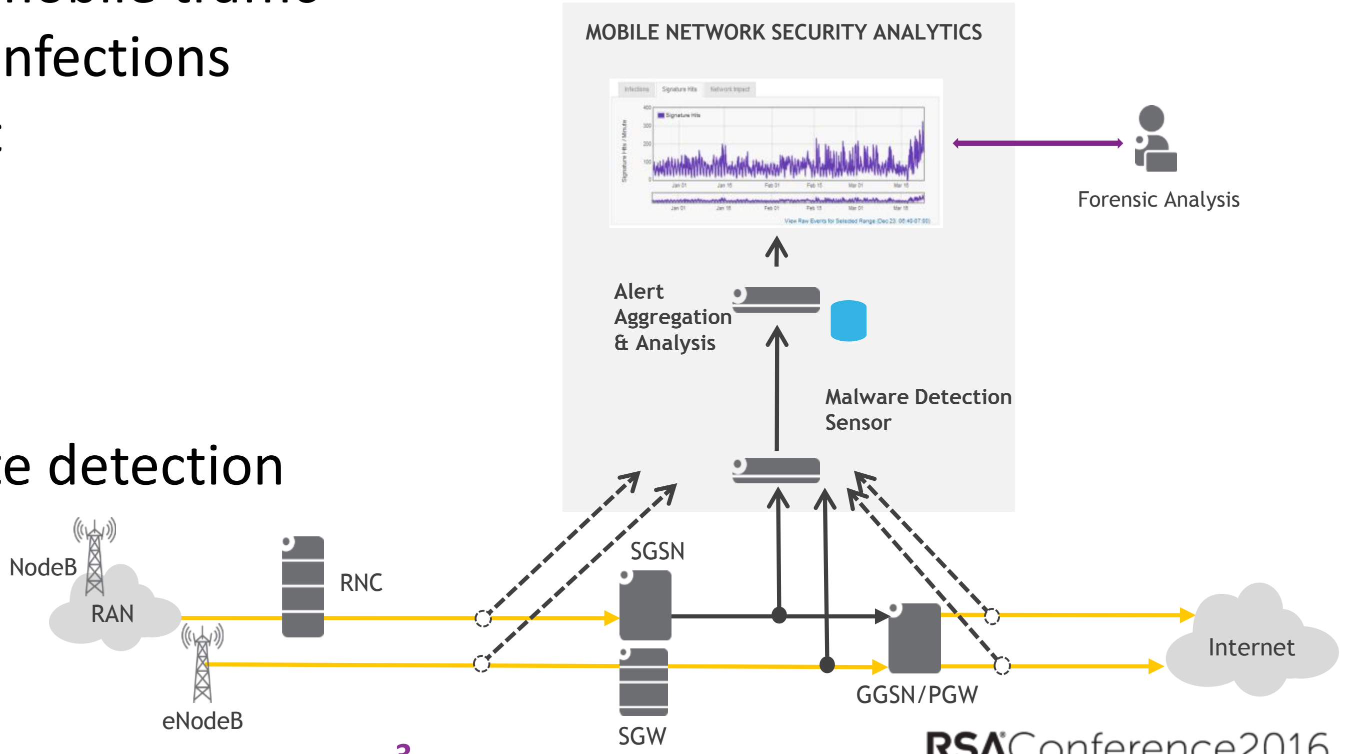
Agenda

- Introduction
- Tools
- The Lab
- Demo
- Q&A

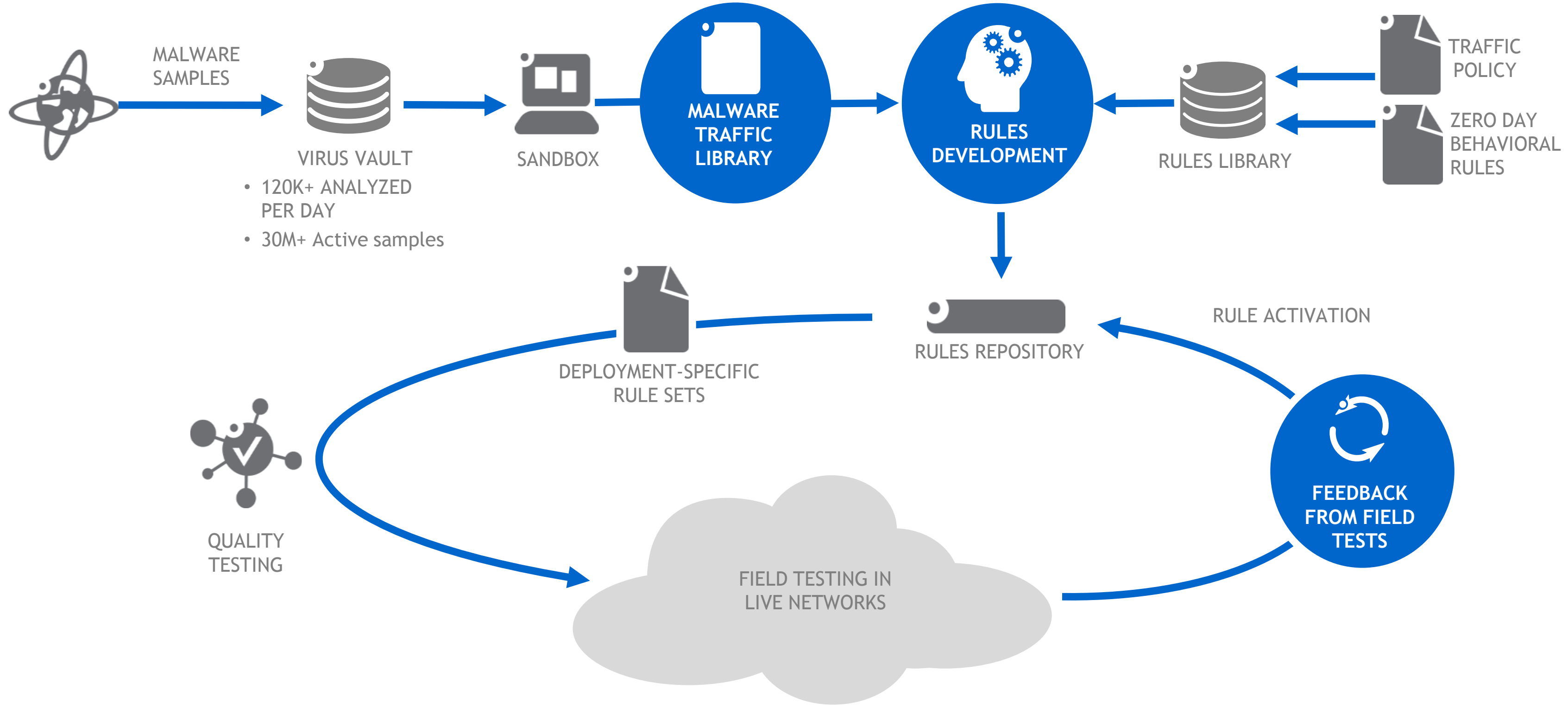


Why Analyze Android Malware

- We monitor mobile traffic for malware infections
  - Malware C&C
  - Exploits
  - DDOS
  - Hacking
- Need accurate detection rules



Developing Malware Detection Rules



Android Malware Analysis

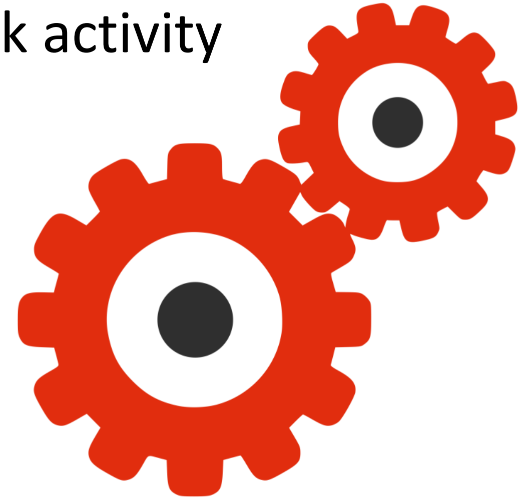
- So, we built our own Android malware analysis lab
- You will learn
  - What tools are required
  - How to set up the network environment
  - How they are used
- Analysis allows you to:
  - Know what the malware does
  - Understand its threat level
  - Detect and remediate the infection

Android App

- Contained in APK file (zip format)
- Main components include:
  - Manifest
  - Dalvik byte code (classes.dex file)
  - Resources
  - Assets
  - Libraries

Basic Analysis Process

- Explore what's in APK file
- Decompile DEX and review source
- Run app on phone or AVD & capture network activity



Tools – Android Studio

- If you are going to analyze apps you have to know a bit about how they are made…
- Also provides many of the tools needed for analysis…
  - ADB (debugging)
  - AVD (simulated phones)

Tools – Apktool

- Tool for reverse engineering Android packages (apk files)
- Extract components
  - Manifest, Resources, Libraries, Assets, Byte-code (Smali)
- Can edit and modify components
- Rebuild modified app

Tools – ADB

- Android Debug Bridge
- Comes with Android Studio
- Provides:
  - Shell access
  - Access to file system
  - Scripted remote control
  - Application Install/Uninstall

Tools – dex2jar

- Converts Dalvik byte code to Java byte code
- First step in de-compiling an Android app.

