

Pengantar *Mobile Security*



idsecconf 2011
Indonesian Security Conference



*Risks,
Secure Design
and Testing*



Zaki Akhmad
za@indocisc.co.id

Risks



Hilang
Shouldering



Strong password
Data storage



Risiko privasi lokasi

Secure Design



Secure from the beginning not only secure by testing



Identifikasi lalu
lindungi data sensitif



Jalankan aplikasi dengan
hak akses minimum

Praktikkan prinsip *secure coding*

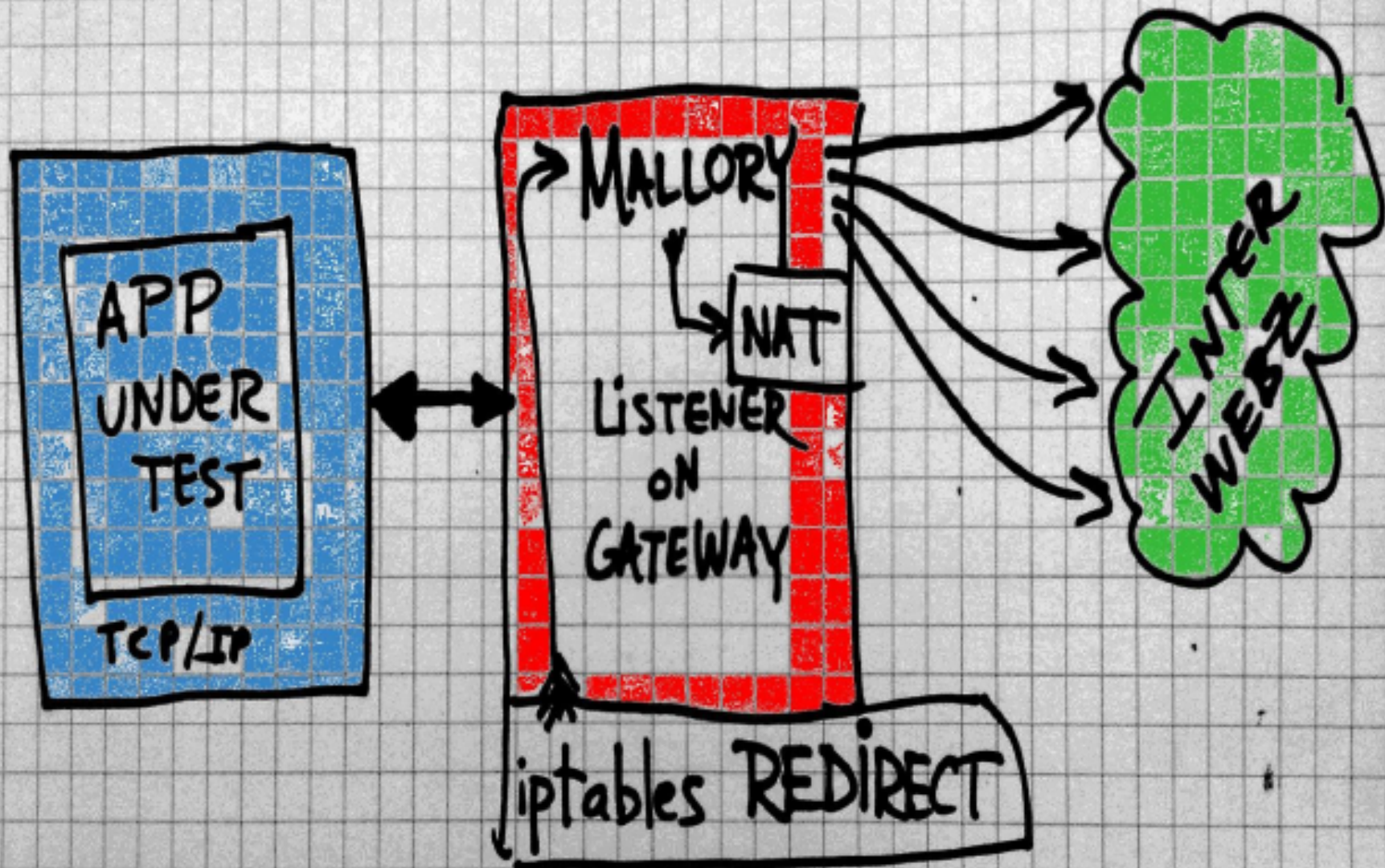
```
1 int main()  
2 {  
3     char array[10];  
4     array[10] = 100;  
5     return 0;  
6 }
```


