1 Part 2: Awesome Package Konveyance

Well, the task is clear, it's time to extract the APK from the zip file.

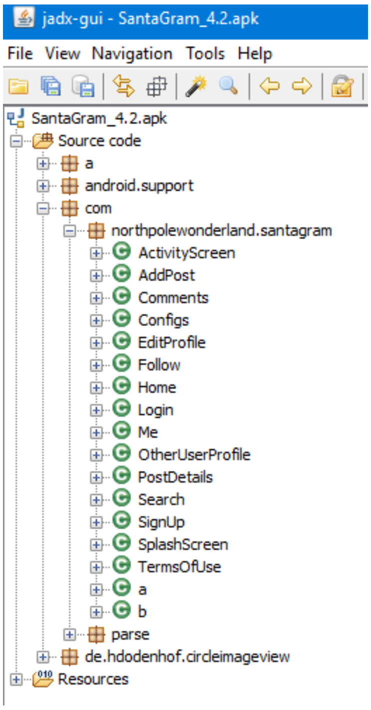
... A minor roadblock, the ZIP file is password protected but a lucky guess that the password is "bugbounty" and the APK is extracted.

Perfect, let us proceed.

1.1 What username and password are embedded in the APK file?

The right tool to answer this question seems to be jadx[1] this is also the tool suggested by one of the elves, Shinny Upatree.

With the APK opened in jadx, there are a few options as to finding the embedded username and password. Option one, browse through the source code for the application, which can be found in the package "com.northpolewonderland.santagram", this can be seen in Figure 1.

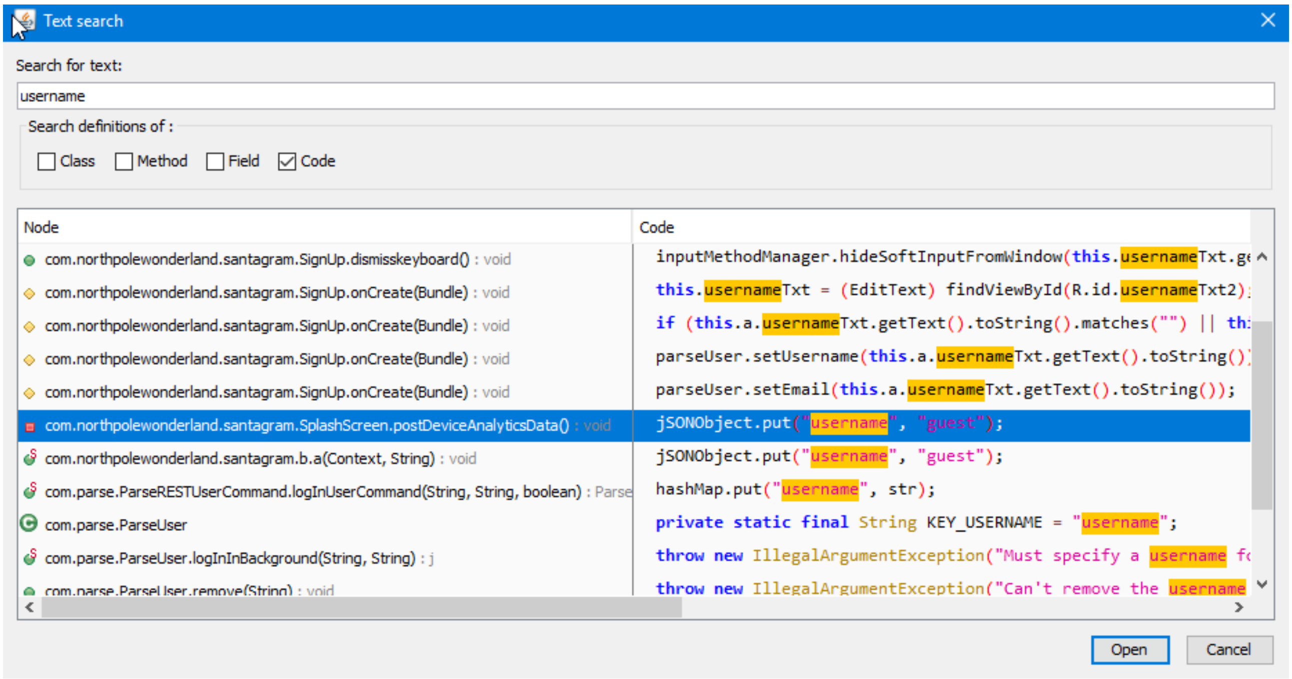


```
SantaGram_4.2.apk
  Source code
    a
    android.support
    com
      northpolewonderland.santagram
        ActivityScreen
        AddPost
        Comments
        Configs
        EditProfile
        Follow
        Home
        Login
        Me
        OtherUserProfile
        PostDetails
        Search
        SignUp
        SplashScreen
        TermsOfUse
        a
        b
      parse
    de.hdodenhof.circleimageview
  Resources
```