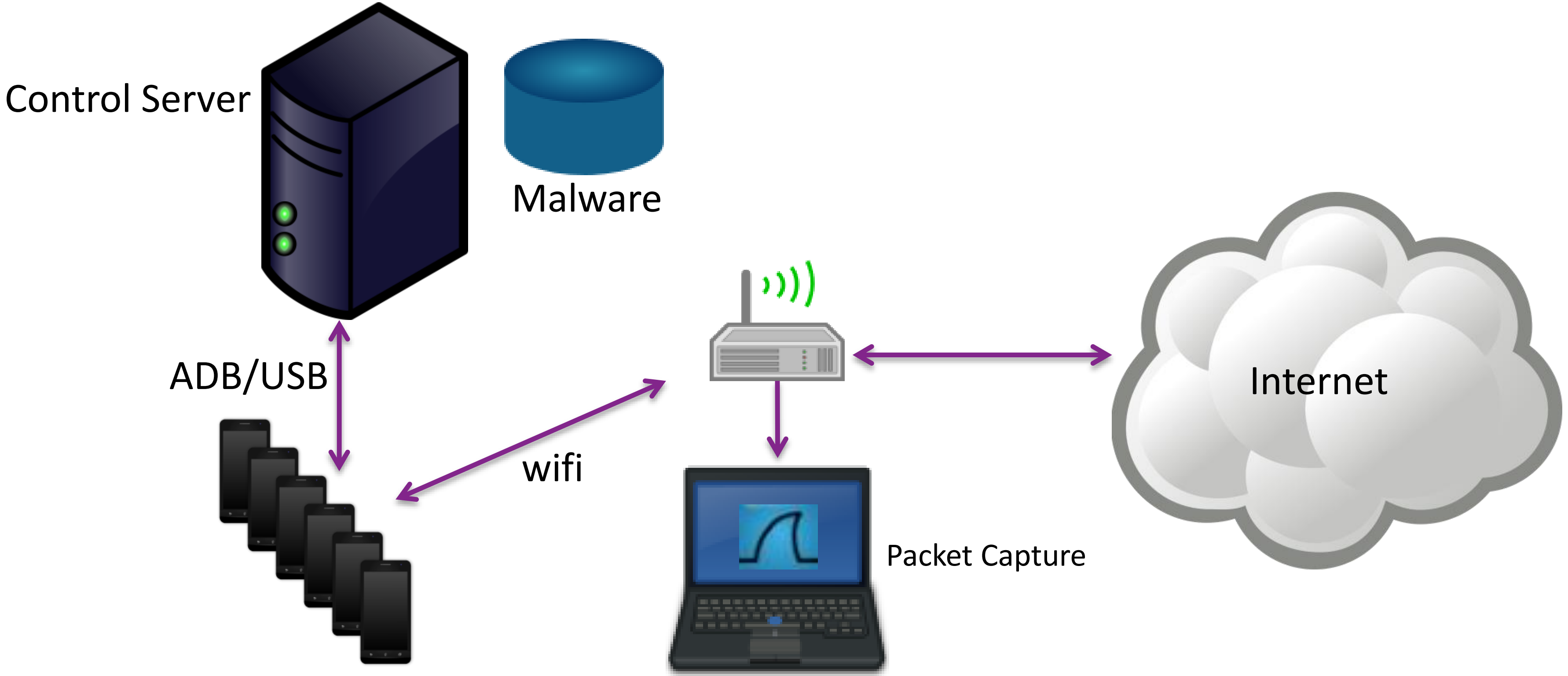
Tools – Java Decompiler

- Converts Java byte code to source code.
- Doesn't always work ☹
- Options include:
  - JD-GUI
  - Luyten (Procyon)

Tools – WireShark

- Capture and network traffic
- Analyze network traffic
- Help develop detection rules

The Lab

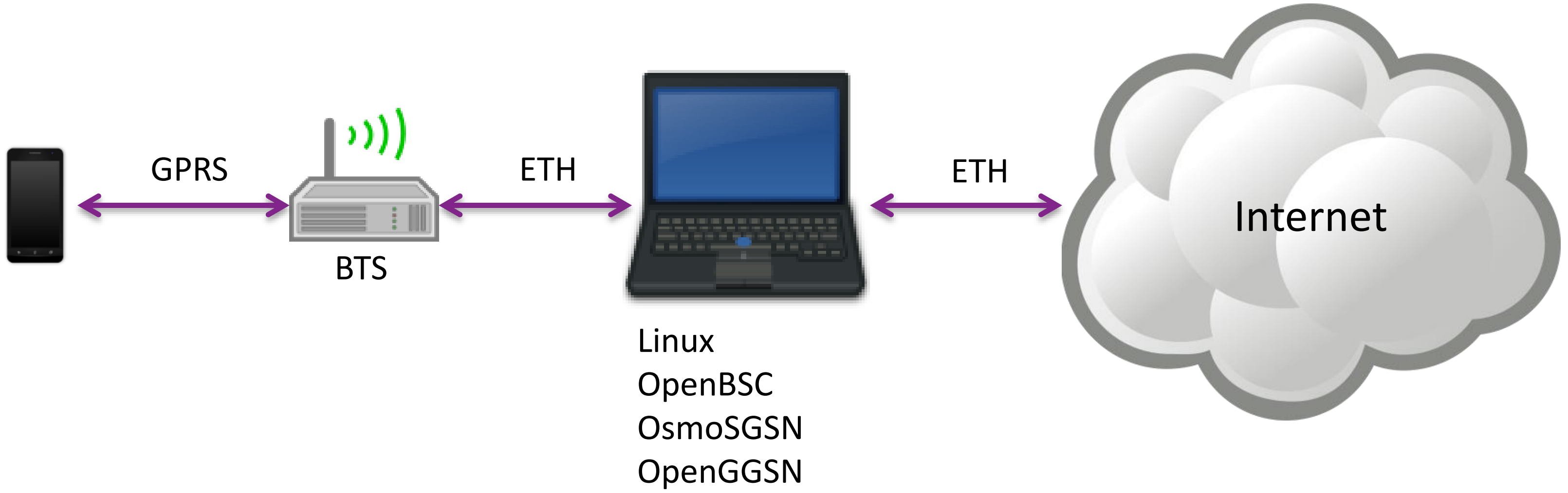

Control Server
Malware
ADB/USB
wifi
Internet
Packet Capture

Malware - DANGER!!
Analysis-1
ZOE
D2
D1
John Morris
Caution:
Malware
Computers, Smart phones, Networks, and Removable media in this area contain malicious software which pose a significant security threat to other devices.
D1-4

BOB
DAN
EVA
FAY
GUS
HAL
IVY
JOE
B4
DANGER - Malware Sandboxes
OREO
DANGER - Malware Sandboxes
SOPHOS

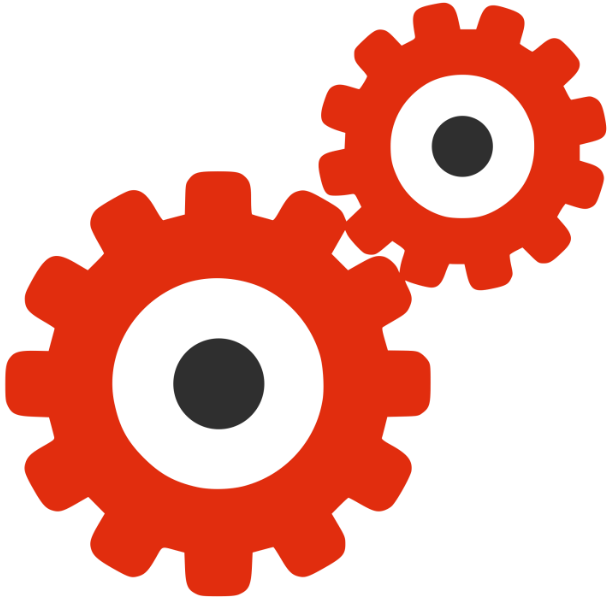
Using a Real Mobile Network

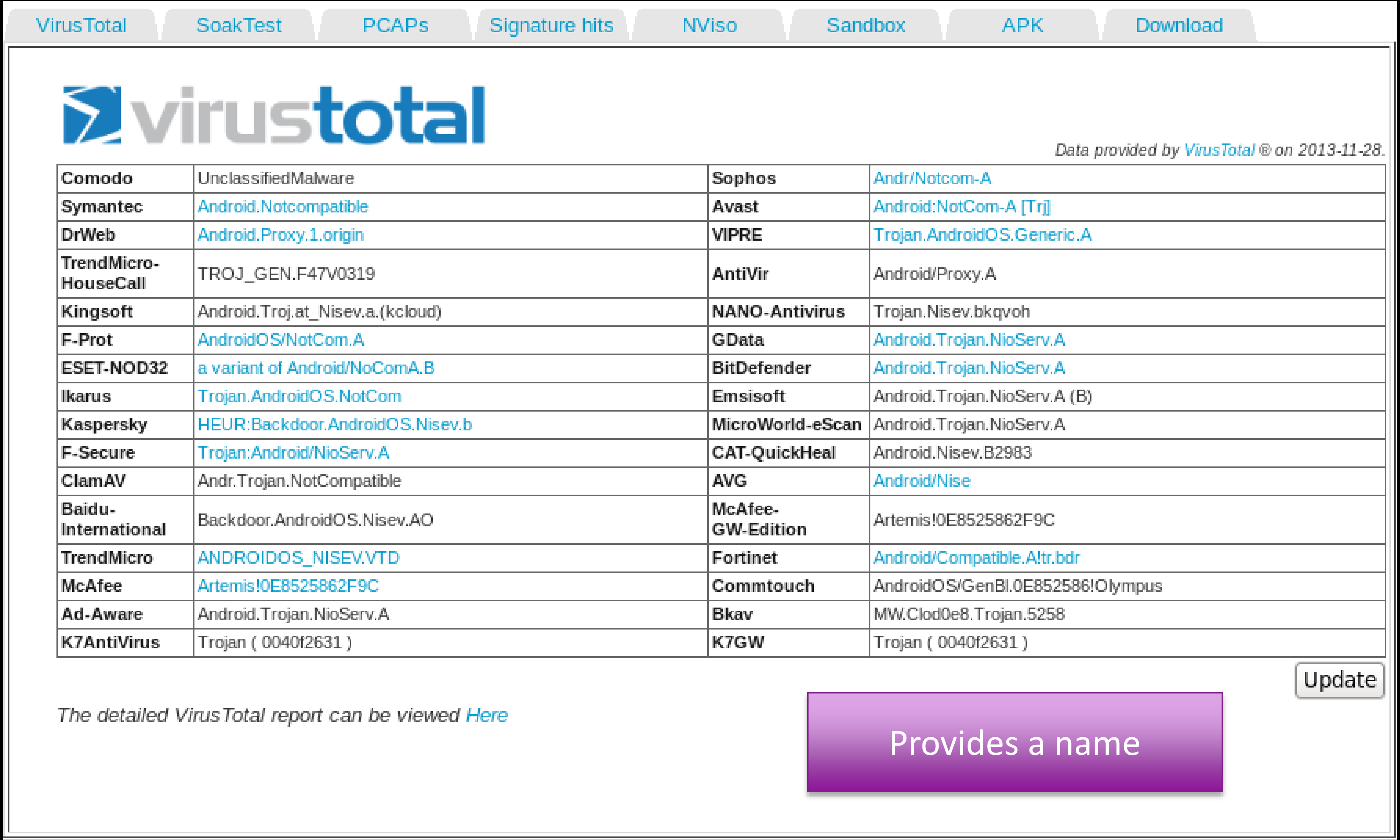
- Some malware may only function on a real mobile network
- You can build your own mobile network.