Testing

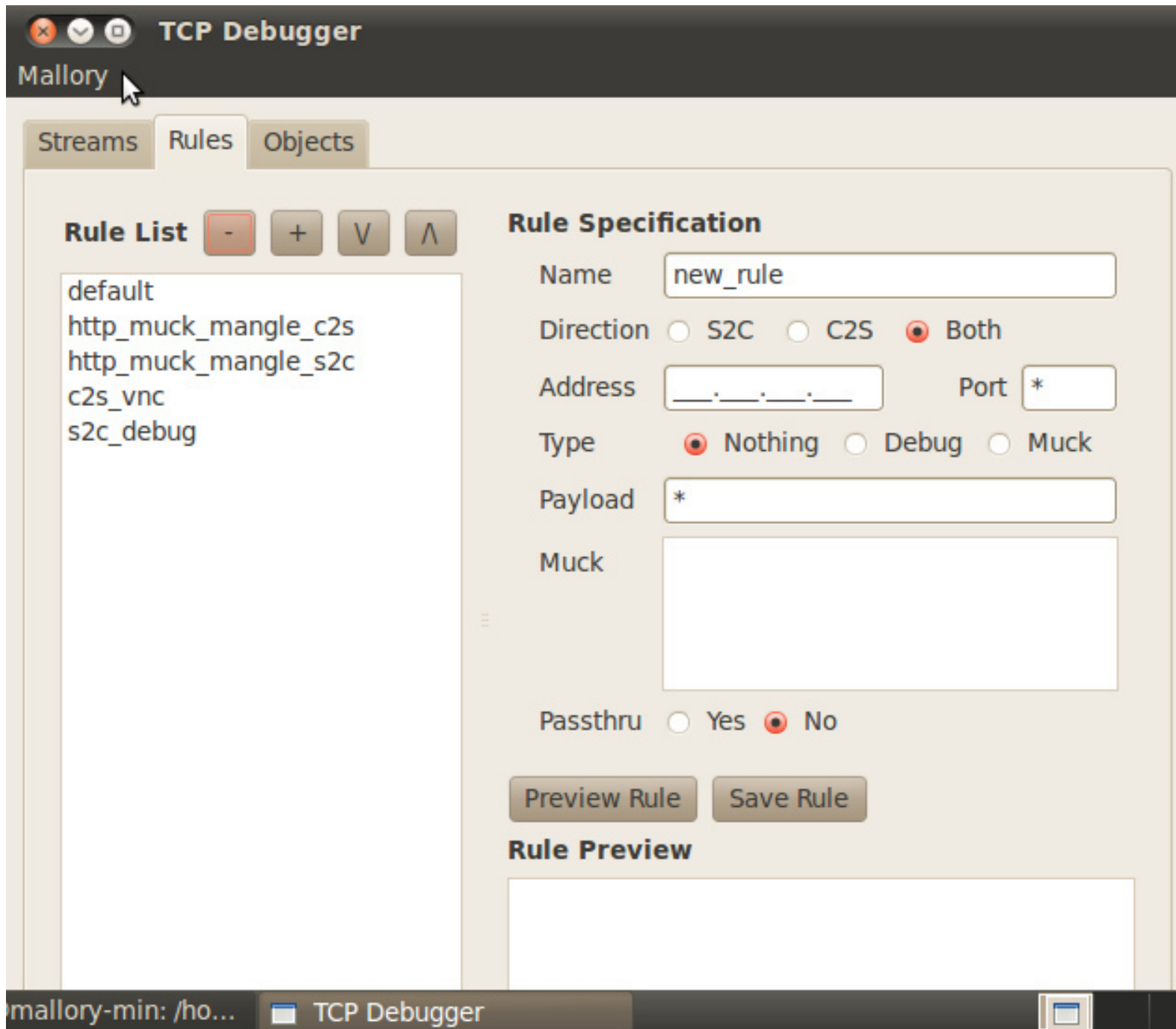


Dynamic analysis
Static analysis

Dynamic analysis



Proxying traffic



Mallory

Masuk



Silakan masukkan alamat surel pengguna untuk mesin scan.

Jika anda memilih salah satu dari profil, anda hanya perlu memasukkan kata sandi.

Sebelum menekan tombol login anda dapat menyimpan ke dalam profil.

Perhatikan, bahwa mesin scan harus mendukung OMP pada port yang ditentukan agar koneksi berhasil.

Profil

za

Simpan Hapus

Alamat server Port

localhost 9390 ?