Figure 1: jadx package explorer of SantaGram

Or, and personally I like this better, perhaps try and get lucky and use the search feature to search for "username". The results of this search can be seen in Figure 2 and shows that there indeed is a username present.

[1] The GitHub repository can be found at https://github.com/skylot/jadx.



Search for text:

username

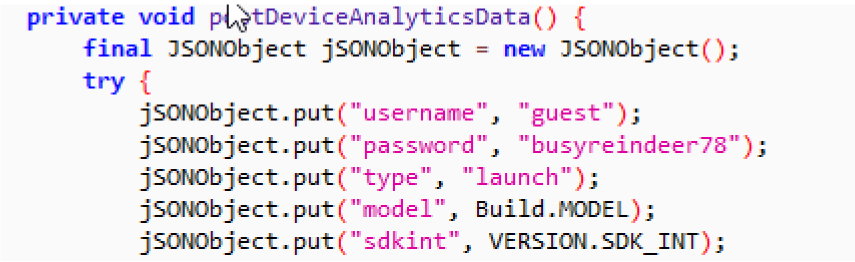
Search definitions of :

□ Class □ Method □ Field ☑ Code

Node	Code
com.northpolewonderland.santagram.SignUp.dismisskeyboard() : void	inputMethodManager.hideSoftInputFromWindow(this.usernameTxt.ge
com.northpolewonderland.santagram.SignUp.onCreate(Bundle) : void	this.usernameTxt = (EditText) findViewById(R.id.usernameTxt2);
com.northpolewonderland.santagram.SignUp.onCreate(Bundle) : void	if (this.a.usernameTxt.getText().toString().matches("") || thi
com.northpolewonderland.santagram.SignUp.onCreate(Bundle) : void	parseUser.setUsername(this.a.usernameTxt.getText().toString()
com.northpolewonderland.santagram.SignUp.onCreate(Bundle) : void	parseUser.setEmail(this.a.usernameTxt.getText().toString());
com.northpolewonderland.santagram.SplashScreen.postDeviceAnalyticsData() : void	jSONObject.put("username", "guest");
com.northpolewonderland.santagram.b.a(Context, String) : void	jSONObject.put("username", "guest");
com.parse.ParseRESTUserCommand.logInUserCommand(String, String, boolean) : Parse	hashMap.put("username", str);
com.parse.ParseUser	private static final String KEY_USERNAME = "username";
com.parse.ParseUser.logInInBackground(String, String) : j	throw new IllegalArgumentException("Must specify a username fo
com.parse.ParseUser.remove(String) : void	throw new IllegalArgumentException("Can't remove the username

Figure 2: jadx search results

Time to open the SplashScreen file to take a closer look, and you wouldn't have guessed it, but alongside that username,there is also a password. Check Figure 3 and have a look for yourself.



