



# Security in IoT Ecosystem

## Module 7

### Smart Socket Pentest Part III

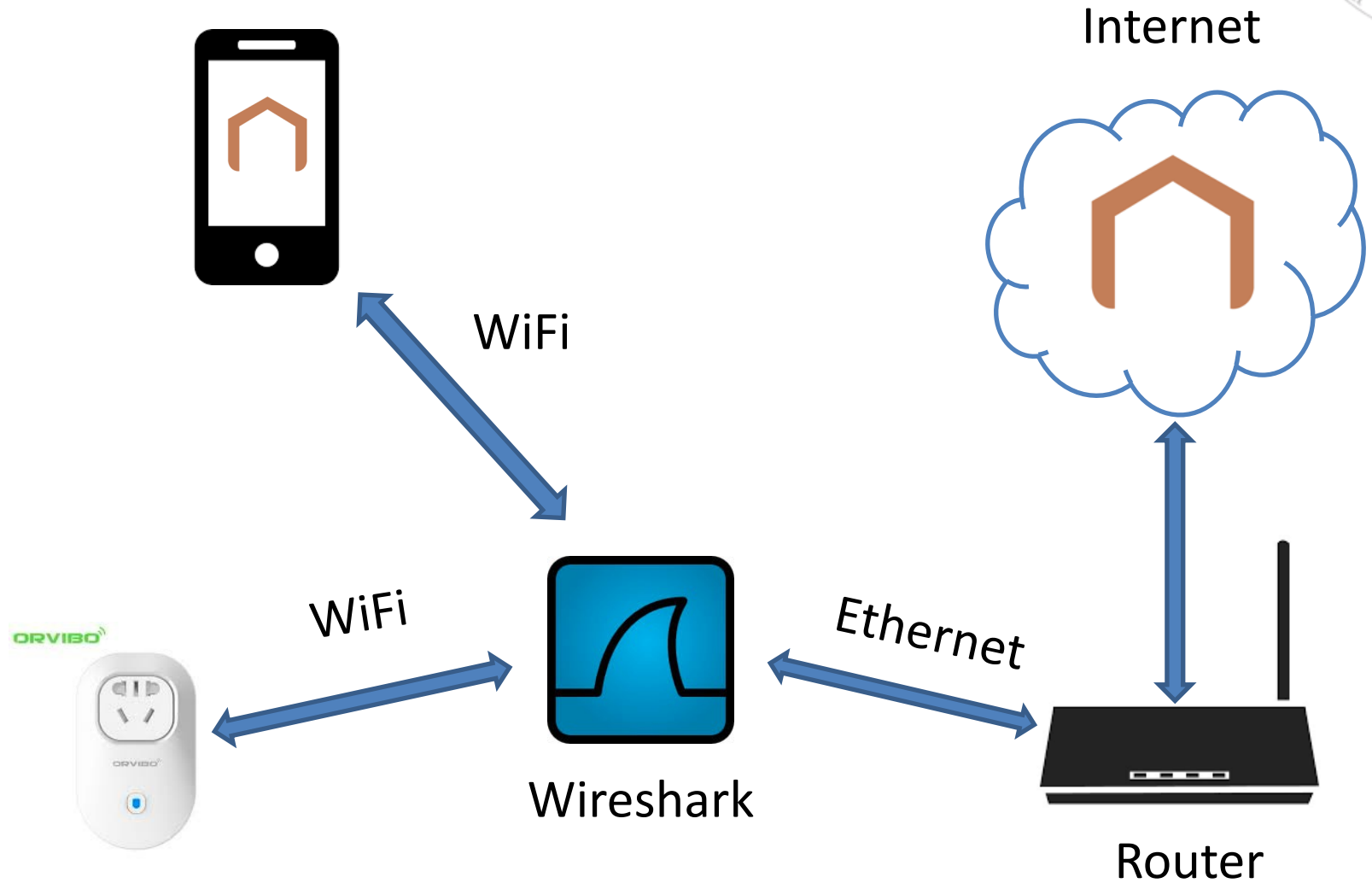
Prof.: Joaquín Recas

# Smart Socket Initial Setup



1. Initial Setup
2. Capture Traffic
3. Traffic analysis
4. Apk Analysis

# Study communications:



# Information we know



- IP numbers:
  - Orvibo server, Raspberry Pi, Smartphone & Smartsocket
- There are messages with payload between the Smartplug and the Orvibo server
  - Encrypted content!



# Next steps



- Can we decrypt the messages?
  - We need method and encryption key
- Where can we find the key?
  - Inside the device
  - On the Orvibo server
  - **In the HomeMate App**