Automation

- We have automated the analysis process using:
  - Web based user interface
  - Real phones and AVDs
  - Malware database
  - APKtool/Dex2Jar/GD-GUI
  - ADB scripting
  - Monkey Script
  - WireShark
  - Interface to Virus Total





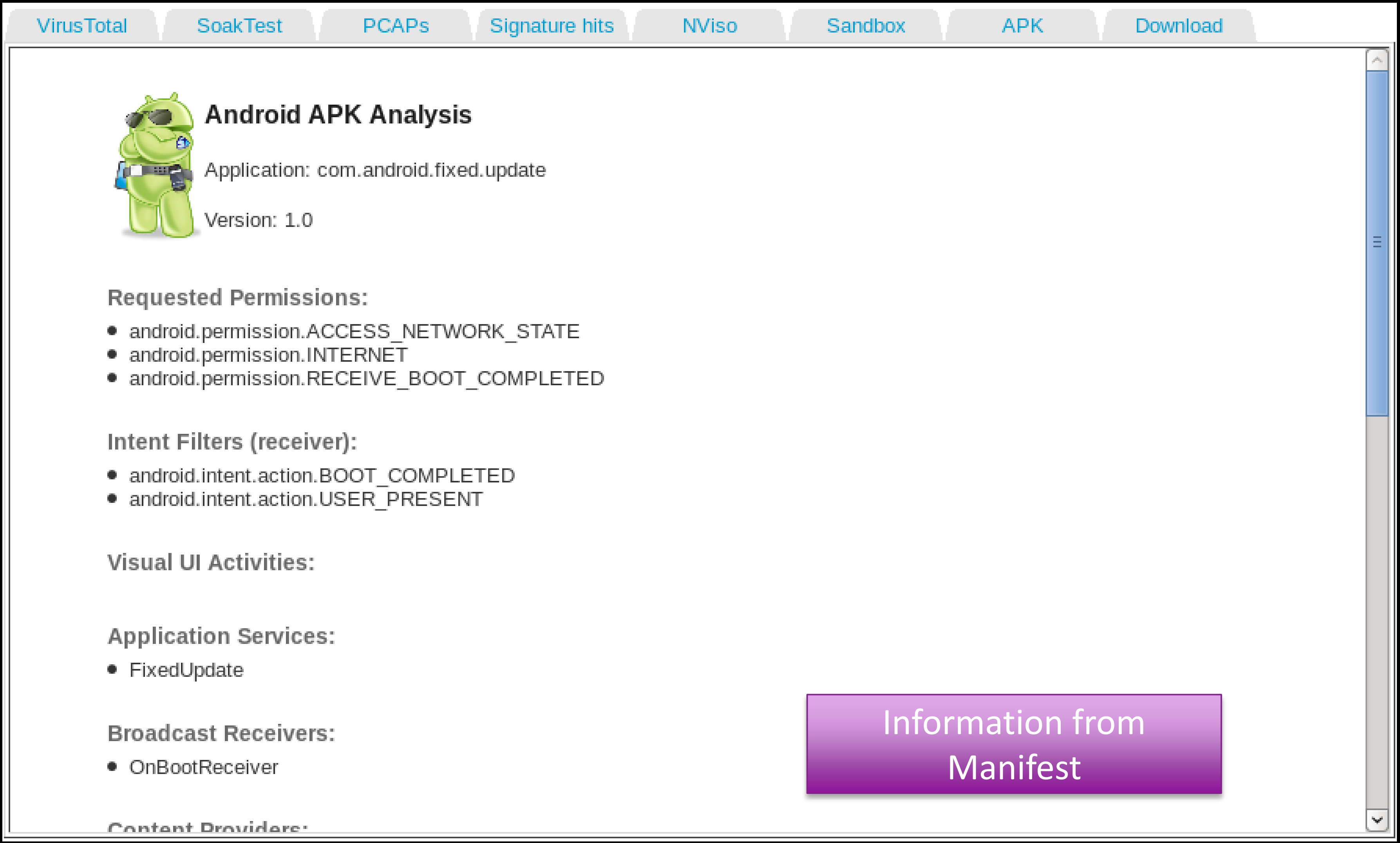
Data provided by VirusTotal ® on 2013-11-28.

Comodo	UnclassifiedMalware	**Sophos**	Andr/Notcom-A
Symantec	Android.Notcompatible	**Avast**	Android:NotCom-A [Trj]
DrWeb	Android.Proxy.1.origin	**VIPRE**	Trojan.AndroidOS.Generic.A
TrendMicro-HouseCall	TROJ_GEN.F47V0319	**AntiVir**	Android/Proxy.A
Kingsoft	Android.Troj.at_Nisev.a.(kcloud)	**NANO-Antivirus**	Trojan.Nisev.bkqvoh
F-Prot	AndroidOS/NotCom.A	**GData**	Android.Trojan.NioServ.A
ESET-NOD32	a variant of Android/NoComA.B	**BitDefender**	Android.Trojan.NioServ.A
Ikarus	Trojan.AndroidOS.NotCom	**Emsisoft**	Android.Trojan.NioServ.A (B)
Kaspersky	HEUR:Backdoor.AndroidOS.Nisev.b	**MicroWorld-eScan**	Android.Trojan.NioServ.A
F-Secure	Trojan:Android/NioServ.A	**CAT-QuickHeal**	Android.Nisev.B2983
ClamAV	Andr.Trojan.NotCompatible	**AVG**	Android/Nise
Baidu-International	Backdoor.AndroidOS.Nisev.AO	**McAfee-GW-Edition**	Artemis!0E8525862F9C
TrendMicro	ANDROIDOS_NISEV.VTD	**Fortinet**	Android/Compatible.A!tr.bdr
McAfee	Artemis!0E8525862F9C	**Commtouch**	AndroidOS/GenBl.0E852586!Olympus
Ad-Aware	Android.Trojan.NioServ.A	**Bkav**	MW.Clod0e8.Trojan.5258
K7AntiVirus	Trojan (0040f2631)	**K7GW**	Trojan (0040f2631)

Update

The detailed VirusTotal report can be viewed Here

Provides a name



VirusTotal | SoakTest | PCAPs | Signature hits | NViso | Sandbox | APK | Download

Android APK Analysis

Application: com.android.fixed.update

Version: 1.0

Requested Permissions:

- android.permission.ACCESS_NETWORK_STATE
- android.permission.INTERNET
- android.permission.RECEIVE_BOOT_COMPLETED

Intent Filters (receiver):

- android.intent.action.BOOT_COMPLETED
- android.intent.action.USER_PRESENT

Visual UI Activities:

Application Services:

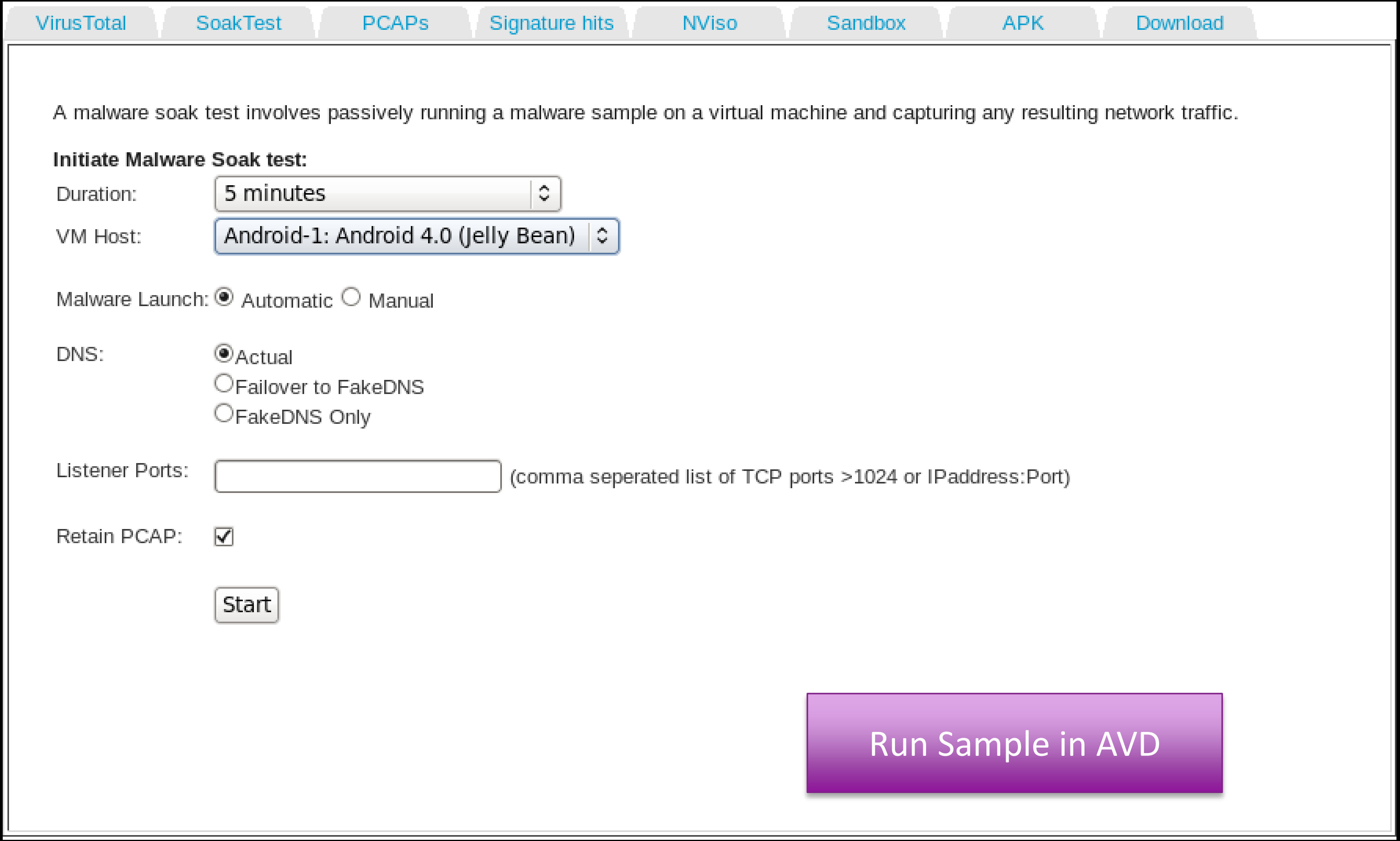
- FixedUpdate

Broadcast Receivers:

- OnBootReceiver

Content Providers:

Information from Manifest



A malware soak test involves passively running a malware sample on a virtual machine and capturing any resulting network traffic.

