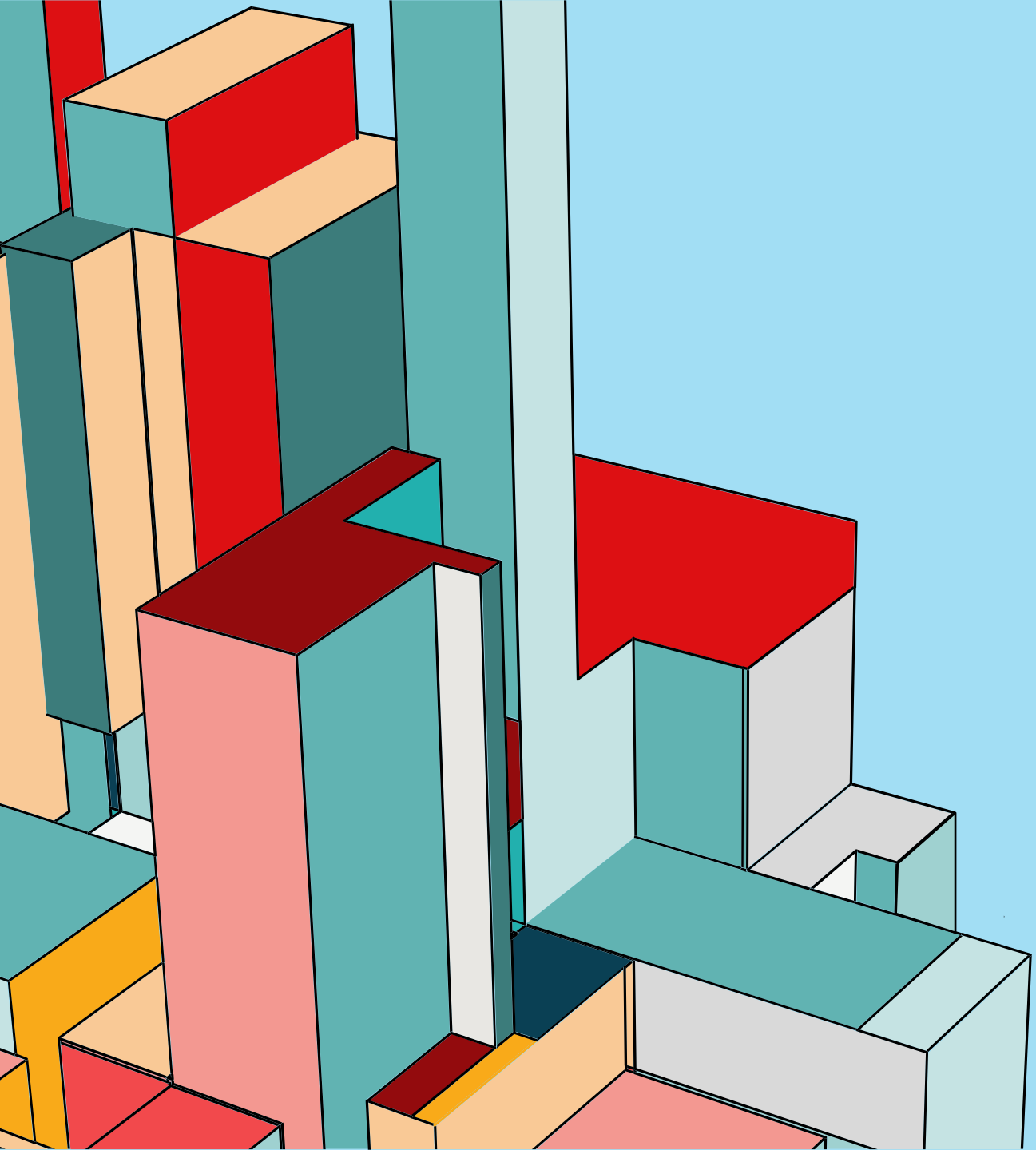
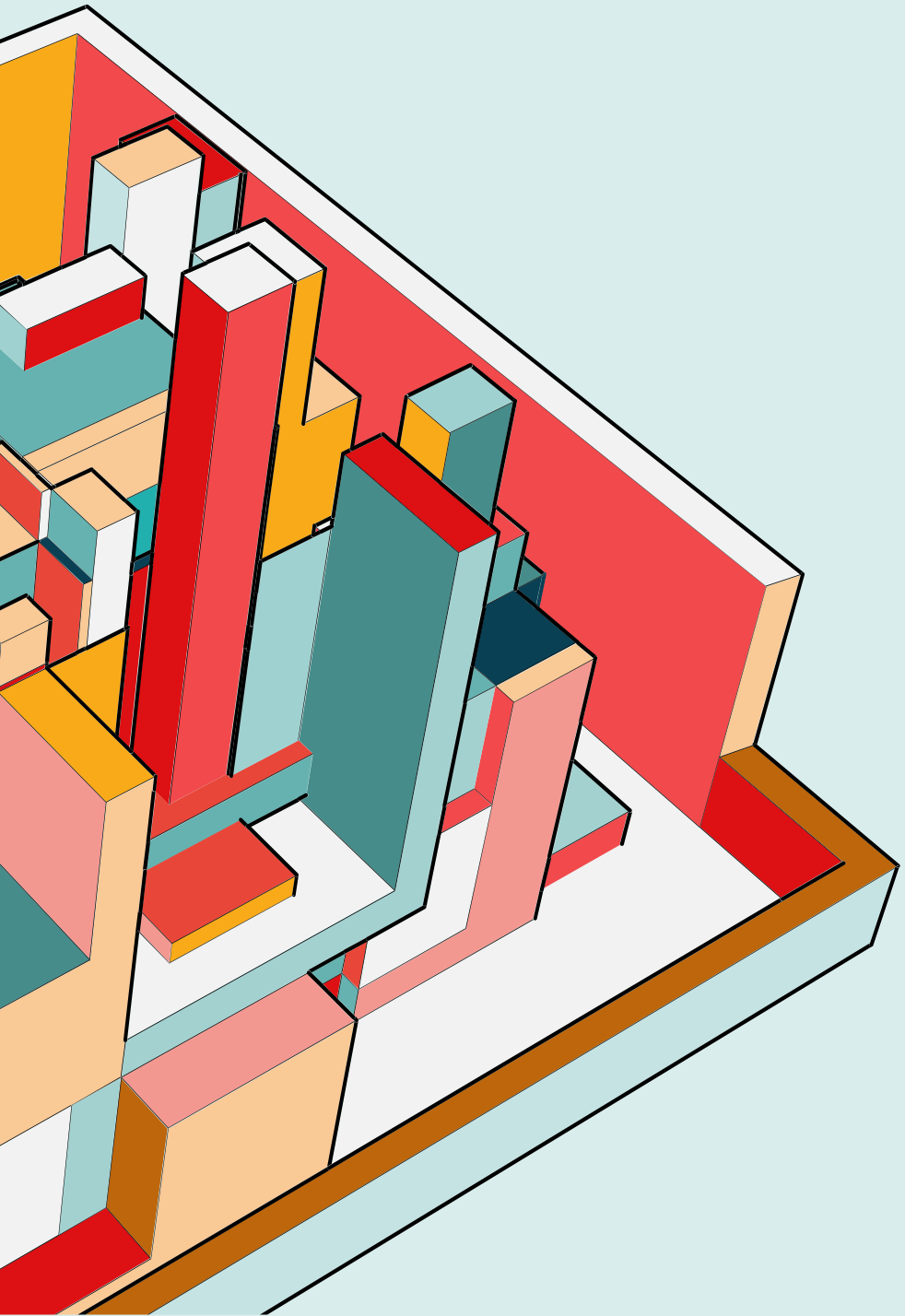
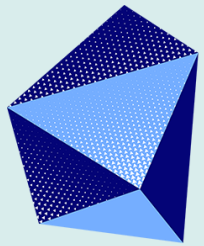