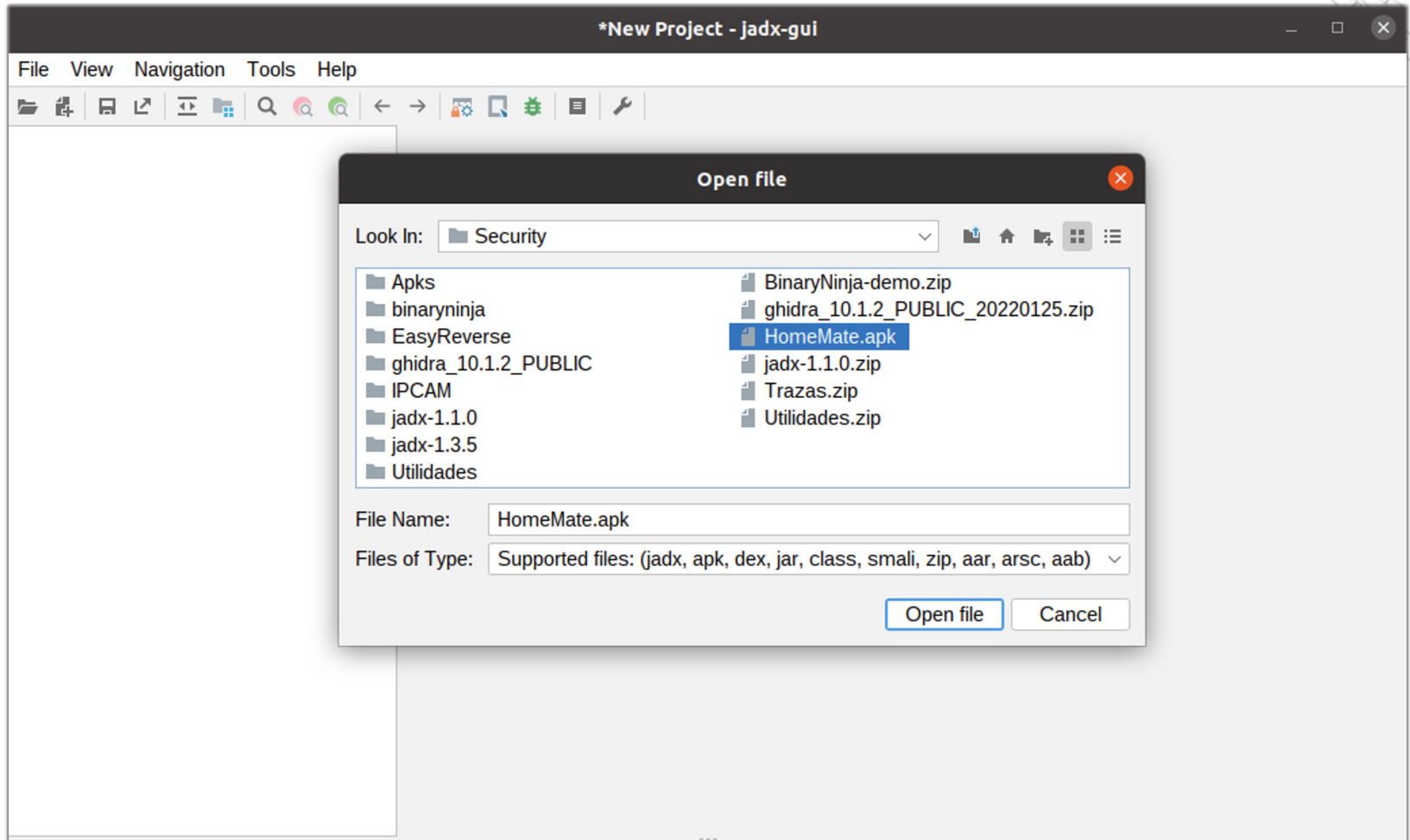
# JADX



- Dex ([Dalvik Executable](#)) to Java decompiler
  - Command line and GUI tools for produce Java source code from Android **Dex** and **Apk** files
- Main features:
  - Decompile Dalvik bytecode to java classes from **APK, dex, aar** and **zip** files
  - Decode *AndroidManifest.xml* and other resources from *resources.arsc*
  - Deobfuscator included
- `jadx-gui` features:
  - View **decompiled code** with highlighted syntax
  - Jump to declaration
  - Find usage
  - Full text search

<https://github.com/skylot/jadx>

# jadx-gui





# jadx-gui: HomeMate



The screenshot shows the jadx-gui interface for the HomeMate.apk. The left sidebar displays the project structure, with the following packages visible:

- android.arch
  - core.internal
    - FastSafeIterableMap
      - mHashMap HashMap<K, SafeIterableMap\$Entry<K, V>
      - ceil(K) Map\$Entry<K, V>
      - contains(K) boolean
      - get(K) SafeIterableMap\$Entry<K, V>
      - putIfAbsent(K, V) V
      - remove(K) V
      - SafeIterableMap
        - lifecycle
      - net
      - support
- butterknife
- c.keeu.homematesecurity
- cn.colourlife.oauthlogin
- com
- cz.msebera
- de.greenrobot.event
- homateap.orvibo.com.securitylibrary
- io.card.payment
- javax.jmdns
- kotlin
- mtopsdk
- net.sourceforge.pinyin4j
- no.nordicsemi.android.support.v18.scanner
- okhttp3
- okio

The main editor displays the source code for `FastSafeIterableMap` in the package `android.arch.core.internal`. The code includes annotations like `@RestrictTo` and `@Override`, and methods such as `putIfAbsent`. A blue text box is overlaid on the code editor with the text:

Too much information!!  
What are we looking for??

The status bar at the bottom indicates "Issues: 1 errors" and provides options for "Code", "Smali", "Simple", "Fallback", and "Split view".



# jadx-gui: Search

The screenshot shows the jadx-gui application window titled "\*HomeMate - jadx-gui". A "Text search: import" dialog box is open in the foreground, allowing the user to search for the text "import". The dialog includes options to search definitions (Class, Method, Field, Code, Resource, Comments) and search options (Case insensitive, Regex, Active tab only). The "Code" option is selected under "Search definitions of:", and "Case insensitive" is checked under "Search options:". The dialog shows "Showing results 0 to 0 of 0".

In the background, the jadx-gui interface displays a file tree on the left and decompiled Java code on the right. A blue callout box with the text "It will take some time..." is overlaid on the code. At the bottom left, a red box highlights a progress bar labeled "Decompiling..." with a value of 23%.

```
otation.RestrictTo.Scope.LIBRARY_GROUP}})
.core.internal.SafeIterableMap<K, V> {
.SafeIterableMap.Entry<K, V>> mHashMap = new java.util.H

try<K, V> get(K r2) {
.SafeIterableMap$Entry<K, V>> r0 = r1.mHashMap
y r0 = (android.arch.core.internal.SafeIterableMap.Entry

l K r4, @android.support.annotation.NonNull V r5) {
r3 = this;
android.arch.core.internal.SafeIterableMap$Entry r0 = r3.get(r4)
if (r0 == 0) goto L9
V r1 = r0.mValue
L8:
return r1
L9:
```

It will take some time...