Initiate Malware Soak test:

Duration: 5 minutes

VM Host: Android-1: Android 4.0 (Jelly Bean)

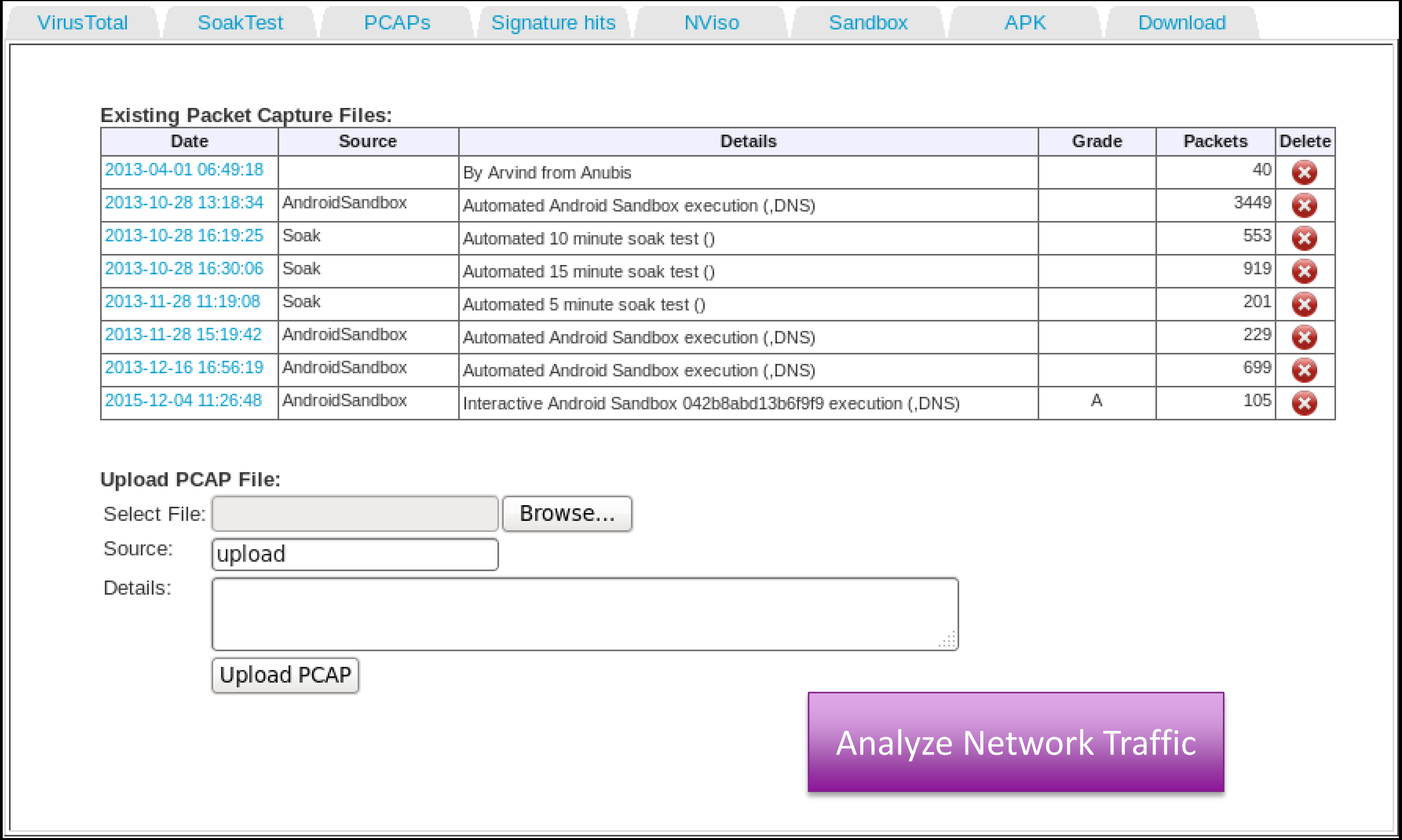
Malware Launch: [✓ Automatic] Manual

DNS: [✓ Actual] Failover to FakeDNS FakeDNS Only

Listener Ports: (comma seperated list of TCP ports >1024 or IPaddress:Port)

Retain PCAP: ☑

Run Sample in AVD



VirusTotal | SoakTest | PCAPs | Signature hits | NViso | Sandbox | APK | Download

Existing Packet Capture Files:

Date	Source	Details	Grade	Packets	Delete
2013-04-01 06:49:18		By Arvind from Anubis		40	✖
2013-10-28 13:18:34	AndroidSandbox	Automated Android Sandbox execution (,DNS)		3449	✖
2013-10-28 16:19:25	Soak	Automated 10 minute soak test ()		553	✖
2013-10-28 16:30:06	Soak	Automated 15 minute soak test ()		919	✖
2013-11-28 11:19:08	Soak	Automated 5 minute soak test ()		201	✖
2013-11-28 15:19:42	AndroidSandbox	Automated Android Sandbox execution (,DNS)		229	✖
2013-12-16 16:56:19	AndroidSandbox	Automated Android Sandbox execution (,DNS)		699	✖
2015-12-04 11:26:48	AndroidSandbox	Interactive Android Sandbox 042b8abd13b6f9f9 execution (,DNS)	A	105	✖

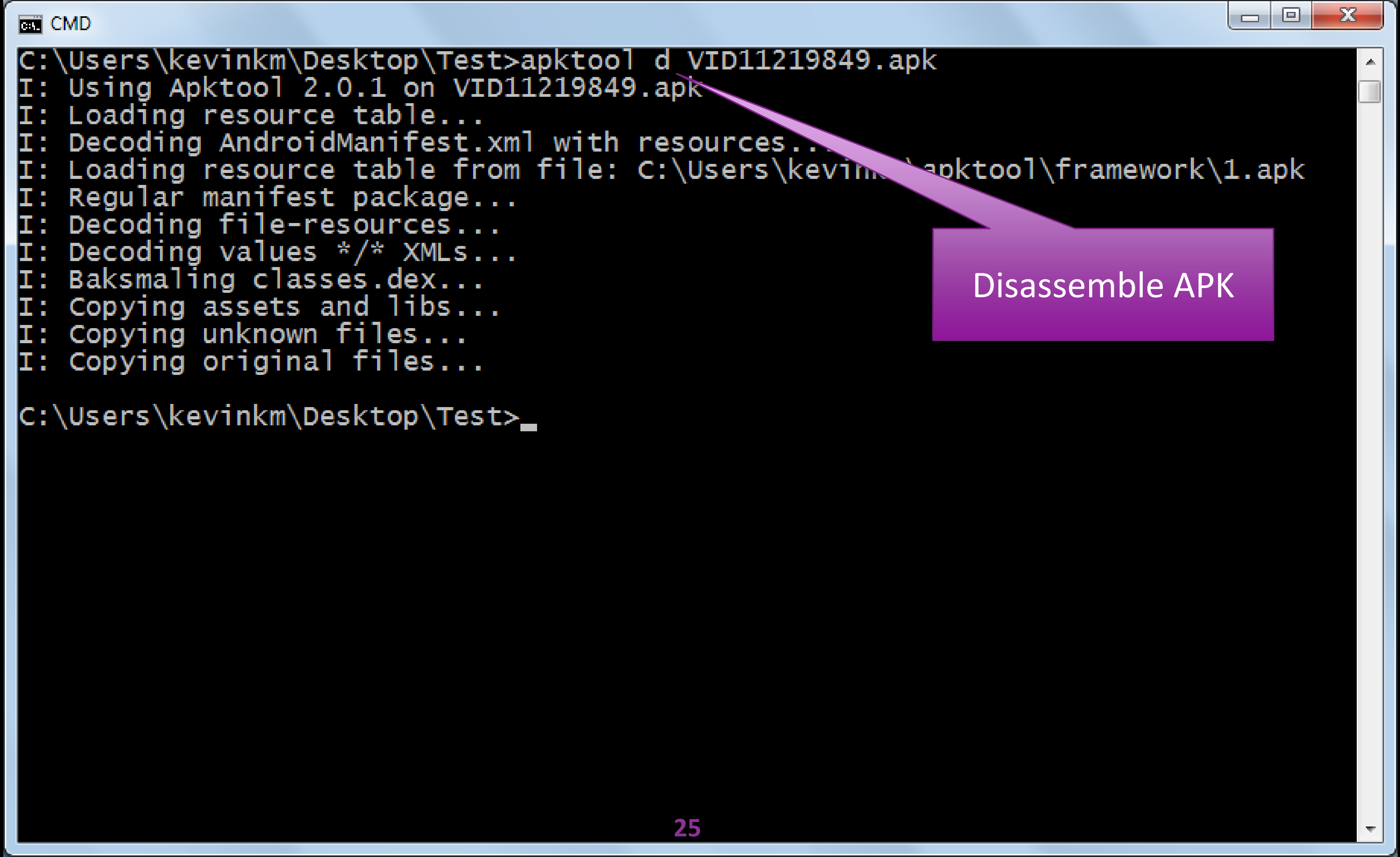
Upload PCAP File:

Select File:	Browse...
Source:	upload
Details:	