MOB4MOBS



ABOUT ME

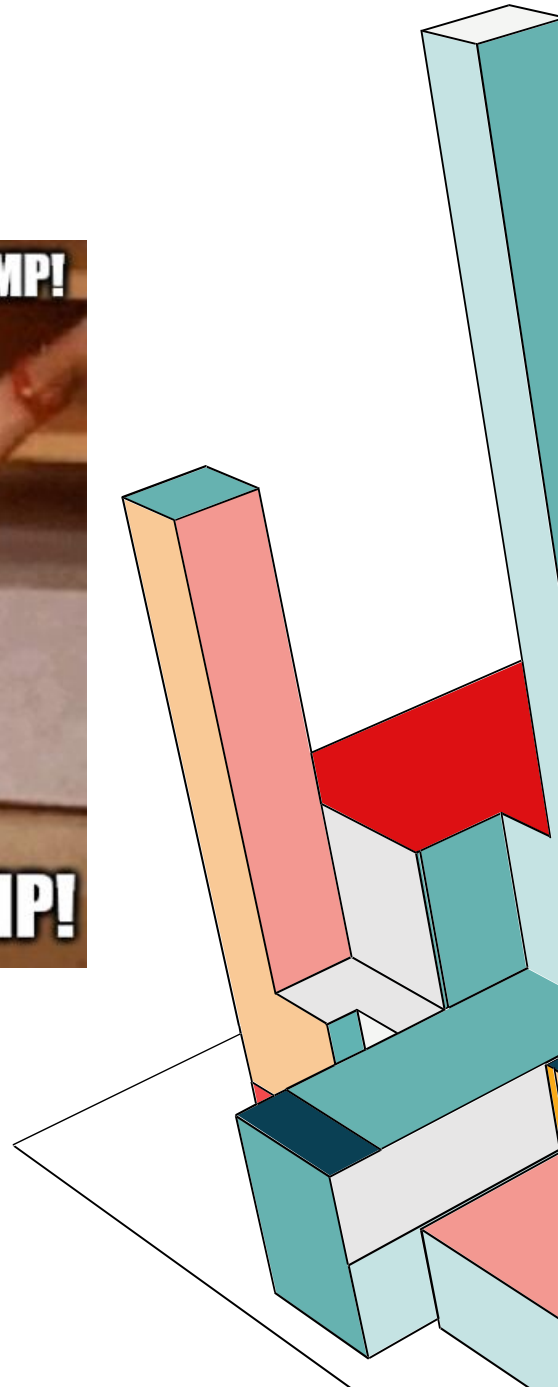
Security, Testing and Assurance @



CyberCX

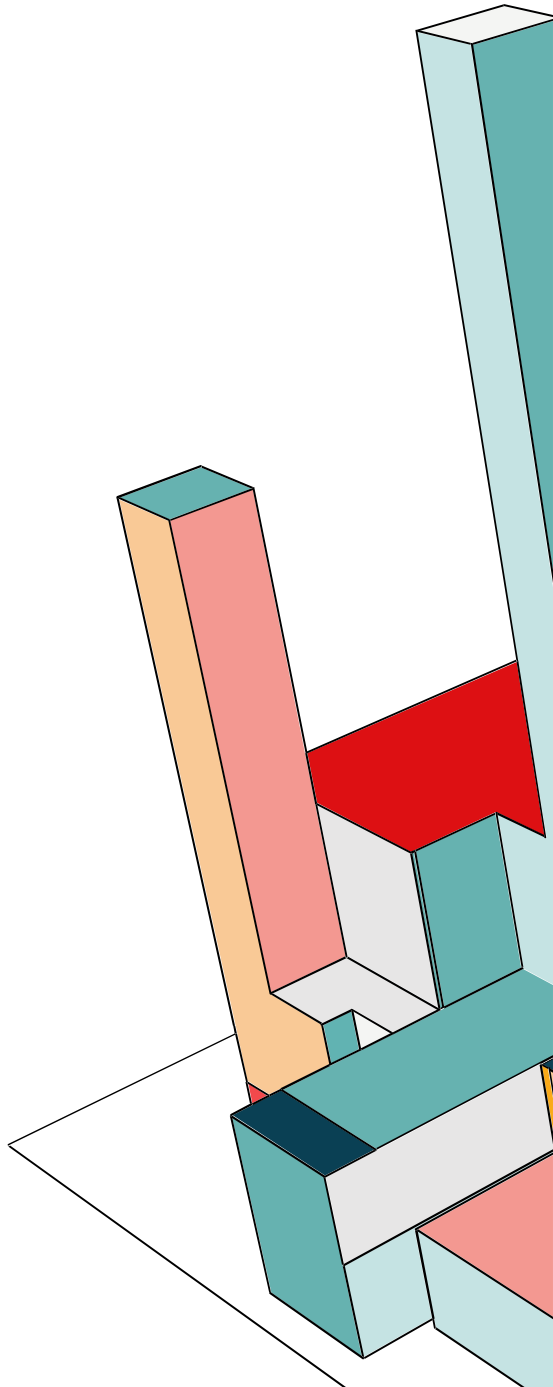
WHAT WE'RE GONNA DO

- Rules of Engagement
- What's An App Anyway?
- Taking Note
- slaoG chtertS
- Where Do You Go From Here?