Decompiling... 23%

Code Smali Simple Fallback Split view



# jadx-gui: Search

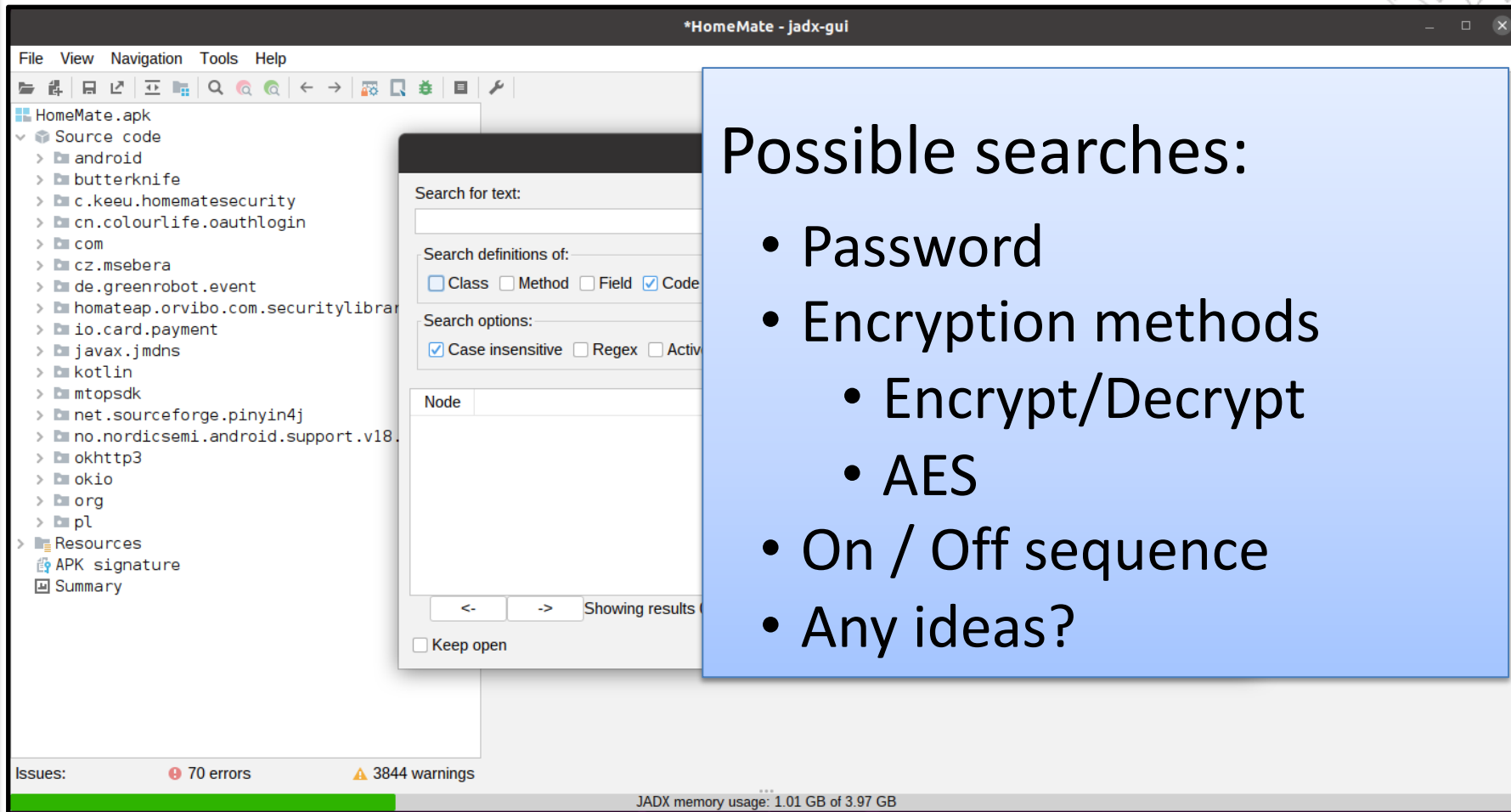
**Increase VM RAM to 6GB:**

- Turn off
- Select the VM
- Go to settings-> System
- Increase base memory

The screenshot shows the jadx-gui interface with a search for 'import' in the 'arch' directory. A dialog box indicates 'Jadx is running low on memory'. The status bar at the bottom shows 'JADX memory usage: 0.94 GB of 2.69 GB'.



# jadx-gui: Search



The screenshot shows the jadx-gui search dialog box. The dialog has the following fields and options:

- Search for text:** A text input field.
- Search definitions of:** Radio buttons for Class, Method, Field, and Code. The Code option is selected.
- Search options:** Checkboxes for Case insensitive, Regex, and Active. The Case insensitive option is selected.
- Node:** A text input field for specifying a search node.
- Showing results:** A button with left and right arrows.
- Keep open:** A checkbox.

The background shows the jadx-gui interface with a file tree on the left and a status bar at the bottom indicating 70 errors and 3844 warnings.

## Possible searches:

- Password
- Encryption methods
  - Encrypt/Decrypt
  - AES
- On / Off sequence
- Any ideas?

# jadx-gui: Password



The screenshot shows the jadx-gui interface with a search window titled "Text search: Password". The search results are displayed in a table with two columns: "Node" and "Code".