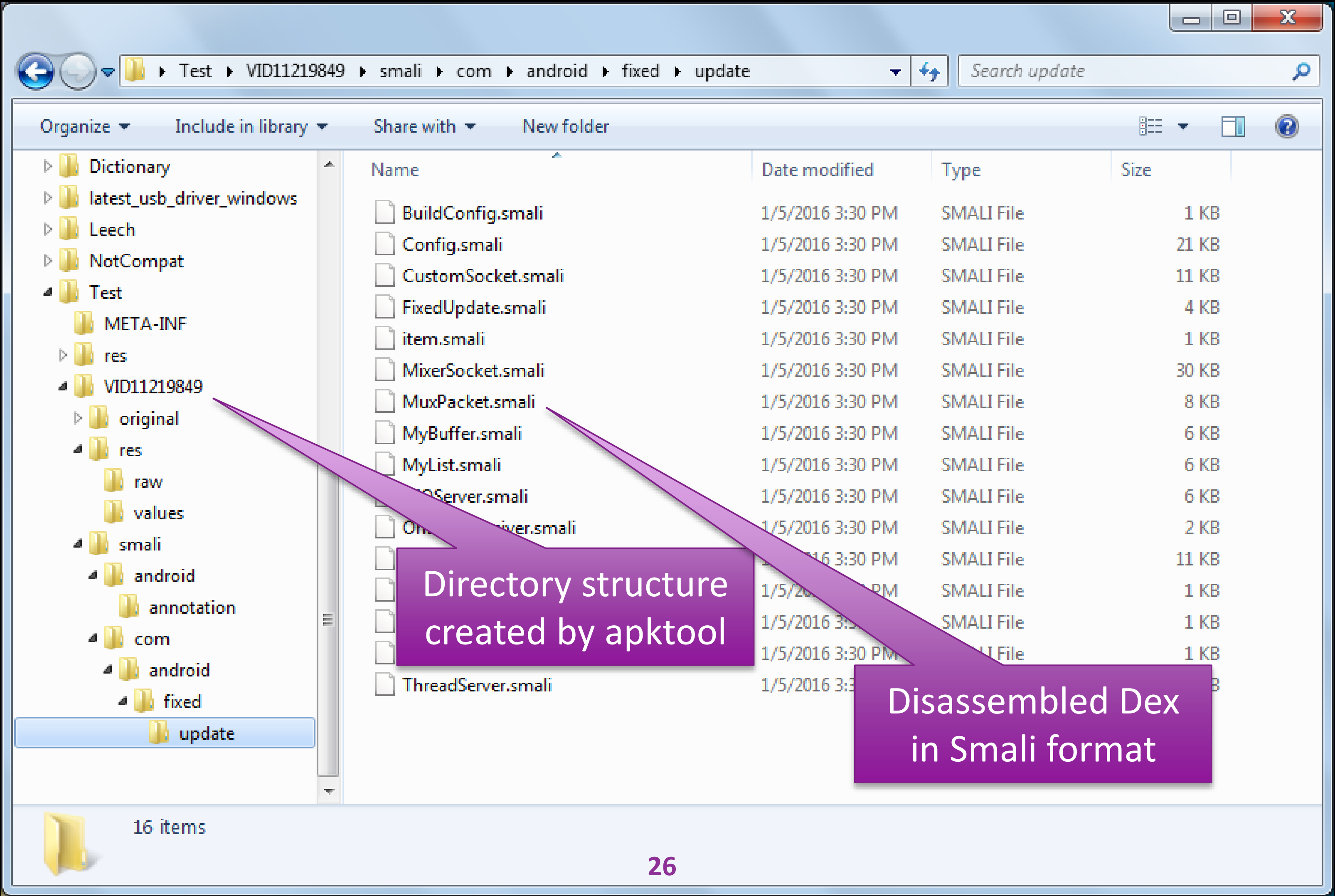
Upload PCAP

Analyze Network Traffic

Manual Demo – NotCompatible Proxy Bot



```
C:\Users\kevinkm\Desktop\Test>apktool d VID11219849.apk
I: Using Apktool 2.0.1 on VID11219849.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: C:\Users\kevin[illegible]apktool\framework\1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...

C:\Users\kevinkm\Desktop\Test>_
```



Test ▸ VID11219849 ▸ smali ▸ com ▸ android ▸ fixed ▸ update

Search update

Organize ▾ Include in library ▾ Share with ▾ New folder

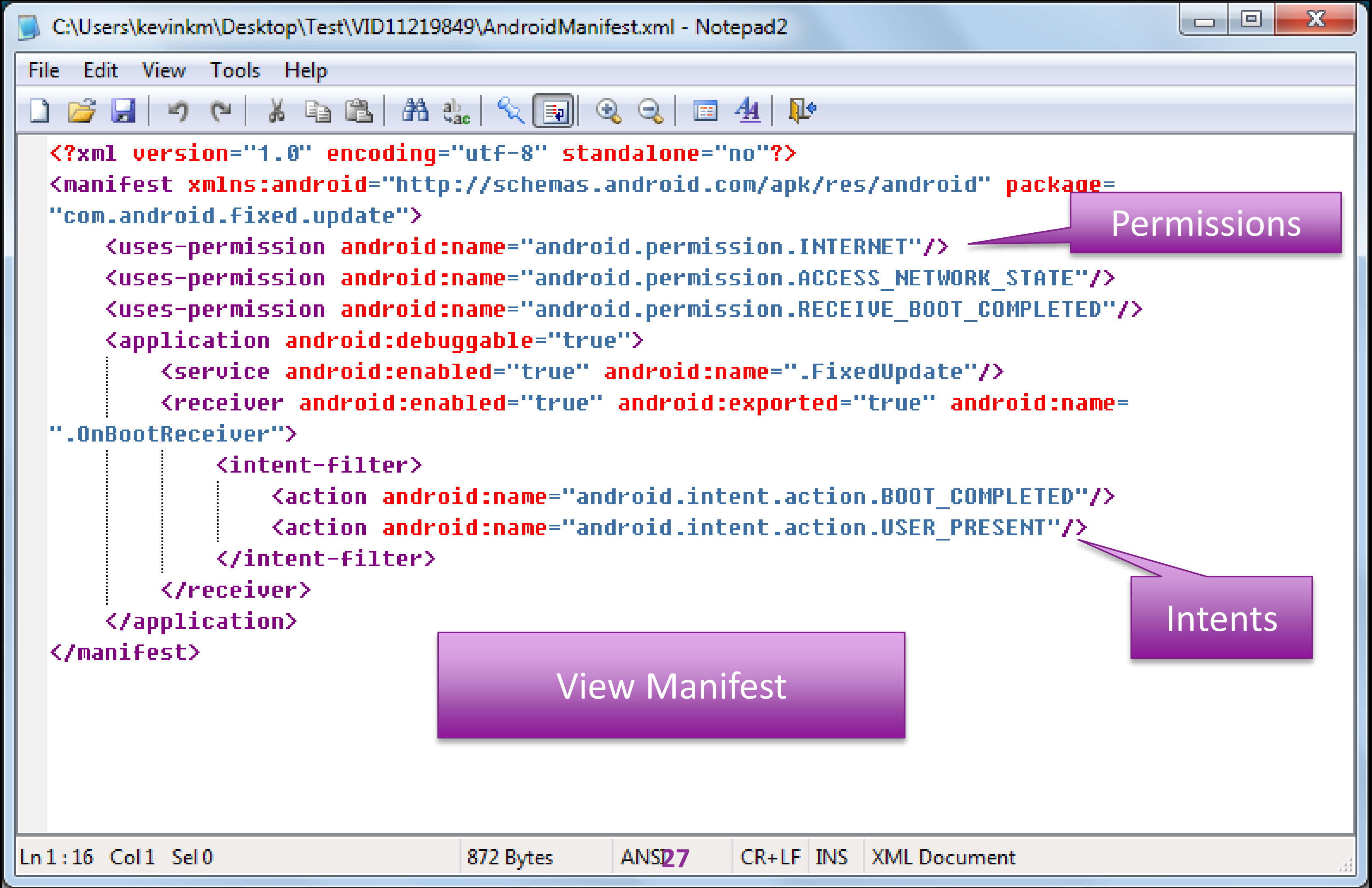
- Dictionary
- latest_usb_driver_windows
- Leech
- NotCompat
- Test
  - META-INF
  - res
  - VID11219849
    - original
    - res
      - raw
      - values
    - smali
      - android
        - annotation
      - com
        - android
          - fixed
            - update

Name	Date modified	Type	Size
BuildConfig.smali	1/5/2016 3:30 PM	SMALI File	1 KB
Config.smali	1/5/2016 3:30 PM	SMALI File	21 KB
CustomSocket.smali	1/5/2016 3:30 PM	SMALI File	11 KB
FixedUpdate.smali	1/5/2016 3:30 PM	SMALI File	4 KB
item.smali	1/5/2016 3:30 PM	SMALI File	1 KB
MixerSocket.smali	1/5/2016 3:30 PM	SMALI File	30 KB
MuxPacket.smali	1/5/2016 3:30 PM	SMALI File	8 KB
MyBuffer.smali	1/5/2016 3:30 PM	SMALI File	6 KB
MyList.smali	1/5/2016 3:30 PM	SMALI File	6 KB
OServer.smali	1/5/2016 3:30 PM	SMALI File	6 KB
On iver.smali	1/5/2016 3:30 PM	SMALI File	2 KB
[illegible]	16 3:30 PM	SMALI File	11 KB
[illegible]	1/5/20 PM	SMALI File	1 KB
[illegible]	1/5/2016 3:	SMALI File	1 KB
[illegible]	1/5/2016 3:30 PM	I File	1 KB
ThreadServer.smali	1/5/2016 3:3	[illegible]	B