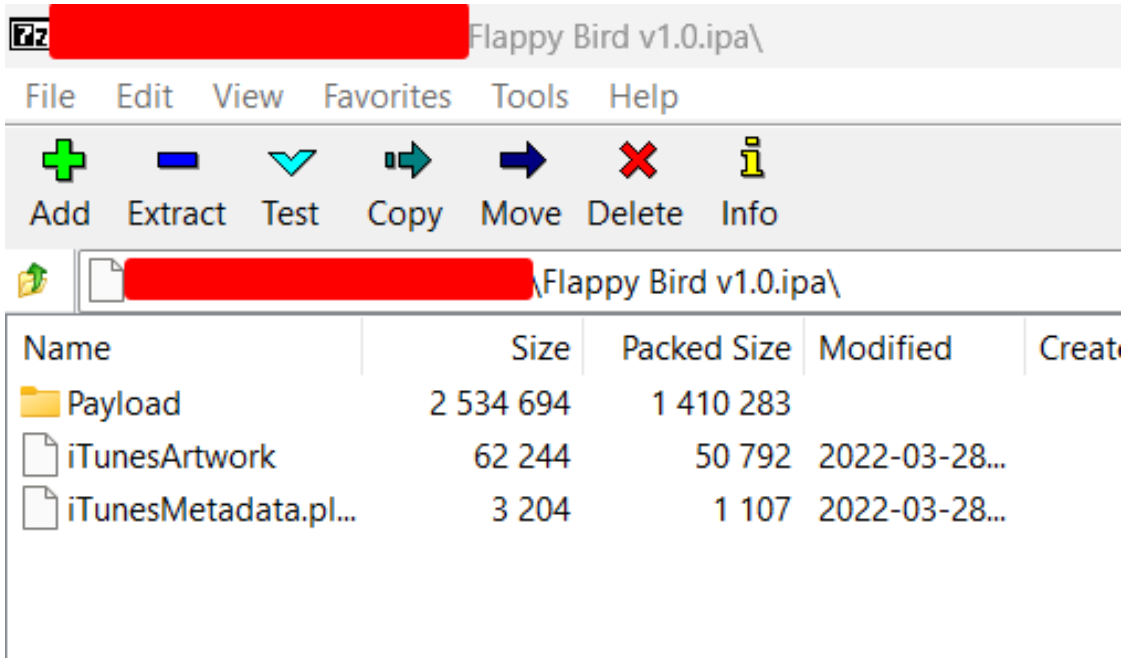


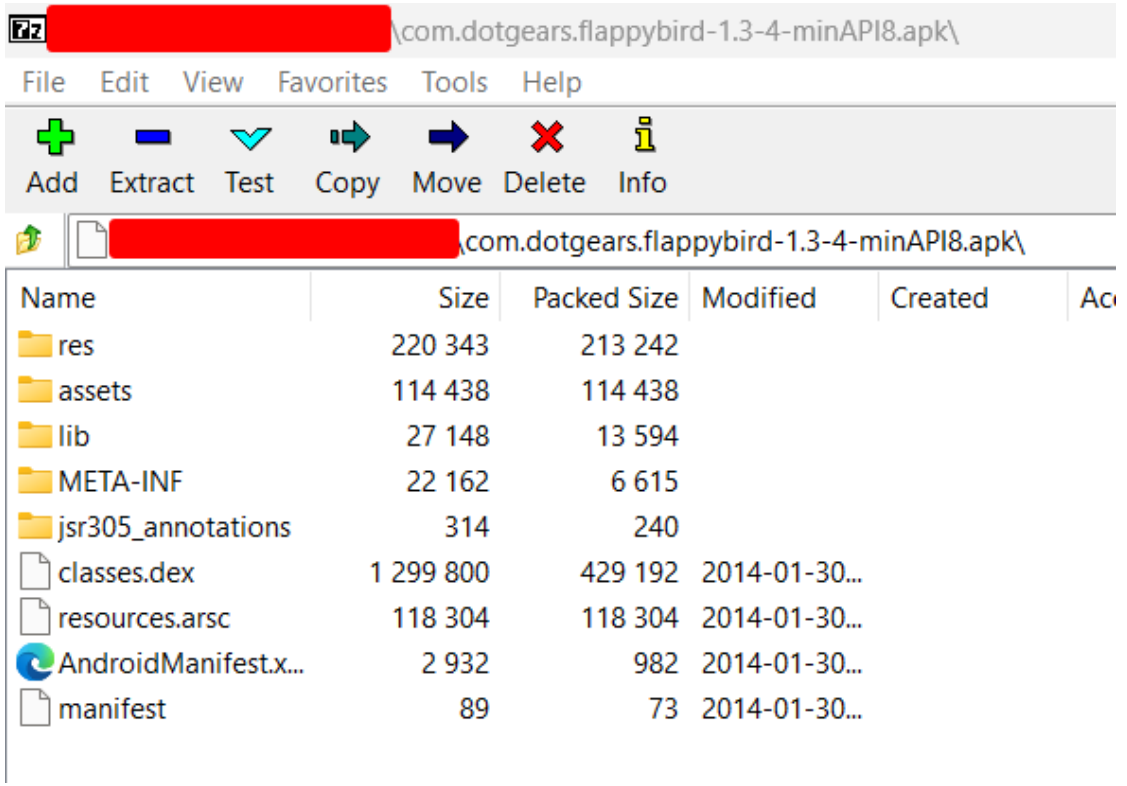
HTTPS://JOE-DS.GITHUB.IO/MOB4MOBS

- Do anything to the app on your device: it can't even talk to the Internet.
- DO NOT attack github.io. The one challenge that has a solution on the site does not need an automated tool.
- You can use your Android device (if you trust me…) or *an* Android device or the freely available Android Studio.