Node	Code
com.orvibo.homemate.view.custom.inputpassword.GridPasswordView.s	void setPasswordVisibility(boolean)
com.video.go.camera.ShareCameraItem.setPassword(String) void	void setPassword(String)
com.orvibo.homemate.core.ProcessPayload.modifyPassword(int, long)	void modifyPassword(int, long, JSONObject)
com.orvibo.homemate.api.UserApi.resetPassword(String, BaseResult	void resetPassword(String, BaseResultListener)
com.danale.video.sdk.platform.entity.Session.forgetPassword(int,	boolean forgetPassword(int, String, String, PlatformResultHandler)
com.orvibo.homemate.model.ResetPassword.onEventMainThread(ResetP	void onEventMainThread(ResetPasswordEvent)
com.orvibo.homemate.view.custom.inputpassword.PasswordView.getPa	String getPassword()
com.orvibo.homemate.view.custom.inputpassword.GridPasswordView.c	boolean getPasswordVisibility()
org.apache.http.auth.NTCredentials.getPassword() String	String getPassword()
com.danale.video.sdk.platform.entity.Session.forgetPassword(int,	boolean forgetPassword(int, String, PlatformResultHandler)
com.orvibo.homemate.bo.CameraInfo.setPassword(String) void	void setPassword(String)
okhttp3.HttpUrl.password() String	String password()
com.video.go.util.LocalInfo.getPassword() String	String getPassword()
com.danale.video.sdk.platform.result.ModifyPasswordResult.Modify	void ModifyPasswordResult(int)
org.apache.http.auth.UsernamePasswordCredentials.UsernamePasswo	void UsernamePasswordCredentials(String, String)
com.orvibo.homemate.model.ResetPassword.onResetPasswordResult(lo	void onResetPasswordResult(Long, int)
org.apache.commons.httpclient.HttpURL.setRawPassword(char[]) vo	void setRawPassword(char[])
com.orvibo.homemate.view.custom.inputpassword.GridPasswordView.c	void clearPassword()
com.orvibo.homemate.view.custom.inputpassword.PasswordView.setPa	void setPasswordType>PasswordType)

Showing results 1 to 100 of 195

Issues: 70 errors 3844 warnings Code Smali Simple Fallback Split view

JADX memory usage: 1.14 GB of 3.97 GB

# jadx-gui: AES



\*HomeMate - jadx-gui

File View Navigation Tools Help

HomeMate.apk AESCrypt

Text search: aes

Search for text: aes

Search definitions of:  Class  Method  Field  Code  Resource  Comments

Search options:  Case insensitive  Regex  Active tab only

Node	Code
com.ali.auth.third.core.storage.aes.AESCrypt.AESCrypt() void	void AESCrypt()
com.ali.auth.third.ui.support.BaseActivityResultHandler.onTaeSDKA	void onTaeSDKActivityResult(int, int, Intent, BaseWebViewActivity, Map<C
com.ali.auth.third.login.handler.LoginActivityResultHandler.onTae	void onTaeSDKActivityResult(int, int, Intent, BaseWebViewActivity, Map<C
com.orvibo.homemate.ap.ApConstant.ENC_TKIPAES String	String ENC_TKIPAES
com.alibaba.wireless.security.open.staticdataencrypt.IStaticDataE	int OPEN_ENUM_CIPHER_AES256
okhttp3.CipherSuite.TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 CipherS	CipherSuite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
okhttp3.CipherSuite.TLS_DHE_RSA_WITH_AES_256_CBC_SHA CipherSuite	CipherSuite TLS_DHE_RSA_WITH_AES_256_CBC_SHA
com.ali.auth.third.core.storage.aes.AESCrypt.AES_MODE String	String AES_MODE
okhttp3.CipherSuite.TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 CipherSui	CipherSuite TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
okhttp3.CipherSuite.TLS_DH_anon_WITH_AES_256_CBC_SHA CipherSuite	CipherSuite TLS_DH_anon_WITH_AES_256_CBC_SHA
com.alibaba.sdk.android.oss.model.ObjectMetadata.AES_256_SERVER_S	String AES_256_SERVER_SIDE_ENCRYPTION
com.danale.video.jni.DtmfAudioCodec.WIFI_ENCTYPE_WPA2_AES int	int WIFI_ENCTYPE_WPA2_AES
okhttp3.CipherSuite.TLS_ECDH_RSA_WITH_AES_256_CBC_SHA CipherSuite	CipherSuite TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
com.alibaba.wireless.security.open.staticdataencrypt.IStaticDataE	int OPEN_ENUM_CIPHER_AES192
okhttp3.CipherSuite.TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA CipherSu	CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
com.videogo.exception.ErrorCode.ERROR_CAS_AES_DECRYPT_FAILED int	int ERROR_CAS_AES_DECRYPT_FAILED
okhttp3.CipherSuite.TLS_PSK_WITH_AES_128_CBC_SHA CipherSuite	CipherSuite TLS_PSK_WITH_AES_128_CBC_SHA
com.alibaba.wireless.security.open.staticdataencrypt.IStaticDataE	int OPEN_ENUM_CIPHER_AES128
okhttp3.CipherSuite.TLS_DH_anon_WITH_AES_256_GCM_SHA384 CipherSui	CipherSuite TLS_DH_anon_WITH_AES_256_GCM_SHA384

Showing results 1 to 100 of 510

Keep open

Open Cancel

Issues: 70 errors 3844 warnings Code Small Simple Fallback Split view

JADX memory usage: 1.07 GB of 3.97 GB

Text) throws GeneralSecurityExc

commonUtils.getHashString(bytes)