Nama Pengguna

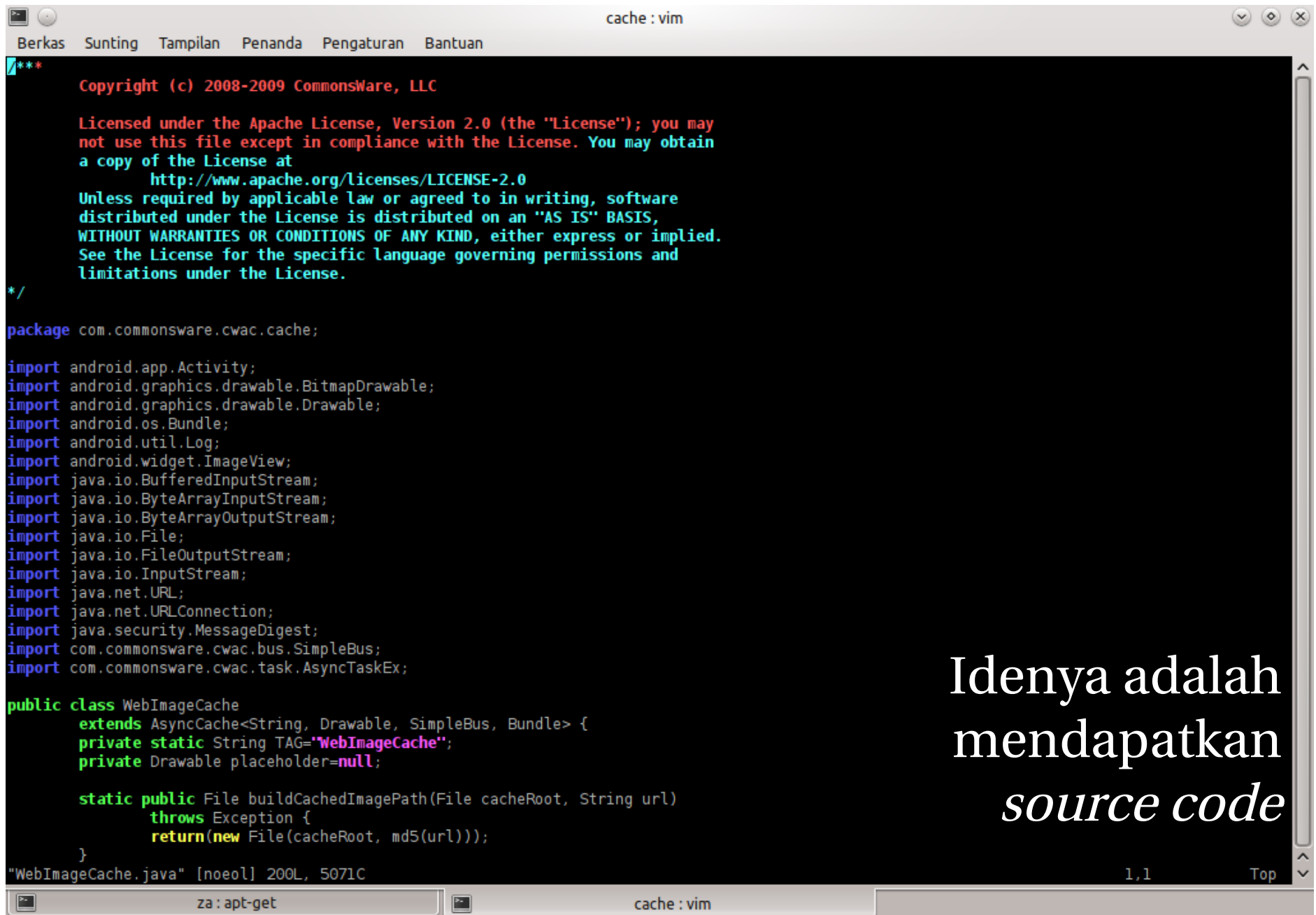
za

Kata Sandi

Masuk Batal

*Server side
assessment*

Static Analysis



```
cache : vim
Berkas Sunting Tampilan Penanda Pengaturan Bantuan

***
Copyright (c) 2008-2009 CommonsWare, LLC

Licensed under the Apache License, Version 2.0 (the "License"); you may
not use this file except in compliance with the License. You may obtain
a copy of the License at
    http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
*/

package com.commonware.cwac.cache;

import android.app.Activity;
import android.graphics.drawable.BitmapDrawable;
import android.graphics.drawable.Drawable;
import android.os.Bundle;
import android.util.Log;
import android.widget.ImageView;
import java.io.BufferedInputStream;
import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.io.File;
import java.io.FileOutputStream;
import java.io.InputStream;
import java.net.URL;
import java.net.URLConnection;
import java.security.MessageDigest;
import com.commonware.cwac.bus.SimpleBus;
import com.commonware.cwac.task.AsyncTaskEx;

public class WebImageCache
    extends AsyncCache<String, Drawable, SimpleBus, Bundle> {
    private static String TAG="WebImageCache";
    private Drawable placeholder=null;

    static public File buildCachedImagePath(File cacheRoot, String url)
        throws Exception {
        return(new File(cacheRoot, md5(url)));
    }
}

"WebImageCache.java" [noeol] 200L, 5071C
1,1 Top
```