- You do not need to root or jailbreak anything.
- The only person you are competing with is yourself: don't jump on it during any of the talks! Take it home, and enjoy the event instead!



ZIPS AND LINUXES (SORTA) || WEB APPS++





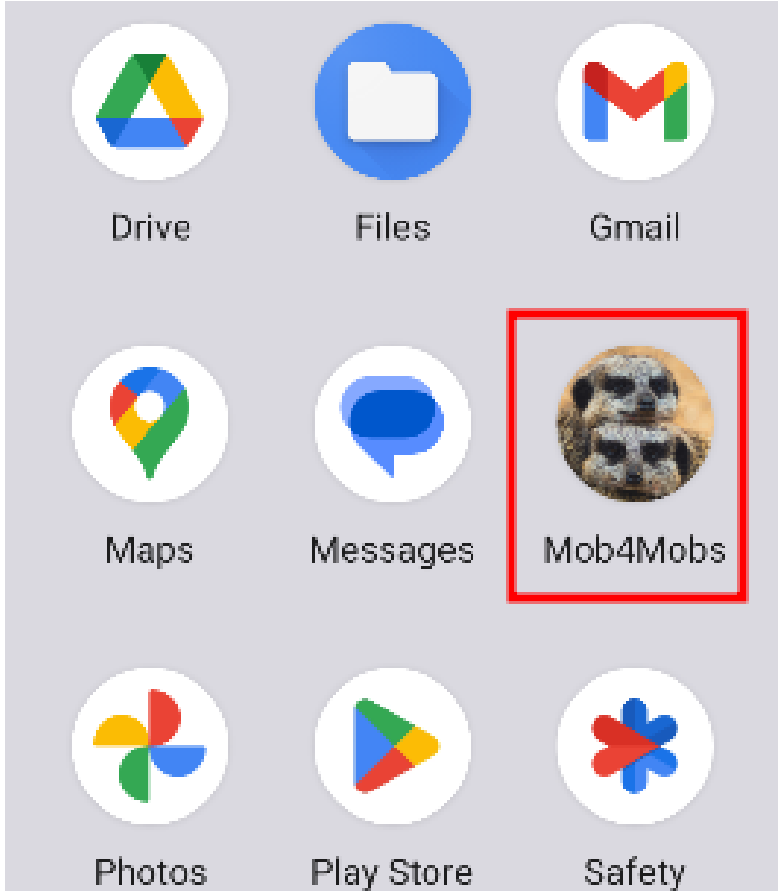
DECOMPILERS (YES, YOU'LL NEED THEM)