# com.orvibo.homemate.ap.ApConstant



Tons of useful information!!  
Code for Initial pairing

```
1 package com.orvibo.  
2  
3 /* loaded from: class  
4 public class ApConstant {  
5     public static final  
6     public static final  
7     public static final  
8     public static final  
9     public static final String AUTH_OPEN = "OPEN";  
10    public static final String AUTH_SHARED = "SHARED";  
11    public static final String AUTH_WPA2PSK = "WPA2PSK";  
12    public static final String AUTH_WPAPSK = "WPAPSK";  
13    public static final String AUTH_WPAPSKWPA2PSK = "WPAPSKWPA2PSK";  
14    public static final String BATTERY_VALUE = "batteryValue";  
15    public static final String CMD = "cmd";  
16    public static final int CMD_GET_DEVICE = 79;  
17    public static final int CMD_RECEIVE_MEASURE_DATA = 143;  
18    public static final int CMD_REMAIN_TIME = 158;  
19    public static final int CMD_REQUEST_MEASURE = 160;  
20    public static final int CMD_SCAN_WIFI = 80;  
21    public static final int CMD_SET_WIFI = 81;  
22    public static final String CMD_TYPE = "cmdType";  
23    public static final String CO_CONCENTRATION = "coConcentration";  
24    public static final String DEVICE_NAME = "deviceName";  
25    public static final String ENC = "enc";  
26    public static final String ENC_AES = "AES";  
27    public static final String ENC_NONE = "NONE";  
28    public static final String ENC_TKIP = "TKIP";  
29    public static final String ENC_TKIPAES = "TKIPAES";  
30    public static final String ENC_WEP = "WEP";  
31    public static final String ENTITYFY = "EntityWifi";  
32    public static final String ENTITY_DEVICE = "entityDevice";  
33    public static final String ENTITY_WIFI = "entityWifi";  
34    public static final String HARDWARE_VERSION = "hardwareVersion";
```

# com.orvibo.homemate.ap.ApConstant



## Encrypt/Decrypt byte arrays

```
File View Navigation Tools Help
HomeMate.apk
  Source code
    android
    butterknife
    c.keuu.homematesecurity
    cn.colourlife.oauthlogin
    com
    cz.msebera
    de.greenrobot.event
    homemateap.orvibo.com.securitylibrary
      BuildConfig
      SecurityAes
    io.card.payment
    javax.jmdns
    kotlin
    mtopsdk
    net.sourceforge.pinyin4j
    no.nordicsemi.android.support.v18.scanner
    okhttp3
    okio
    org
    pl
  Resources
    APK signature
    Summary

package homemateap.orvibo.com.securitylibrary;

/* loaded from: classes3.dex */
8 public class SecurityAes {
    private static native String[] createPassword(byte[] bArr);

    private static native byte[] createSecurityKey(byte[] bArr);

    private static native byte[] decryptByte(byte[] bArr, int i, boolean z, String str);

    private static native byte[] decryptByteKey(byte[] bArr, int i, byte[] bArr2);

    private static native byte[] encryptByte(byte[] bArr, int i, boolean z, String str);

    private static native byte[] encryptByteKey(byte[] bArr, int i, byte[] bArr2);

    private static native boolean nativeIsPk(String str);

    static {
10     System.loadLibrary("HomeMate_Security");
    }

32 public static byte[] encrypt(byte[] data, String key, boolean isPk) {
33     if (data == null || data.length == 0) {
34         return null;
35     }
36     if (key == null) {
37         key = "";
38     }
39     return encryptByte(data, data.length, isPk, key);
40 }

47 public static byte[] decrypt(byte[] data, String key, boolean isPk) {
48     if (data == null || data.length == 0) {
49         return null;
50     }
51     return decryptByte(data, data.length, isPk, key);
52 }
}
```

Issues: 70 errors 3844 warnings Code Smali Simple Fallback Split view

JADX memory usage: 1.12 GB of 3.97 GB



# com.orvibo.homemate.ap.ApConstant



The screenshot shows an IDE window titled '\*HomeMate - jadx-gui'. The left sidebar displays a project tree for 'HomeMate.apk' with the following structure:

- Source code
  - android
  - butterknife
  - c.keeu.homematesecurity
  - cn.colourlife.oauthlogin
  - com
  - cz.msebera
  - de.greenrobot.event
  - homematep.orvibo.com.securitylibrary
    - BuildConfig
    - SecurityAes
  - io.card.payment
  - javax.jmdns
  - kotlin
  - mtopsdk
  - net.sourceforge.pinyin4j
  - no.nordicsemi.android.support.v18.scanner
  - okhttp3
  - okio
  - org
  - pl
- Resources
  - APK signature
  - Summary

The main editor displays the source code for 'SecurityAes'. A blue callout box with the text 'Source code is not available!!' is overlaid on the code. The code includes:

```
private static void loadLibrary() {
    System.loadLibrary("HomeMate_Security");
}

public static byte[] encrypt(byte[] data, String key, boolean isPk) {
    if (data == null || data.length == 0) {
        return null;
    }
    if (key == null) {
        key = "";
    }
    return encryptByte(data, data.length, isPk, key);
}

public static byte[] decrypt(byte[] data, String key, boolean isPk) {
    if (data == null || data.length == 0) {
        return null;
    }
    if (key == null) {
        key = "";
    }
    return decryptByte(data, data.length, isPk, key);
}

public static byte[] encryptKey(byte[] data, byte[] key) {
    if (data == null || data.length == 0) {
        return null;
    }
    return encryptByteKey(data, data.length, key);
}
```

The IDE status bar at the bottom shows 'Issues: 70 errors, 3844 warnings' and 'JADX memory usage: 1.14 GB of 3.97 GB'.

# Looking for decryptByte



```
iot@ubuntu: ~/Desktop/HomeMate/homemate
File Edit View Search Terminal Help
iot@ubuntu:~/Desktop/HomeMate/homemate$ rgrep decryptByte
Binary file lib/armeabi-v7a/libHomeMate_Security.so matches
Binary file lib/armeabi-v7a/libweibosdkcore.so matches
Binary file lib/arm64-v8a/libHomeMate_Security.so matches
Binary file lib/arm64-v8a/libweibosdkcore.so matches
Binary file classes4.dex matches
iot@ubuntu:~/Desktop/HomeMate/homemate$
```

We find it in a binary 🥲



# Binary Ninja

- Interactive disassembler, decompiler, and binary analysis platform for reverse engineers, malware analysts, vulnerability researchers, and software developers that runs on Windows, macOS, Linux.

## Disassemble

Disassemble executables and libraries from multiple formats, platforms, and architectures.