16 items

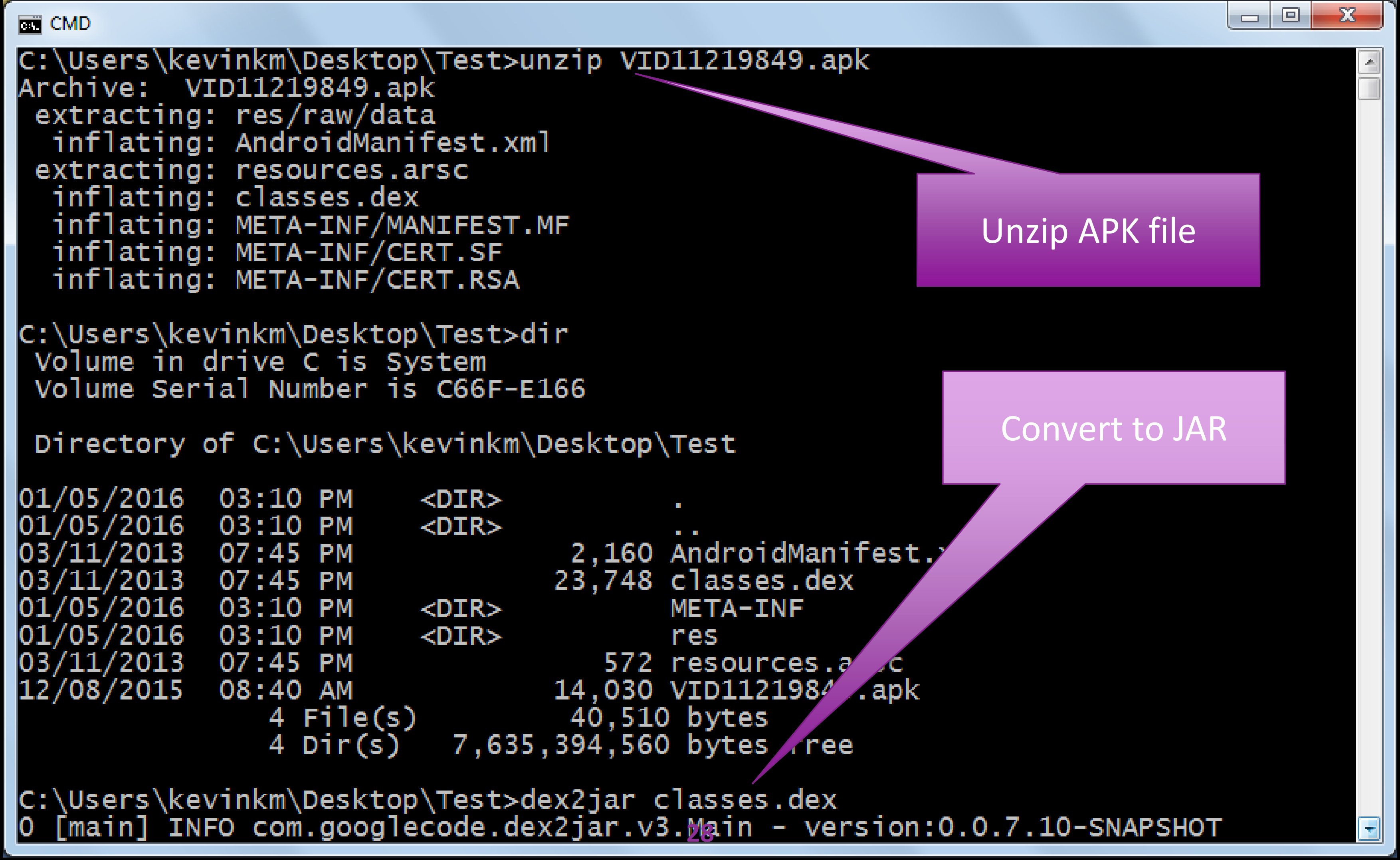
Directory structure created by apktool

Disassembled Dex in Smali format

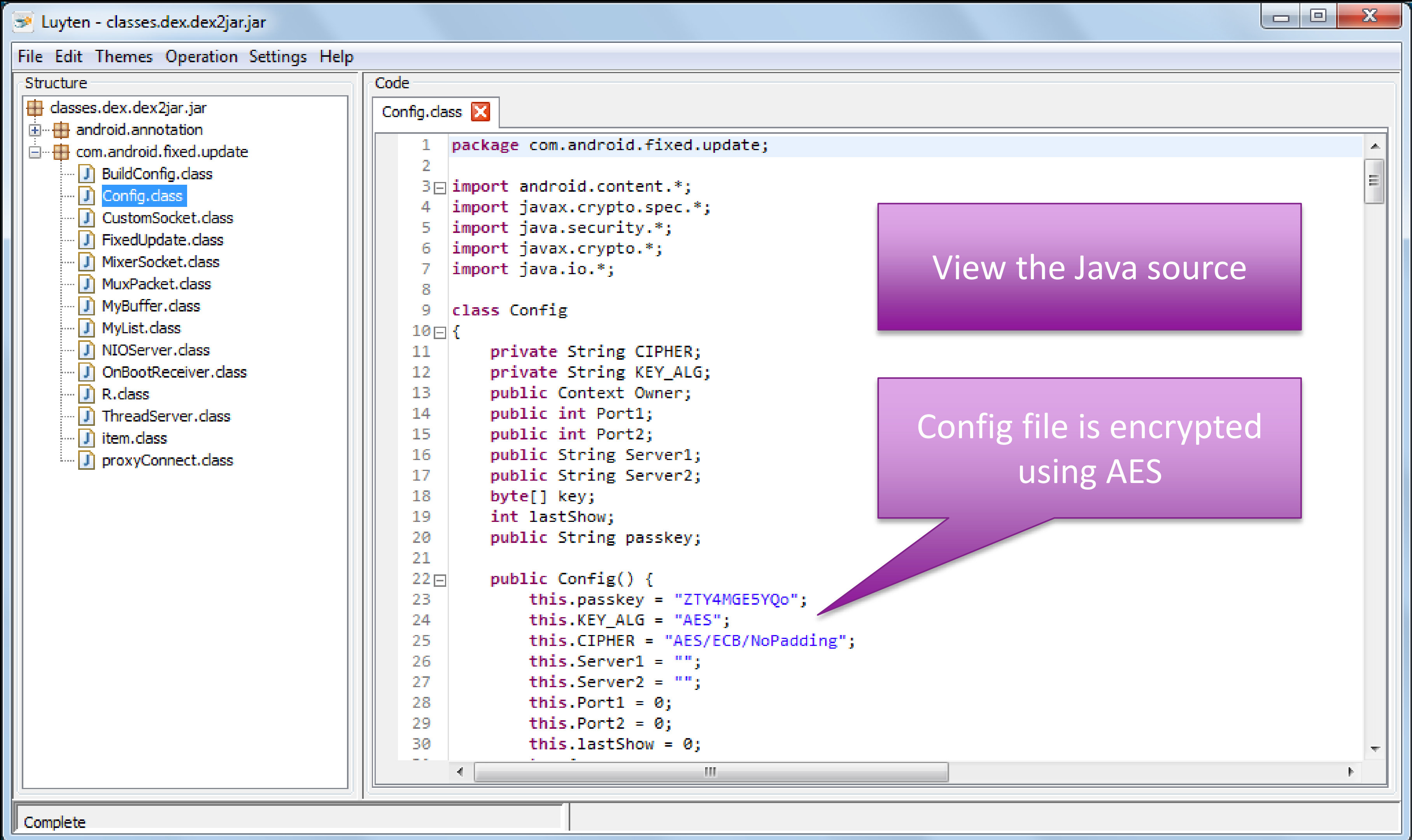

C:\Users\kevinkm\Desktop\Test\VID11219849\AndroidManifest.xml - Notepad2
File Edit View Tools Help

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package=
"com.android.fixed.update">
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <application android:debuggable="true">
        <service android:enabled="true" android:name=".FixedUpdate"/>
        <receiver android:enabled="true" android:exported="true" android:name=
".OnBootReceiver">
            <intent-filter>
                <action android:name="android.intent.action.BOOT_COMPLETED"/>
                <action android:name="android.intent.action.USER_PRESENT"/>
            </intent-filter>
        </receiver>
    </application>
</manifest>
```

Permissions
Intents
View Manifest
Ln 1 : 16 Col 1 Sel 0
872 Bytes
ANSI
CR+LF INS XML Document



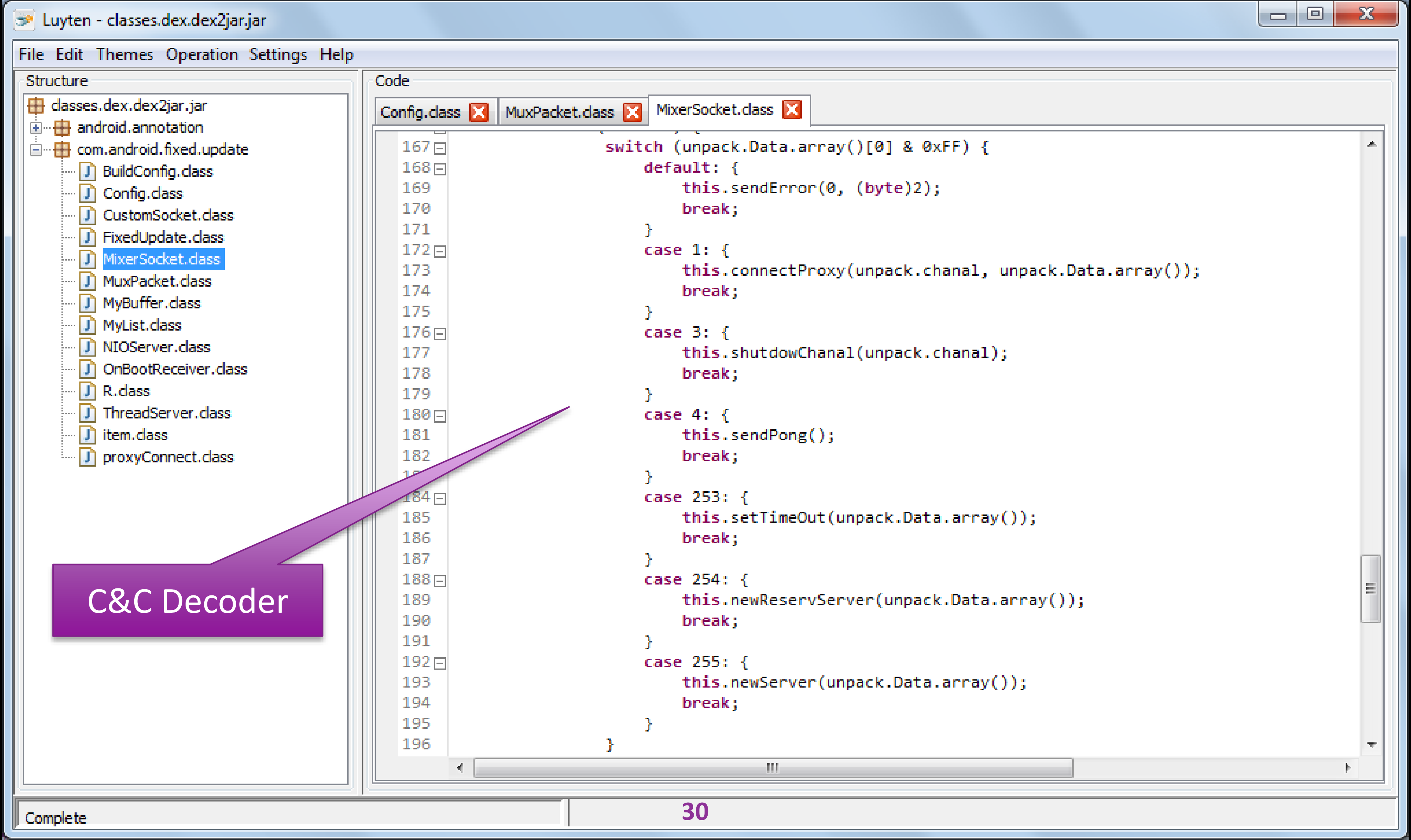
```
C:\Users\kevinkm\Desktop\Test>unzip VID11219849.apk
Archive:  VID11219849.apk
 extracting: res/raw/data
  inflating: AndroidManifest.xml
 extracting: resources.arsc
  inflating: classes.dex
  inflating: META-INF/MANIFEST.MF
  inflating: META-INF/CERT.SF
  inflating: META-INF/CERT.RSA

C:\Users\kevinkm\Desktop\Test>dir
 Volume in drive C is System
 Volume Serial Number is C66F-E166

 Directory of C:\Users\kevinkm\Desktop\Test

01/05/2016  03:10 PM    <DIR>          .
01/05/2016  03:10 PM    <DIR>          ..
03/11/2013  07:45 PM             2,160 AndroidManifest.x
03/11/2013  07:45 PM            23,748 classes.dex
01/05/2016  03:10 PM    <DIR>          META-INF
01/05/2016  03:10 PM    <DIR>          res
03/11/2013  07:45 PM               572 resources.a  c
12/08/2015  08:40 AM            14,030 VID1121984 .apk
               4 File(s)         40,510 bytes
               4 Dir(s)   7,635,394,560 bytes  ree