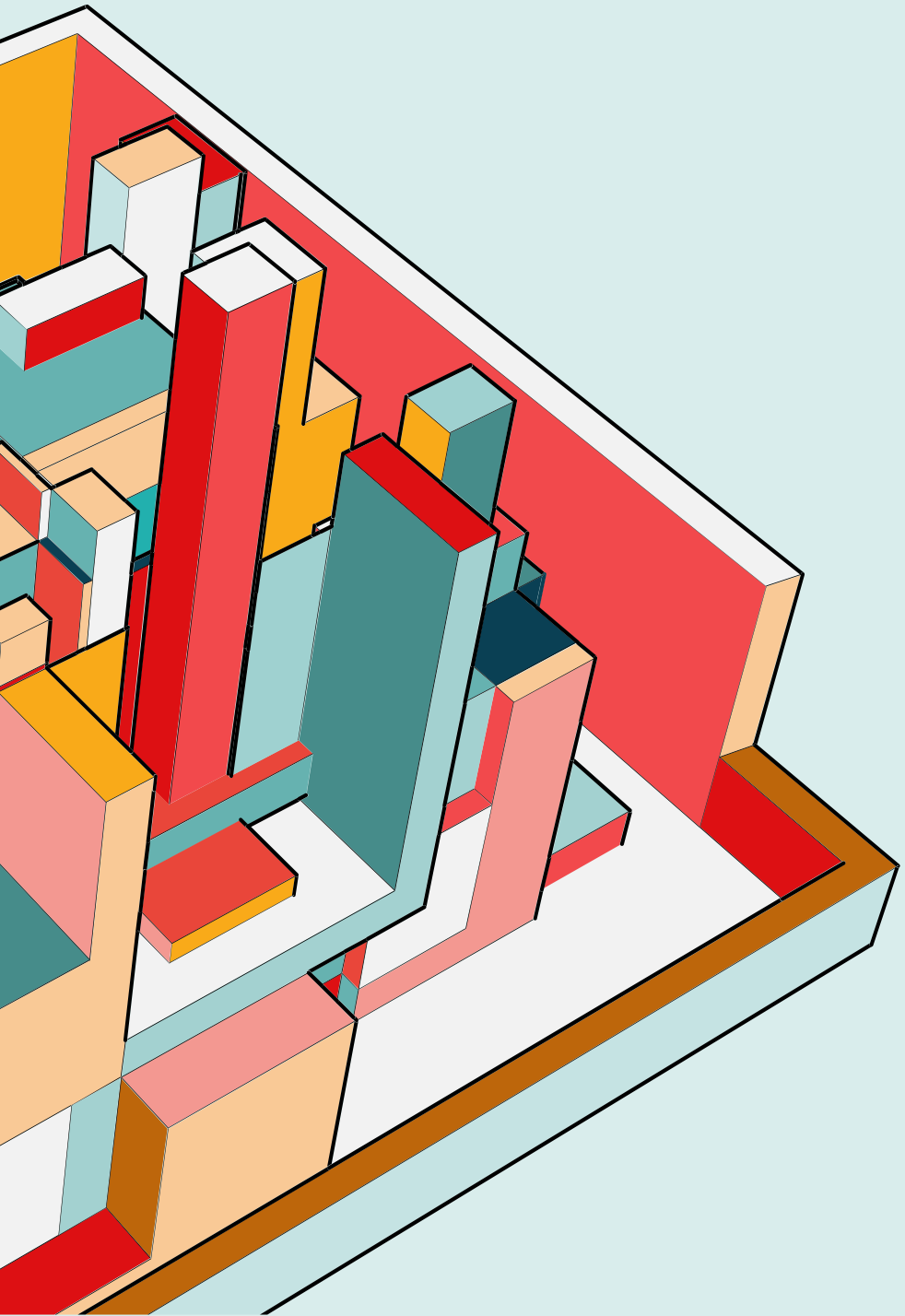
A CHALLENGE FOR THE INF-MINDED

“If I had a mobile app associated with the site, one Android and one iOS, how could you potentially find out? You’d look in a… well known… location.”

CH-CH-CHALLENGES!

- Grab the APK from https://joe-ds.github.io/mob4mobs
- If you are really struggling, you can grab the source code from https://github.com/joe-ds/mob4mobs.
- But I don't recommend doing that, even though Java is ugly and Kotlin is not. Get used to reading decompiled output.
- *I really hope at least some of you understand why there are so many meerkats…*