## Decompile

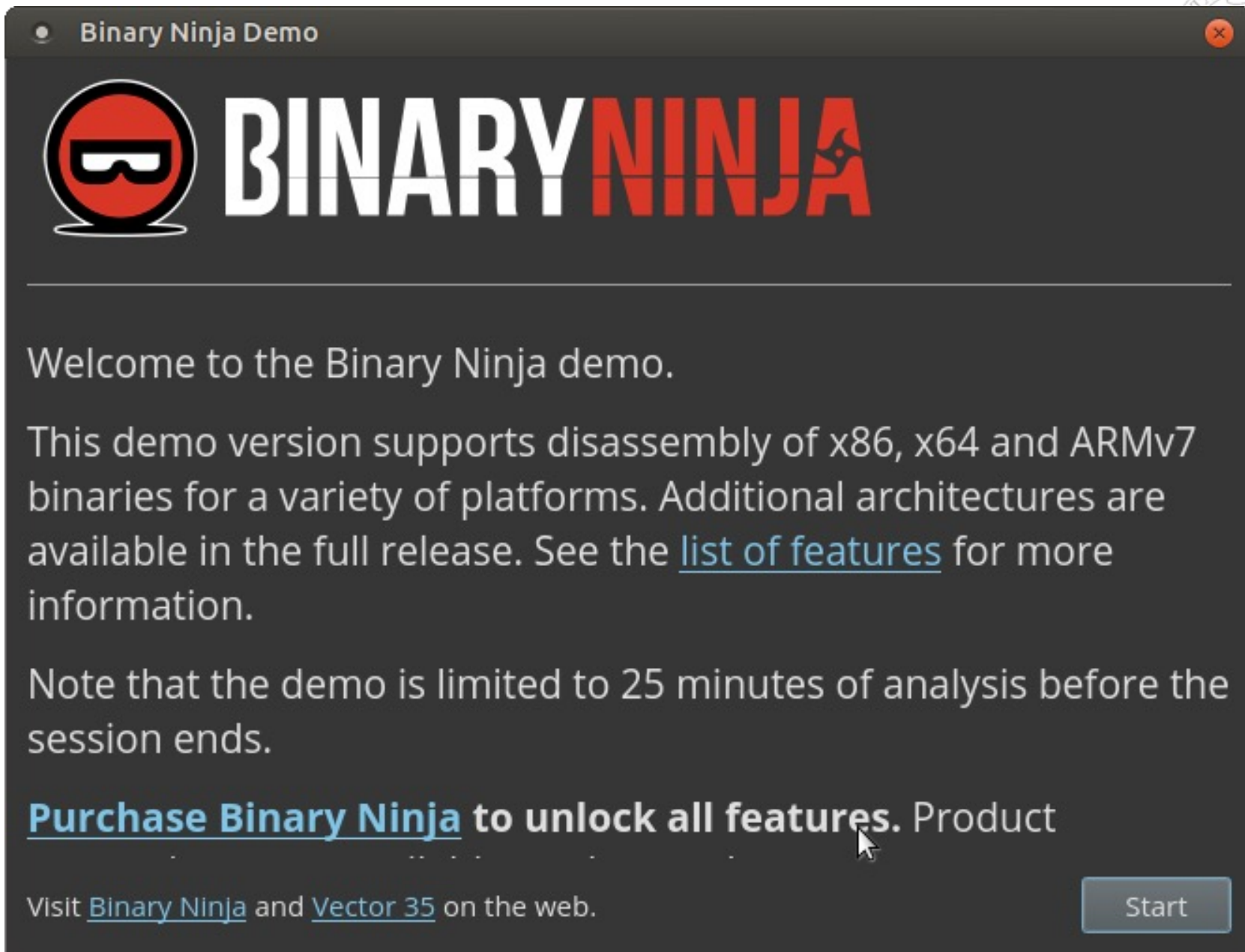
Decompile code to C or BNIL for any supported architecture - including your own

## Analyze

Visualize control flow and navigate through cross-references interactively.

## Annotate

Name variables and functions, apply types, create structures, and add comments.

A screenshot of a software window titled "Binary Ninja Demo". The window has a dark grey background. At the top left is the Binary Ninja logo, a red circle with a white 'B' and a black outline. To its right, the text "BINARY NINJA" is displayed in a large, bold, sans-serif font. "BINARY" is white and "NINJA" is red. Below the logo and title, there is a horizontal line. The main content area contains the following text:

Welcome to the Binary Ninja demo.

This demo version supports disassembly of x86, x64 and ARMv7 binaries for a variety of platforms. Additional architectures are available in the full release. See the [list of features](#) for more information.

Note that the demo is limited to 25 minutes of analysis before the session ends.

**[Purchase Binary Ninja](#) to unlock all features.** Product

Visit [Binary Ninja](#) and [Vector 35](#) on the web.

At the bottom right of the window is a light blue button with the text "Start".

Start

# Binary Ninja: dedcryptByte



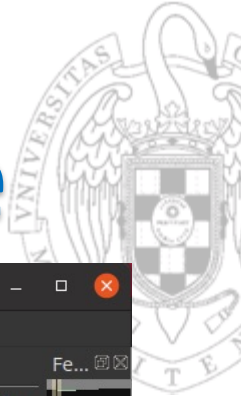
The screenshot shows the Binary Ninja interface with the following components:

