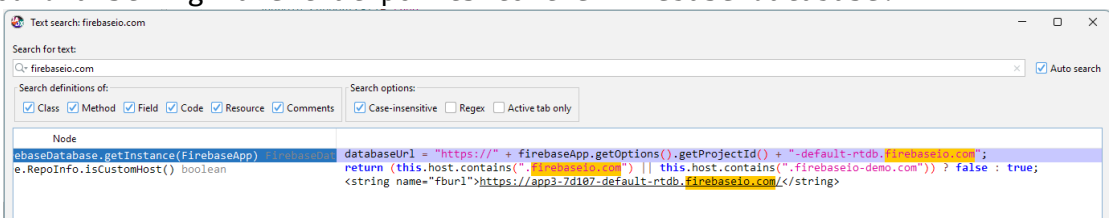
ANDROID

Fire in the base camp

1. **Using JADX**: We started by using **JADX** to decompile the app and followed the **MainActivity class.**

```
    /* JADX INFO: Access modifiers changed from: protected */
    @Override // androidx.fragment.app.FragmentActivity, androidx.activity.ComponentActivity, androidx.core.app.ComponentActivity, android.app.A
29  public void onCreate(Bundle bundle) {
30      super.onCreate(bundle);
31      setContentView(C0496R.layout.activity_main);
32      this.diceimg = (ImageView) findViewById(C0496R.id.dimg);
33      this.dicetext = (TextView) findViewById(C0496R.id.dtext);
34      this.rollbut = (Button) findViewById(C0496R.id.rbut);
35      this.mDatabase = FirebaseDatabase.getInstance().getReference();
36      this.path1 = getResources().getString(C0496R.string.fb4).substring(0, 7);
37      this.path2 = getResources().getString(C0496R.string.fb3).substring(10, 15);
38      this.path3 = getResources().getString(C0496R.string.fb4).substring(18, 21);
39      this.path4 = getResources().getString(C0496R.string.fb2).substring(16, 20);
40      this.path5 = getResources().getString(C0496R.string.fb1).substring(12, 17);
43      final String[] stringArray = getResources().getStringArray(C0496R.array.numbers);
        final int[] iArr = {C0496R.drawable.dice1, C0496R.drawable.dice2, C0496R.drawable.dice3, C0496R.drawable.dice4, C0496R.drawable.dice5, C
45      this.rollbut.setOnClickListener(new View.OnClickListener() { // from class: com.example.app3.MainActivity.1
            @Override // android.view.View.OnClickListener
47          public void onClick(View view) {
48              Integer num = MainActivity.this.count;
                MainActivity mainActivity = MainActivity.this;
                mainActivity.count = Integer.valueOf(mainActivity.count.intValue() + 1);
                int random = (((int) (Math.random() * 6.0d)) + 1) - 1;
50              MainActivity.this.dicetext.setText(stringArray[random]);
51              MainActivity.this.diceimg.setImageResource(iArr[random]);
52              if (MainActivity.this.count.intValue() == 9999999) {
19                  MainActivity.this.mDatabase.child(MainActivity.this.path1 + MainActivity.this.path2 + MainActivity.this.path3 + MainActivity
                        @Override // com.google.android.gms.tasks.OnCompleteListener
55                      public void onComplete(Task<DataSnapshot> task) {
56                          if (!task.isSuccessful()) {
58                              Toast.makeText(MainActivity.this, "Oops Something went wrong", 0).show();
                            } else {
61                              Toast.makeText(MainActivity.this, "Congratulations!! You know where the flag is.", 0).show();
                            }
```

2. **Finding Firebase Database**: In the decompiled code, we discovered that a Firebase database is used. We searched for the string firebaseio.com and found a string name that points to the Firebase database.



3. **Identifying Database Entries**: By navigating to this string, we found four entries in the Firebase database labeled fb1, fb2, fb3, and fb4.

```
<string name="fb1">/is/this/the/flag</string>
<string name="fb2">/i/think/this/is/the/one</string>
<string name="fb3">/seriously/give/me/the/flag/now</string>
<string name="fb4">/please/give/it/to/me</string>
<string name="fburl">https://app3-7d107-default-rtdb.firebaseio.com/</string>
```

4. **Determining the Correct Path**: The substring in ***MainActivity*** provided the correct path to access the Firebase data.

5. **Crafting the URL**: With the correct path information, we crafted our URL to navigate directly to the relevant entries in the Firebase database.

Code (Python)

```
import os
import json

resources = {
    "fb1": "/is/this/the/flag",
    "fb2": "/i/think/this/is/the/one",
    "fb3": "/seriously/give/me/the/flag/now",
    "fb4": "/please/give/it/to/me"
}

path1 = resources["fb4"][0:7]
path2 = resources["fb3"][10:15]
path3 = resources["fb4"][18:21]
path4 = resources["fb2"][16:20]
path5 = resources["fb1"][12:17]

result = path1 + path2 + path3 + path4 + path5 + '.json'
url = 'https://app3-7d107-default-rtdb.firebaseio.com' + result
print("Final URL:", url)
response = os.popen(f"curl {url}").read()
data = json.loads(response)
extracted_values = [value for key, value in data.items()]
final_result = ''.join(extracted_values)

print("Combined Result:", final_result)
```

```
┌──(osiris㉿ALICE)-
[~/Downloads/CTF/IRONCTF/android/Fire_in_the_base_camp]
└─$ python firecampSolver.py
Final URL: https://app3-7d107-default-
rtdb.firebaseio.com/please/give/me/the/flag.json
Combined Result:
ironCTF{y0u_pu7_0u7_th3_f1r3_1n_th3_b4s3_c4mp_1f84a5c66ff5}
```

Flag: ironCTF{y0u_pu7_0u7_th3_f1r3_1n_th3_b4s3_c4mp_1f84a5c66ff5}