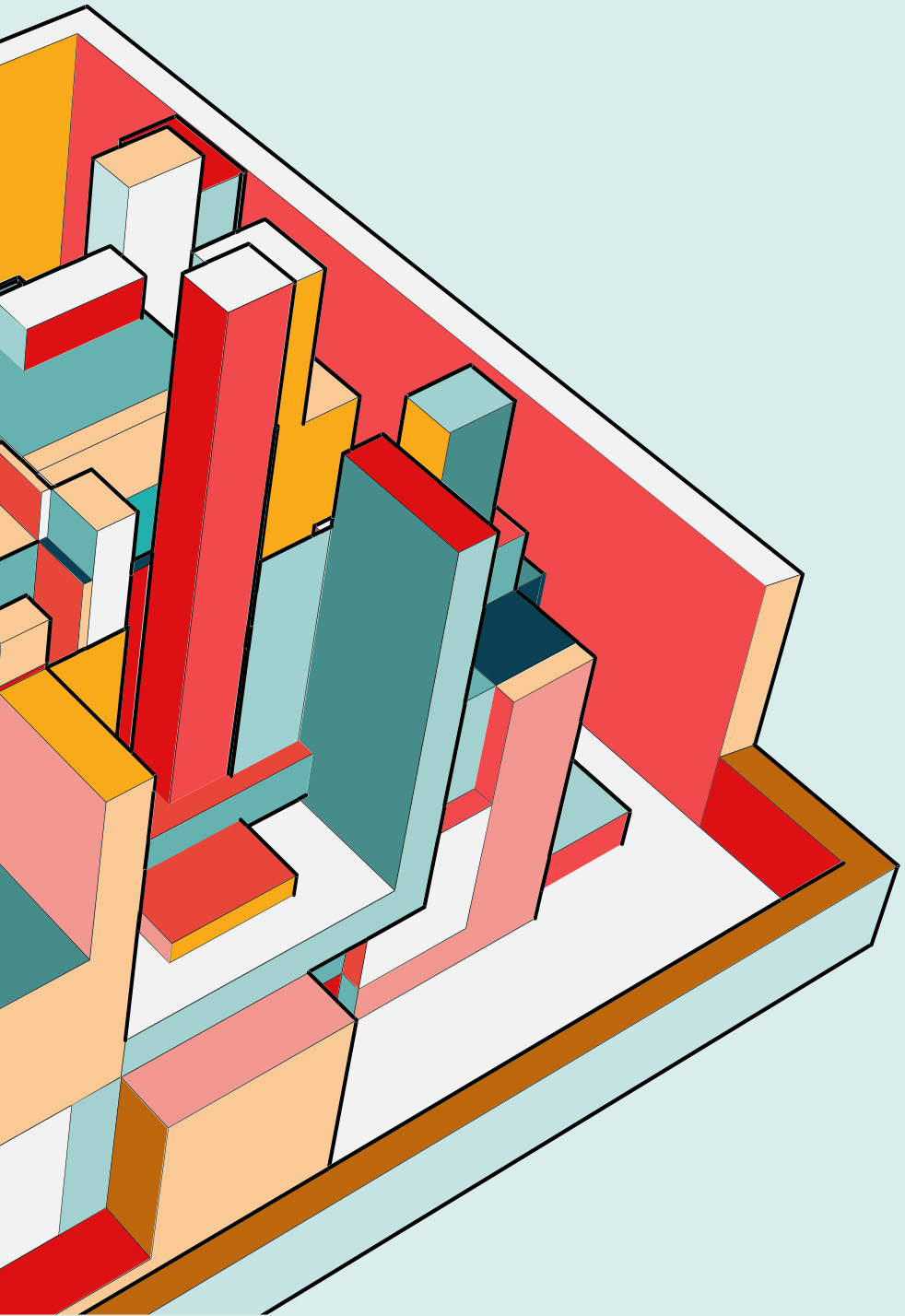


Mob4Mobs Secure Notes

What's your note called?