- File Edit View Tools Window Help** (Menu bar)
- Cross References** (Panel)
- libHome...rity.so (ELF Graph)** (Tab)
- Disassembly** (View)
- int32\_t** (Type)
- Java\_homateap\_orvibo\_com\_securitylibrary\_SecurityAes (int32\_t\* arg1, int32\_t arg2, int32\_t arg3, int32\_t arg4, int32\_t arg5)** (Function Signature)
- Java\_homateap\_orvibo\_com...itylibrary\_SecurityAes\_decryptByteKey:** (Function Name)
- Assembly Code:**

```
push {r4, r5, r6, r7, lr} {var_4} {__saved_r7} {__saved_r6} {__s...
add r7, sp, #0xc {__saved_r7}
sub sp, #0x24
push {r3} {var_3c}
pop {r4} {var_3c}
push {r2} {var_3c_1}
pop {r1} {var_3c_1}
push {r0} {var_3c_2}
pop {r5} {var_3c_2}
movs r0, #0x17
lsls r6, r0, #5
ldr r0, [r5]
ldr r3, [r0, r6]
movs r2, #0
push {r5} {var_3c_3}
pop {r0} {var_3c_3}
str r1, [sp, #0x18] {var_20}
blx r3
str r0, [sp, #0x20] {var_18}
ldr r1, [sp, #0x38] {arg5}
cmp r1, #0
str r1, [sp, #0x14] {var_24}
beq #0x1fec
```
- Tags** (Panel)
- Bookmarks Tags Tag Types** (Sub-panels)
- Location Preview** (Table)
- Symbols** (Panel)
- Symbol List:**
  - \_\_cxa\_finalize
  - raise
  - sub\_1bb8
  - Java\_homateap\_orvibo\_com\_securitylibrary\_SecurityAes\_encryptByte**
  - Java\_homateap\_orvibo\_com\_securitylibrary\_SecurityAes\_decryptByte**
  - Java\_homateap\_orvibo\_com\_securitylibrary\_SecurityAes\_nativeIsPk**
  - Java\_homateap\_orvibo\_com\_securitylibrary\_SecurityAes\_encryptByteKey**
  - Java\_homateap\_orvibo\_com\_securitylibrary\_SecurityAes\_decryptByteKey**
  - Java\_homateap\_orvibo\_com\_securitylibrary\_SecurityAes\_createSecurityKey
  - Java\_homateap\_orvibo\_com\_securitylibrary\_SecurityAes\_createPassword
  - resync
  - AesDestroy
  - AesEncrypt
  - AesDecrypt
  - Cipher
  - InvCipher
  - AesEncryptEx
  - sub\_2e94
  - AesDecryptEx



# Binary Ninja: dedcryptByte



libHomeMate\_Security.so — Binary Ninja

File Edit View Tools Window Help

Cross References libHome...rity.so (ELF Graph) Fe...

int32\_t Java\_homateap\_orvibo\_com\_securitylibrary\_SecurityAes\_decryptByteKey( Disassembly  
int32\_t\* arg1, int32\_t arg2, int32\_t arg3, int32\_t arg4, int32\_t arg5)

```
movs    r2, #0
push   {r5} {var_3c_3}
pop    {r0} {var_3c_3}
str    r1, [sp, #0x18] {var_20}
blx   r3
str    r0, [sp, #0x20] {var_18}
ldr   r1, [sp, #0x38] {arg5}
cmp   r1, #0
str   r1, [sp, #0x14] {var_24}
beq   #0x1fec
```

Tags

Bookmarks Te

Location revle

Symbols

- \_\_cxa\_finalize
- raise
- sub\_1bb8
- Java\_homateap\_or
- Java\_homateap\_or
- Java\_homateap\_or
- Java\_homateap\_or
- Java\_homateap\_or**
- Java\_homateap\_or
- Java\_homateap\_or
- AesInit
- AesDestroy
- AesEncrypt
- AesDecrypt
- Cipher
- InvCipher
- AesEncryptEx
- sub\_2e94
- AesDecryptEx

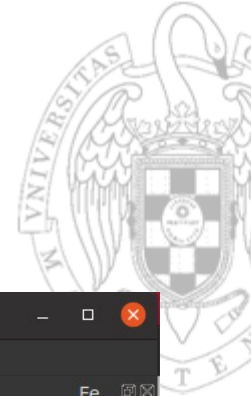
```
movs    r1, #1
push   {r4} {var_3c_10}
pop    {r0} {var_3c_10}
bl     #calloc
ldr   r1, [pc, #0x9c] {data_2094}
add   r1, pc {pkKey@GOT}
ldr   r1, [r1] {pkKey@GOT}
ldr   r6, [r1]
movs   r2, #0x10
```

```
movs    r0, #0xab
lsls   r0, r0, #2
ldr   r2, [r5]
ldr   r2, [r2, r0]
push  {r5} {var_3c_4}
pop   {r0} {var_3c_4}
str   r4, [sp, #0x1c] {var_1c_1}
push  {r1} {var_3c_5}
pop   {r4} {var_3c_5}
blx   r2
str   r0, [sp, #0x10] {var_28_1}
ldr   r0, [r5]
ldr   r3, [r0, r6]
movs   r2, #0
push  {r5} {var_3c_6}
pop   {r0} {var_3c_6}
push  {r4} {var_3c_7}
pop   {r1} {var_3c_7}
```

Selection: 0x1f84 to 0x1f86 (0x2 bytes) ELF Graph Options



# Binary Ninja: pkKey



The screenshot shows the Binary Ninja interface for the file `libHomeMate_Security.so`. The main window displays assembly code with the following sections:

```
00007ffc int32_t (* const _Unwind_VRS_Pop@GOT)() = _Unwind_VRS_Pop

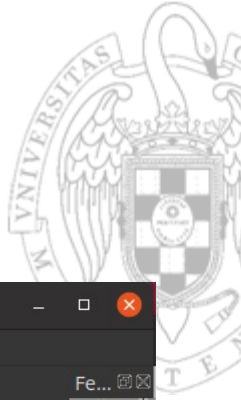
.got (PROGBITS) section ended {0x7ec8-0x8000}

.data (PROGBITS) section started {0x8000-0x800c}
00008000 data_8000:
00008000 00 00 00 00
...
00008004 uint32_t pkKey = 0x5d3c
00008008 uint32_t base64char = 0x5d0c
.data (PROGBITS) section ended {0x8000-0x800c}

.extern section started {0x8010-0x807c}
00008010 extern __aeabi_memclr
00008014 extern __aeabi_memclr4
00008018 extern __aeabi_memcpy
0000801c extern __aeabi_memset
00008020 extern __cxa_atexit
00008024 extern __cxa_begin_cleanup
00008028 extern void __cxa_call_unexpected(void*) __noreturn
0000802c extern __cxa_finalize
00008030 extern __cxa_type_match
00008034 extern __gnu_Unwind_Find_exidx
00008038 extern __sf
0000803c extern void __stack_chk_fail() __noreturn
00008040 extern __stack_chk_guard
00008044 extern void abort() __noreturn
00008048 extern calloc
0000804c extern fprintf
00008050 extern free
00008054 extern rand48
```