Idenya adalah
mendapatkan
source code



Wordpress untuk Android

Dapatkan berkas .apk

<http://android.trac.wordpress.org/export/236/tags/1.4.1/bin/wp-android.apk>

atau

Pull berkas apk dari perangkat Android

```
za@zara:~/idsecconf2011$ unzip wp-android.apk
```

```
Archive:  wp-android.apk
```

```
  inflating: res/anim/cycle_5.xml
  inflating: res/anim/shake.xml
 extracting: res/drawable/add.png
 extracting: res/drawable/app_icon.png
 extracting: res/drawable/bottom_bar.9.png
 extracting: res/drawable/btn_check_off_pressed.png
 extracting: res/drawable/btn_check_off_selected.png
 extracting: res/drawable/btn_check_on_pressed.png
 extracting: res/drawable/btn_check_on_selected.png
 extracting: res/drawable/btn_dropdown_normal.9.png
 extracting: res/drawable/btn_dropdown_pressed.9.png
 extracting: res/drawable/btn_dropdown_selected.9.png
  inflating: res/drawable/comment_pending_bg_selector.xml
  inflating: res/drawable/comment_pending_gradient.xml
 extracting: res/drawable/comments_tab.png
 extracting: res/drawable/comments_tab_active.png
 extracting: res/drawable/content_bg.9.png
 extracting: res/drawable/gallery_selected_default.9.png
 extracting: res/drawable/grey_wp_button.9.png
 extracting: res/drawable/grey_wp_button_active.9.png
 extracting: res/drawable/grey_wp_button_down.9.png
  inflating: res/drawable/home_gradient.xml
 extracting: res/drawable/ic_menu_add.png
 extracting: res/drawable/ic_menu_close_clear_cancel.png
 extracting: res/drawable/ic_menu_delete.png
 extracting: res/drawable/ic_menu_edit.png
 extracting: res/drawable/ic_menu_more.png
 extracting: res/drawable/ic_menu_notifications.png
 extracting: res/drawable/ic_menu_preferences.png
 extracting: res/drawable/ic_menu_prefs.png
 extracting: res/drawable/ic_menu_rotate.png
 extracting: res/drawable/ic_popup_sync_1.png
  inflating: res/drawable/list_bg.xml
  inflating: res/drawable/list_bg_selector.xml
  inflating: res/drawable/list_divider.xml
  inflating: res/drawable/list_header_bg.xml
```

```
idsecconf2011 : bash
Berkas  Sunting  Tampilan  Penanda  Pengaturan  Bantuan
za@zara:~/idsecconf2011$ ../tools/android/apktool/apktool d wp-android.apk
I: Baksmaling...
I: Loading resource table...
I: Loaded.
I: Loading resource table from file: /home/za/apktool/framework/1.apk
I: Loaded.
I: Decoding file-resources...
I: Decoding values*/* XMLs...
I: Done.
I: Copying assets and libs...
za@zara:~/idsecconf2011$
```

\$ apktool
a tool for reengineering Android apk files

idsecconf2011 : apt-get idsecconf2011 : svn idsecconf2011 : bash idsecconf2011 : bash