test

Search

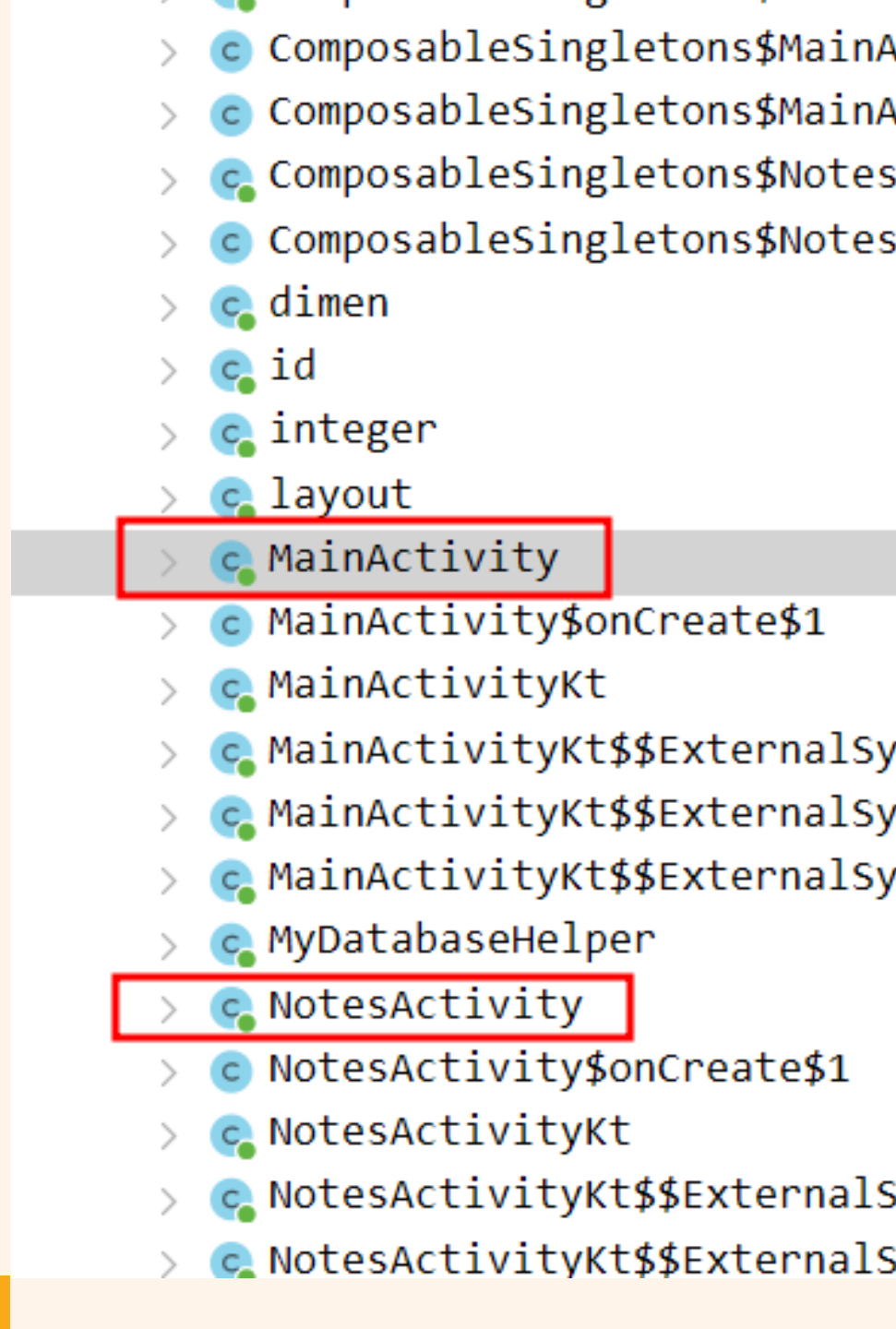


Viewing note: test

Enter password to decrypt (optional)

This is a test note.

ACTIVITIES


ComposableSingletons$MainA
ComposableSingletons$MainA
ComposableSingletons$Notes
ComposableSingletons$Notes
dimen
id
integer
layout
MainActivity
MainActivity$onCreate$1
MainActivityKt
MainActivityKt$$ExternalSy
MainActivityKt$$ExternalSy
MainActivityKt$$ExternalSy
MyDatabaseHelper
NotesActivity
NotesActivity$onCreate$1
NotesActivityKt
NotesActivityKt$$ExternalS
NotesActivityKt$$ExternalS

A Clue

```
import android.database.sqlite.SQLiteDatabase
import android.database.sqlite.SQLiteOpenHelper
```

WHERE'S THE REST?

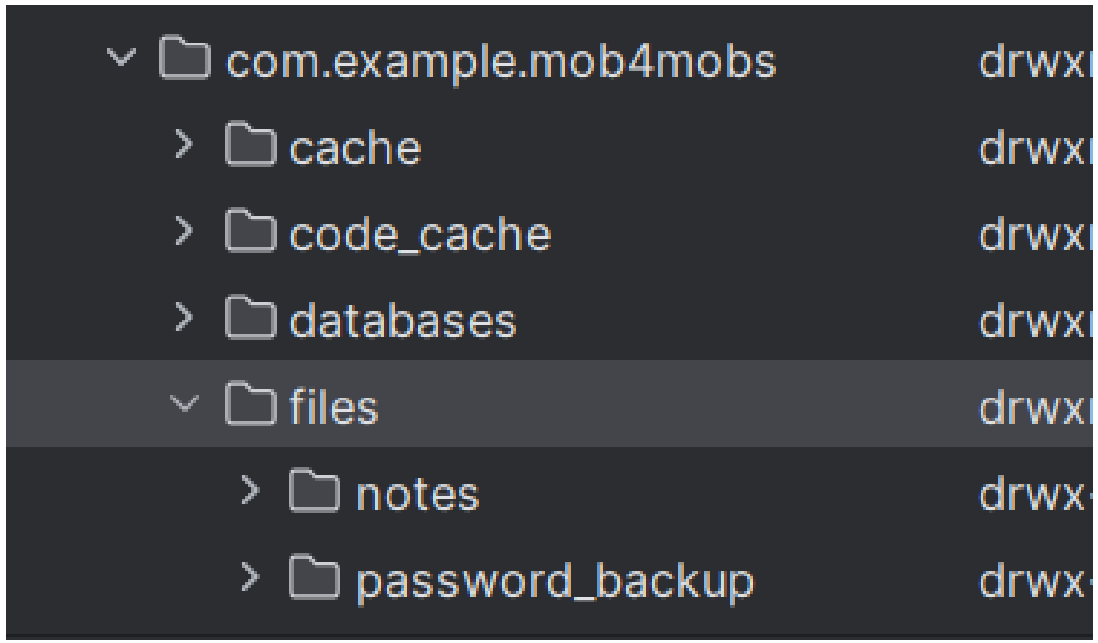
"Find the other notes."