C:\Users\kevinkm\Desktop\Test>dex2jar classes.dex
0 [main] INFO com.googlecode.dex2jar.v3.Main - version:0.0.7.10-SNAPSHOT
```



```
package com.android.fixed.update;

import android.content.*;
import javax.crypto.spec.*;
import java.security.*;
import javax.crypto.*;
import java.io.*;

class Config
{
    private String CIPHER;
    private String KEY_ALG;
    public Context Owner;
    public int Port1;
    public int Port2;
    public String Server1;
    public String Server2;
    byte[] key;
    int lastShow;
    public String passkey;

    public Config() {
        this.passkey = "ZTY4MGE5YQo";
        this.KEY_ALG = "AES";
        this.CIPHER = "AES/ECB/NoPadding";
        this.Server1 = "";
        this.Server2 = "";
        this.Port1 = 0;
        this.Port2 = 0;
        this.lastShow = 0;
```

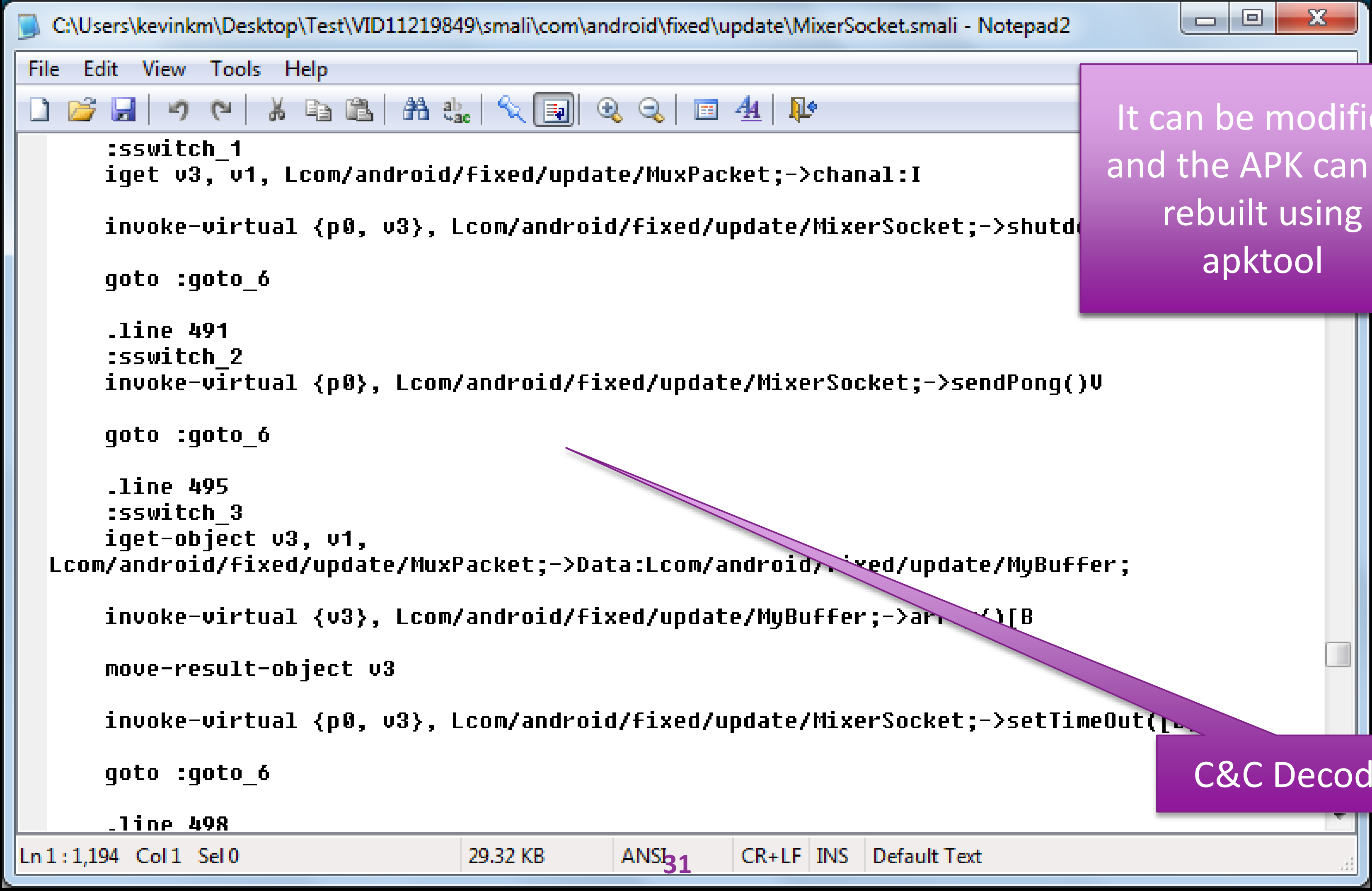
View the Java source

Config file is encrypted using AES



```
        switch (unpack.Data.array()[0] & 0xFF) {
            default: {
                this.sendError(0, (byte)2);
                break;
            }
            case 1: {
                this.connectProxy(unpack.chanal, unpack.Data.array());
                break;
            }
            case 3: {
                this.shutdowChanal(unpack.chanal);
                break;
            }
            case 4: {
                this.sendPong();
                break;
            }
            case 253: {
                this.setTimeOut(unpack.Data.array());
                break;
            }
            case 254: {
                this.newReservServer(unpack.Data.array());
                break;
            }
            case 255: {
                this.newServer(unpack.Data.array());
                break;
            }
        }
```

C&C Decoder

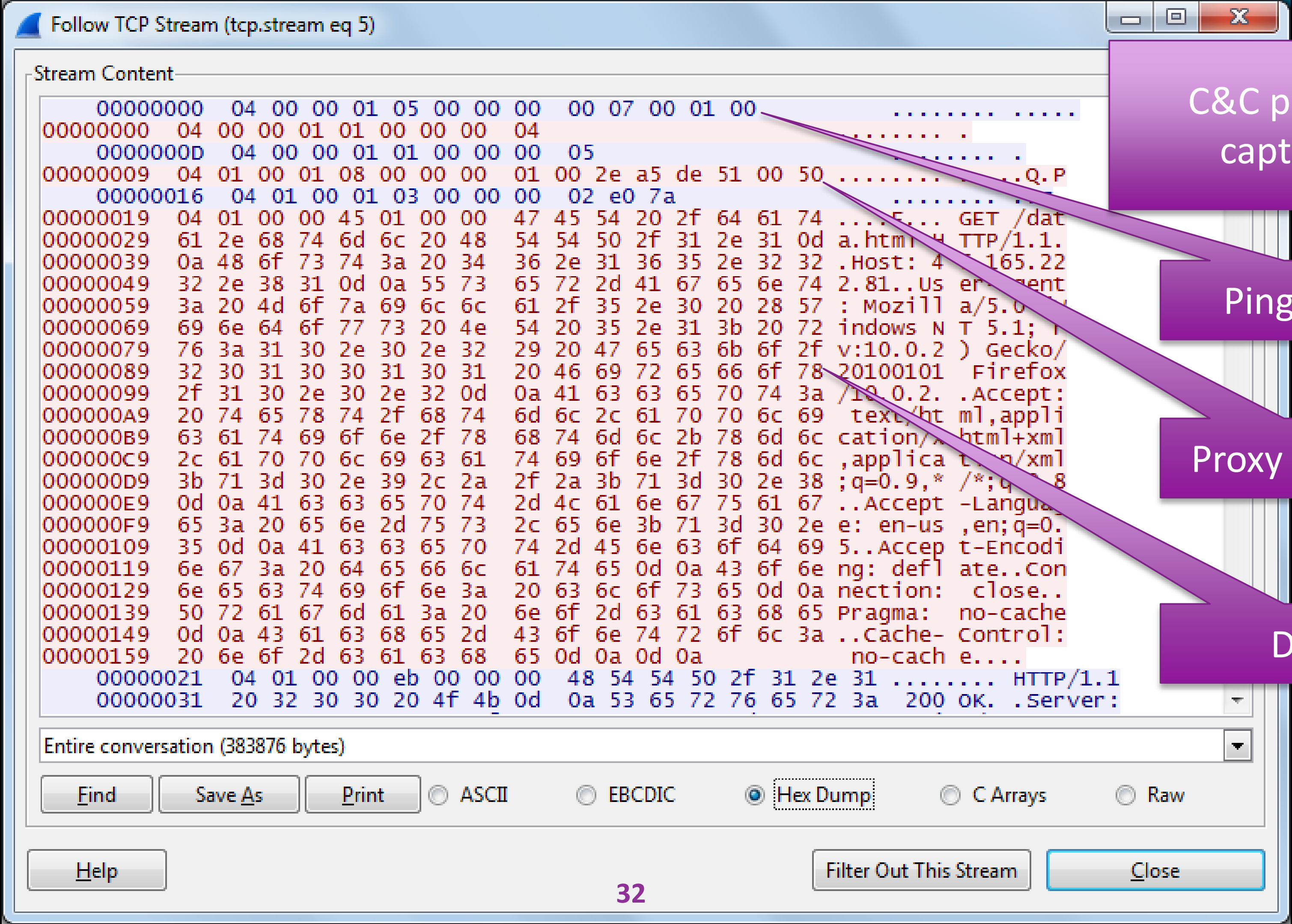

C:\Users\kevinkm\Desktop\Test\VID11219849\smali\com\android\fixed\update\MixerSocket.smali - Notepad2
File Edit View Tools Help

```
    :sswitch_1
    iget v3, v1, Lcom/android/fixed/update/MuxPacket;->chanal:I

    invoke-virtual {p0, v3}, Lcom/android/fixed/update/MixerSocket;->shutd

    goto :goto_6

    .line 491
    :sswitch_2
    invoke-virtual {p0}, Lcom/android/fixed/update/MixerSocket;->sendPong()V

    goto :goto_6

    .line 495
    :sswitch_3
    iget-object v3, v1,
Lcom/android/fixed/update/MuxPacket;->Data:Lcom/android/fixed/update/MyBuffer;

    invoke-virtual {v3}, Lcom/android/fixed/update/MyBuffer;->ar    ()[B

    move-result-object v3

    invoke-virtual {p0, v3}, Lcom/android/fixed/update/MixerSocket;->setTimeOut([

    goto :goto_6

    .line 498
```

Ln 1 : 1,194   Col 1   Sel 0   29.32 KB   ANSI   CR+LF   INS   Default Text

It can be modified and the APK can be rebuilt using apktool

C&C Decoder