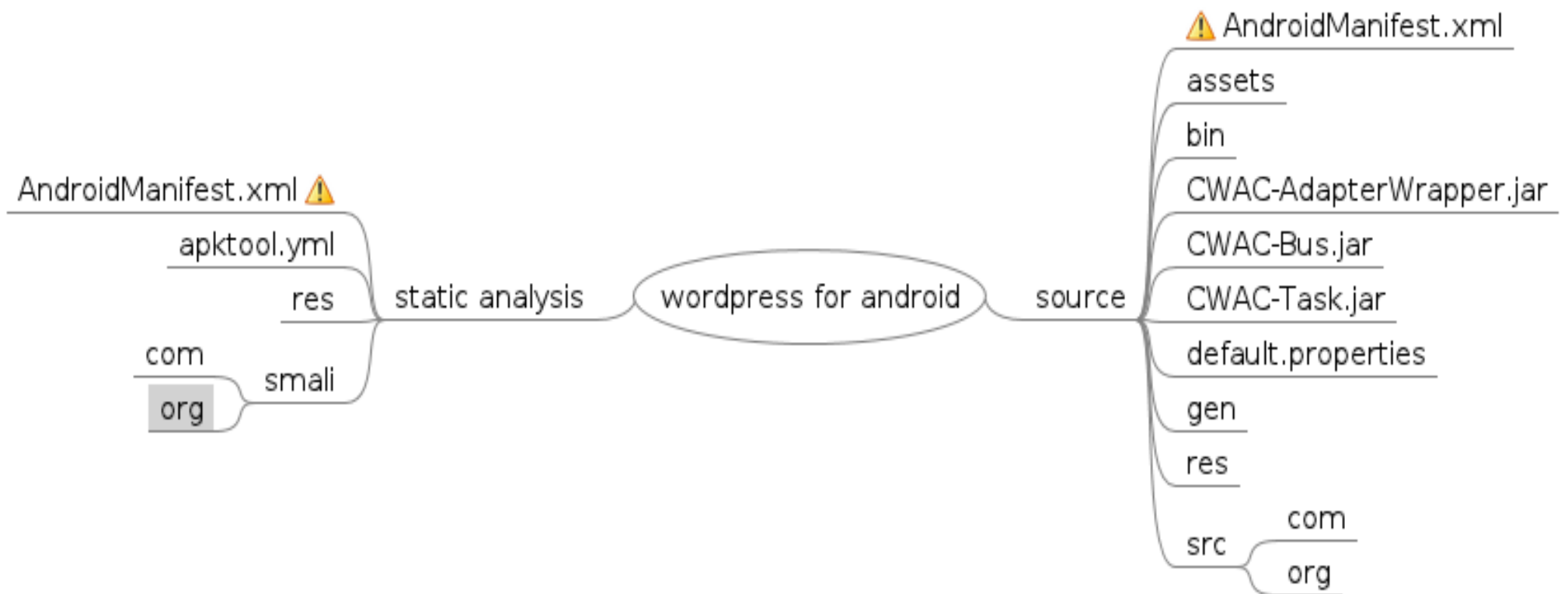
Bandingkan

Dapatkan *source code*

```
$ svn co http://android.svn.wordpress.org/
```

```
za@zara:~/idsecconf2011$ svn co http://android.svn.wordpress.org
```

```
A   android.svn.wordpress.org/trunk
A   android.svn.wordpress.org/trunk/default.properties
A   android.svn.wordpress.org/trunk/.classpath
A   android.svn.wordpress.org/trunk/assets
A   android.svn.wordpress.org/trunk/.project
A   android.svn.wordpress.org/trunk/AndroidManifest.xml
A   android.svn.wordpress.org/trunk/src
A   android.svn.wordpress.org/trunk/src/org
A   android.svn.wordpress.org/trunk/src/org/xmlrpc
A   android.svn.wordpress.org/trunk/src/org/xmlrpc/android
A   android.svn.wordpress.org/trunk/src/org/xmlrpc/android/XMLRPCSerializer.java
A   android.svn.wordpress.org/trunk/src/org/xmlrpc/android/Base64Coder.java
A   android.svn.wordpress.org/trunk/src/org/xmlrpc/android/XMLRPCFault.java
A   android.svn.wordpress.org/trunk/src/org/xmlrpc/android/Base64.java
A   android.svn.wordpress.org/trunk/src/org/xmlrpc/android/XMLRPCClient.java
A   android.svn.wordpress.org/trunk/src/org/xmlrpc/android/XMLRPCException.java
A   android.svn.wordpress.org/trunk/src/org/xmlrpc/android/ApiHelper.java
A   android.svn.wordpress.org/trunk/src/org/wordpress
A   android.svn.wordpress.org/trunk/src/org/wordpress/android
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/Settings.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/TabView.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/Preferences.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/models
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/models/MediaFile.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/models/Blog.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/models/Post.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/ViewPosts.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/UploadDialog.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/AddAccount.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/Signup.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/NewAccount.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/ServiceUpdateUIListener.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/CommentBroadcastReceiver.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/ViewPost.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/ViewComments.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/ReplyToComment.java
A   android.svn.wordpress.org/trunk/src/org/wordpress/android/AddAccountSettings.java
```



Referensi

Himanshu Dwivedi, “Mobile Application Security”

Intrepidus Group, “Mallory”

Jack Maninno, “Reversing Android Apps”

OWASP, “Mobile Security Project”



foto-foto
[flickr.com/zakiakhmad](https://www.flickr.com/photos/zakiakhmad/)