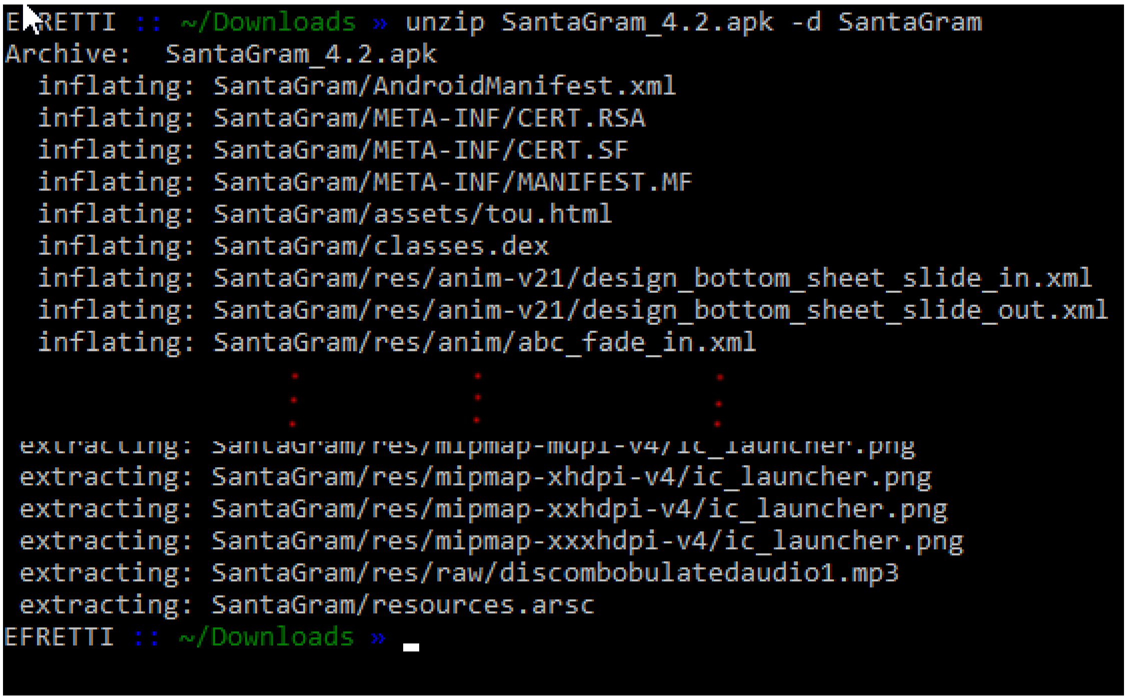
```
private void postDeviceAnalyticsData() {
    final JSONObject jSONObject = new JSONObject();
    try {
        jSONObject.put("username", "guest");
        jSONObject.put("password", "busyreindeer78");
        jSONObject.put("type", "launch");
        jSONObject.put("model", Build.MODEL);
        jSONObject.put("sdkint", VERSION.SDK_INT);
```

Figure 3: jadx SplashScreen

So there we have it, the embedded username and password.

1.2 What is the name of the audible component (audio file) in the SantaGram APK file?

Right, okay. So to get to the audio file inside the APK, let's unpack it, it's basically a ZIP file. Now this is another part were I happened to get very lucky. Check out Figure 4 to see why.



```
EFRETTI :: ~/Downloads » unzip SantaGram_4.2.apk -d SantaGram
Archive:  SantaGram_4.2.apk
  inflating: SantaGram/AndroidManifest.xml
  inflating: SantaGram/META-INF/CERT.RSA
  inflating: SantaGram/META-INF/CERT.SF
  inflating: SantaGram/META-INF/MANIFEST.MF
  inflating: SantaGram/assets/tou.html
  inflating: SantaGram/classes.dex
  inflating: SantaGram/res/anim-v21/design_bottom_sheet_slide_in.xml
  inflating: SantaGram/res/anim-v21/design_bottom_sheet_slide_out.xml
  inflating: SantaGram/res/anim/abc_fade_in.xml
                  .          .              .
                  .          .              .
                  .          .              .
 extracting: SantaGram/res/mipmap-mdpi-v4/ic_launcher.png
 extracting: SantaGram/res/mipmap-xhdpi-v4/ic_launcher.png
 extracting: SantaGram/res/mipmap-xxhdpi-v4/ic_launcher.png
 extracting: SantaGram/res/mipmap-xxxhdpi-v4/ic_launcher.png
 extracting: SantaGram/res/raw/discombobulatedaudio1.mp3
 extracting: SantaGram/resources.arsc
EFRETTI :: ~/Downloads » _
```

Figure 4: Unzipping the SantaGram APK.

As you can see, the second last line actually shows the file that we're looking for. To make sure, I did scroll through all of the output of the 'unzip' command.

But there we have it folks, another challenge down.