The line `00008004 uint32_t pkKey = 0x5d3c` is highlighted with a red box. The left sidebar shows the Symbols list, and the bottom status bar indicates the selection range is `0x8004 to 0x8008 (0x4 bytes)`.





# Binary Ninja: pkKey

libHomeMate\_Security.so — Binary Ninja

File Edit View Tools Window Help

Cross References libHome...rity.so (ELF Linear)

```

00005ce0 ab 3f 04 80 f4 f4 ff 7f-01 00 00 00 bc f6 ff 7f .?.....
00005cf0 b0 b0 b0 80 e4 f6 ff 7f-a8 0f b1 80 f2 f6 ff 7f .....
00005d00 f8 fd ff 7f f2 f6 ff 7f-b0 ab 06 80 6e f9 ff 7f .....n...
00005d10 a8 0f b1 80 8c f9 ff 7f-ec fd ff 7f 8e f9 ff 7f .....
00005d20 f0 fd ff 7f 98 f9 ff 7f-f4 fd ff 7f 96 f9 ff 7f .....
00005d30 f8 fd ff 7f 94 f9 ff 7f-01 00 00 00 .....
.ARM.exidx section ended {0x5b34-0x5d3c}

.rodata (PROGBITS) section started {0x5d3c-0x6618}
00005d3c                                     6b 68 67 67 khgg
00005d40 64 35 34 38 36 35 53 4e-4a 48 47 46 00 d54865SNJHGF.
00005d4d data_5d4d:
00005d4d                                     6a 61 76 jav
00005d50 61 2f 6c 61 6e 67 2f 53-74 72 69 6e 67 00 a/lang/String.
00005d5e data_5d5e:
00005d5e                                     4f 52 OR
00005d60 56 49 42 4f 00 VTR0.
00005d65 data_5d65:
00005d65                                     25 64 25-64 25 64 25 64
00005d70 64 00
00005d72 data_5d72:
00005d72                                     63 61 6e 27 74 20-73 75 70 70 6f
00005d80 6b 65 79 20 62 69 74 3a-25 64 0a 00 41
00005d90 45 46 47 48 49 4a 4b 4c-4d 4e 4f 50 51
00005da0 55 56 57 58 59 5a 61 62-63 64 65 66 67
00005db0 6b 6c 6d 6e 6f 70 71 72-73 74 75 76 77
00005dc0 30 31 32 33 34 35 36 37-38 39 2b 2f 00
00005dcd data_5dcd:
00005dcd                                     c0 9e 94 ...
00005dd0 4c 53 a8 f4 7c 0a ec 16-00 a7 f3 91 66 LS..|.....f
00005ddd data_5ddd:
00005ddd                                     63 7c 77 c|w
00005de0 7b f2 6b 6f c5 30 01 67-2b fe d7 ab 76 ca 82 c9 {.ko.0.g+...v...
00005de0 71 6 50 47 60 1 14 0 6 0 4 70 0 17 61 00 2 16

```

Selection: 0x5d3c to 0x5d4d (0x11 bytes) ELF Linear Options

Now we have the key!!!

**'khggd54865SNJHGF'**



# Binary Ninja: AES-ECB

libHomeMate\_Security.so — Binary Ninja

File Edit View Tools Window Help

Cross References libHome...rity.so (ELF)

int32\_t AES\_ECB\_en...

... and the method: AES ECB

```

AES_ECB_encrypt
push  {r4, r5, r6, r7, lr} {var_4} {__saved_r7} {__saved_r6} {__saved_r5} {__saved_r4}
sub   sp, #0x2c
movs  r4, #0
str   r1, [sp, #0x24] {var_1c}
str   r0, [sp, #8] {var_38}
push  {r0} {var_44}
pop   {r3} {var_44}
str   r4, [sp, #0x20] {var_20} {0x0}

ldr   r0, [sp, #0x20] {var_20}
mvns  r2, r0
movs  r5, #4
str   r1, [sp, #0x28] {var_18_1}
push  {r1} {var_44_1}
pop   {r6} {var_44_1}
push  {r3} {var_44_2}
pop   {r7} {var_44_2}

ldrb  r0, [r7]
ldrb  r1, [r6]
eors  r1, r0
strb  r1, [r6]
adds  r5, r5, r2
adds  r6, #1
adds  r7, #1
cmp   r5, #0
  
```

Tags

Bookmarks Tags Tag Types

Location	Preview

Symbols

- AES\_init\_ctx
- AES\_ECB\_encrypt**
- AES\_ECB\_decrypt
- base64\_encode
- num\_strchr
- base64\_decode
- base64\_get\_encode\_len
- base64\_get\_decode\_len
- \_\_aeabi\_uidiv
- sub\_4710
- \_\_aeabi\_uidivmod
- \_\_divsi3
- sub\_47a4
- \_\_aeabi\_idivmod
- \_\_aeabi\_ldiv0
- sub\_4860
- sub\_4876
- sub\_48e4
- sub\_4014

Selection: 0x4020 to 0x4022 (0x2 bytes) ELF Graph Options

# Next steps



- Decrypt and understand the messages
  - Get the payload from the On/Off sequence
  - Use python to decrypt its content
  - Try to understand the logic
  - Take control of the device