```
    00000000  04 00 00 01 05 00 00 00  00 07 00 01 00          ........ .....
00000000  04 00 00 01 01 00 00 00  04                        ........ .
    0000000D  04 00 00 01 01 00 00 00  05                    ........ .
00000009  04 01 00 01 08 00 00 00  01 00 2e a5 de 51 00 50   ........ .....Q.P
    00000016  04 01 00 01 03 00 00 00  02 e0 7a              ........ ..z
00000019  04 01 00 00 45 01 00 00  47 45 54 20 2f 64 61 74   ....E... GET /dat
00000029  61 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   a.html H TTP/1.1.
00000039  0a 48 6f 73 74 3a 20 34  36 2e 31 36 35 2e 32 32   .Host: 4 6.165.22
00000049  32 2e 38 31 0d 0a 55 73  65 72 2d 41 67 65 6e 74   2.81..Us er-Agent
00000059  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 57   : Mozill a/5.0 (W
00000069  69 6e 64 6f 77 73 20 4e  54 20 35 2e 31 3b 20 72   indows N T 5.1; r
00000079  76 3a 31 30 2e 30 2e 32  29 20 47 65 63 6b 6f 2f   v:10.0.2 ) Gecko/
00000089  32 30 31 30 30 31 30 31  20 46 69 72 65 66 6f 78   20100101  Firefox
00000099  2f 31 30 2e 30 2e 32 0d  0a 41 63 63 65 70 74 3a   /10.0.2. .Accept:
000000A9  20 74 65 78 74 2f 68 74  6d 6c 2c 61 70 70 6c 69    text/ht ml,appli
000000B9  63 61 74 69 6f 6e 2f 78  68 74 6d 6c 2b 78 6d 6c   cation/x html+xml
000000C9  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 6d 6c   ,applica tion/xml
000000D9  3b 71 3d 30 2e 39 2c 2a  2f 2a 3b 71 3d 30 2e 38   ;q=0.9,* /*;q=0.8
000000E9  0d 0a 41 63 63 65 70 74  2d 4c 61 6e 67 75 61 67   ..Accept -Languag
000000F9  65 3a 20 65 6e 2d 75 73  2c 65 6e 3b 71 3d 30 2e   e: en-us ,en;q=0.
00000109  35 0d 0a 41 63 63 65 70  74 2d 45 6e 63 6f 64 69   5..Accep t-Encodi
00000119  6e 67 3a 20 64 65 66 6c  61 74 65 0d 0a 43 6f 6e   ng: defl ate..Con
00000129  6e 65 63 74 69 6f 6e 3a  20 63 6c 6f 73 65 0d 0a   nection:  close..
00000139  50 72 61 67 6d 61 3a 20  6e 6f 2d 63 61 63 68 65   Pragma:  no-cache
00000149  0d 0a 43 61 63 68 65 2d  43 6f 6e 74 72 6f 6c 3a   ..Cache- Control:
00000159  20 6e 6f 2d 63 61 63 68  65 0d 0a 0d 0a             no-cach e....
    00000021  04 01 00 00 eb 00 00 00  48 54 54 50 2f 31 2e 31   ........ HTTP/1.1
    00000031  20 32 30 30 20 4f 4b 0d  0a 53 65 72 76 65 72 3a    200 OK. .Server:
```

Hex Dump [✓]

C&C packet capture

Ping/Pong

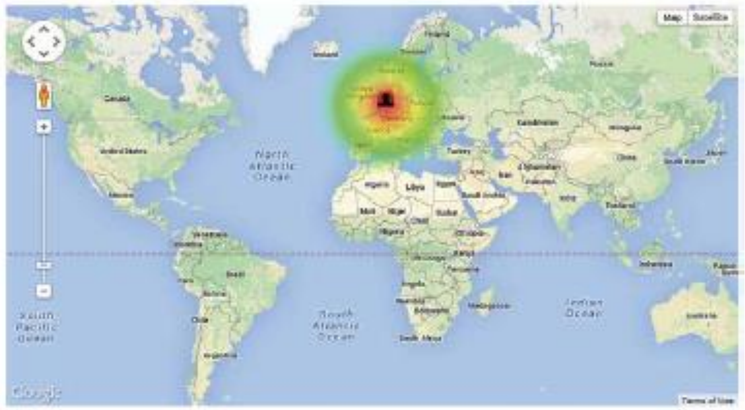
Proxy Request

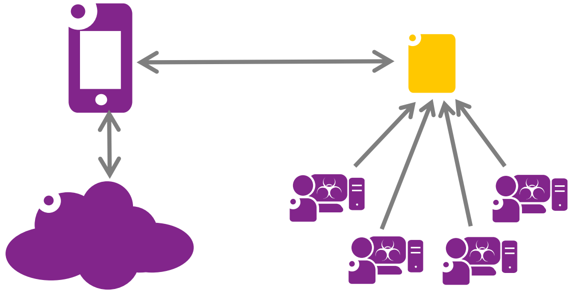
Data

NotCompatible - Overview

- Web Proxy Bot ported from Windows to Android environment.
- Allows remote miscreants to anonymously browse the web through the victim's phone.
- Consumes lots of bandwidth, for example 165MB in two hours over 300K TCP sessions

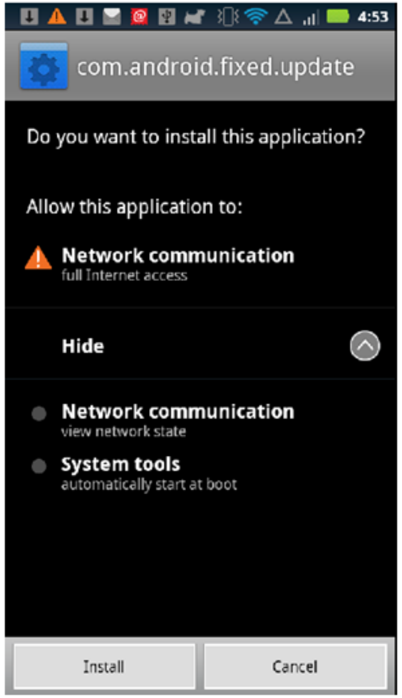
MAP: ANDROID.BOT.NOTCOMPATIBLE





NotCompatible – Infection

- Phishing spam is used to lure the victim to an infected web site.
- Web site tells you the browser is "not compatible" and provides an update.
- The user downloads and installs update.apk
- Malware has no icon or user interface. It is automatically started on BOOT.
- You can get rid of the infection by uninstalling the application.


com.android.fixed.update

Do you want to install this application?

Allow this application to:

Network communication
full Internet access

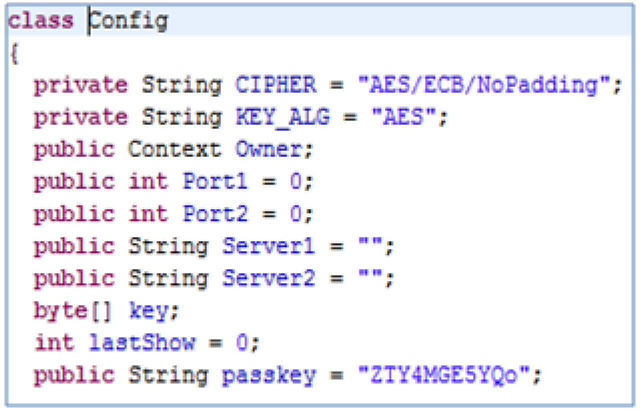
Hide

Network communication
view network state

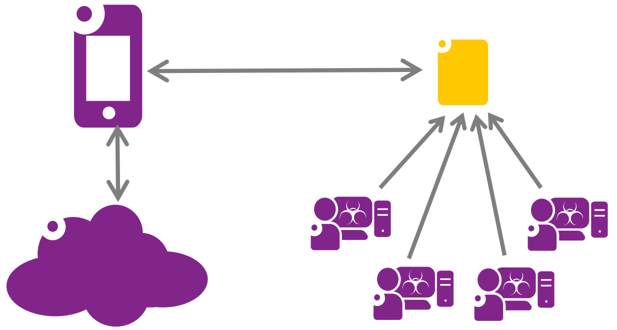
System tools
automatically start at boot

NotCompatible – Operation

- Opens an encrypted configuration file containing the address and port number of the server.
- The bot connects to the server via TCP.
- Sophisticated command and control protocol is then used to multiplex Web proxy services over that connection.
- This provides an anonymous web browsing services to clients.



```
class Config
{
  private String CIPHER = "AES/ECB/NoPadding";
  private String KEY_ALG = "AES";
  public Context Owner;
  public int Port1 = 0;
  public int Port2 = 0;
  public String Server1 = "";
  public String Server2 = "";
  byte[] key;
  int lastShow = 0;
  public String passkey = "ZTY4MGE5YQo";
```



NotCompatible – Command & Control

- Simple command/response packet format contains both commands and data.
- Channel number can multiplex many connection at once.
- The ping and pong are used as a heartbeat when there is no proxy work to be done.
- Once a proxy request is issued the “raw data” commands are used to transfer the data in either direction.

Packet format:

0x04	chan	type	length	…data…

0x04	- Protocol Version (1 byte)
chan	- Multiplexor Channel number (2 bytes)
type	- 0x00:Proxy Data, 0x01:Command (1 byte)
len	- Length of the data field (4 bytes)
data	- Is either proxy packet data or a command

Commands:

```
Initial handshake:          | 00 | 07000v00 |
Proxy to IP:                | 01 | 00 |IP & port|
Proxy to domain name:       | 01 | 01 |len|domain name|
Response to proxy:          | 02 | nnnn |
End of proxy session:       | 03 |
Ping:                       | 04 |
Pong:                       | 05 |
Unknown (from victim):      | FC | 01 |
Set Timeout:                | FD | timeout |
Set Reserve Server:         | FE | server IP and port |
Set Primary Server:         | FF | server IP and port |
```

NotCompatible – Uses & Impact

- Uses
  - Anonymous Web Browsing Service
  - Providing Access to Restricted Foreign Content
  - Ad-Click Fraud
  - Web Site Optimization Fraud
  - APT Probing and Exfiltration

- Impact
  - One user from Finland, roaming in the US, used over 165MBytes in less than two hours of airtime.
  - In the lab it averages 100MBytes per hour.
  - Causes huge data bills
  - Caused the battery to run down quickly
  - Who knows what sites your phone in visiting!!!

Summary

- Android malware analysis enables you to:
  - Know what the malware does
  - Understand the threat level
  - Detect and remediate the infection
- You should now know:
  - What tools are required
  - How to set up the network environment
  - How to use the tools

Questions?

Email: kevin.mcnamee@nokia.com

Twitter: @KevMcNamee