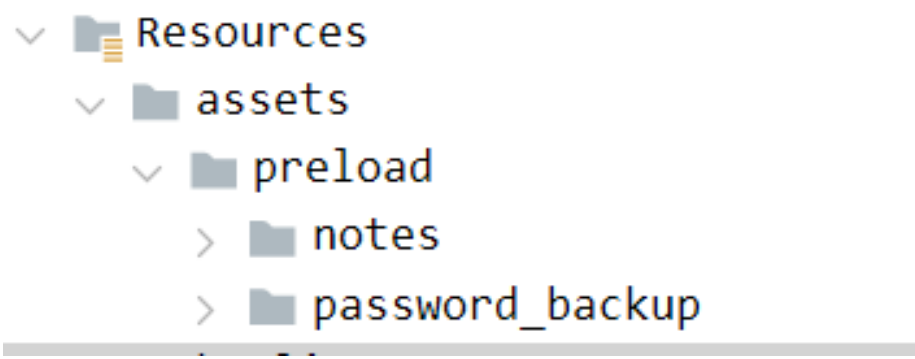
WHERE'S THE REST?

```
public static final String getMatchingNote(MyDatabaseHelper dbHelper, String query) {
    Intrinsics.checkNotNullParameter(dbHelper, "dbHelper");
    Intrinsics.checkNotNullParameter(query, "query");
    SQLiteDatabase db = dbHelper.getReadableDatabase();
    String rawQuery = "SELECT * FROM notes WHERE note = '" + query + "'";
    String result = null;
    Cursor cursor = db.rawQuery(rawQuery, null);
    Intrinsics.checkNotNullExpressionValue(cursor, "rawQuery(...)");
    if (cursor.moveToFirst()) {
        result = cursor.getString(cursor.getColumnIndexOrThrow(MyDatabaseHelper.COLUMN_NAME));
    }
    cursor.close();
    return result;
```

Joe @ CyberCX

DYNAMIC OR STATIC? YOU CHOOSE (DO BOTH!)





DECRYPT

“Decrypt the notes that have stored passwords.”

LOOK, MA, NO SHELL!

AndroidManifest.xml

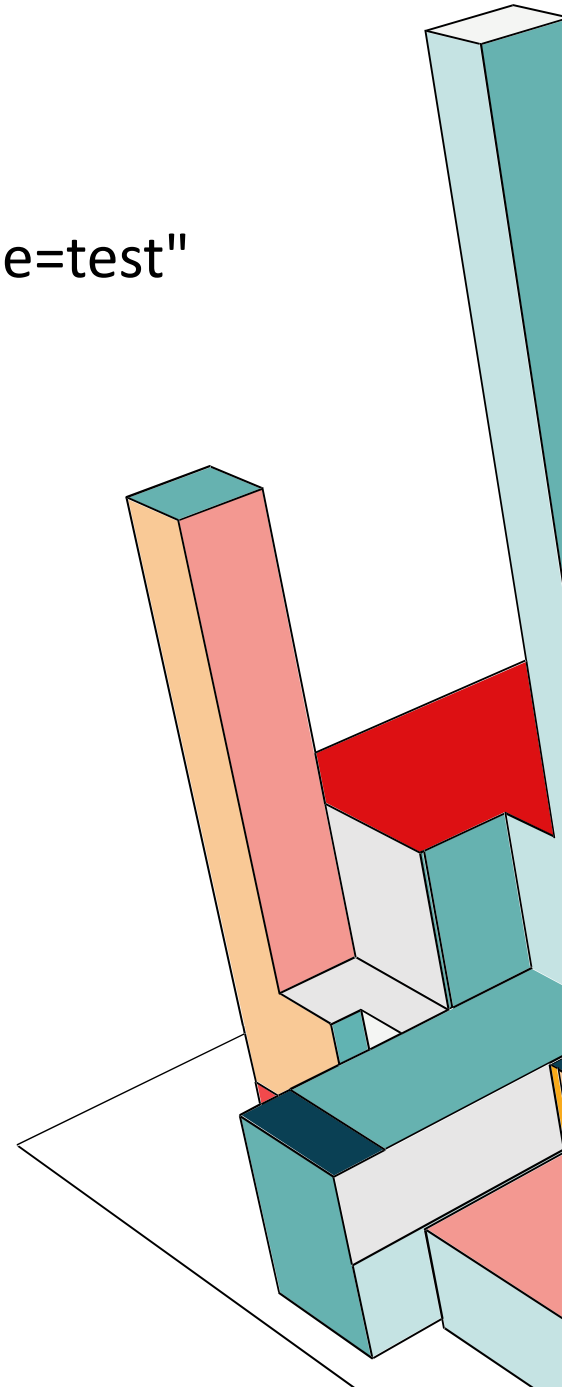
```
29          <activity
                android:theme="@style/Theme.Mob4Mobs"
                android:label="@string/title_activity_notes"
                android:name="com.example.mob4mobs.NotesActivity"
                android:exported="true">
34              <intent-filter>
35                  <action android:name="android.intent.action.VIEW"/>
37                  <category android:name="android.intent.category.DEFAULT"/>
38                  <category android:name="android.intent.category.BROWSABLE"/>
40                  <data
                        android:scheme="mob4mobs"
                        android:host="note"/>
34              </intent-filter>
29          </activity>
```

```
        super.onCreate(savedInstanceState);
        new Utils().setupChallengeFiles(this);
        Intent intent = getIntent();
        if ((intent == null || (data = intent.getData()) == null || (rawNoteName
= data.getQueryParameter(HintConstants.AUTOFILL_HINT_NAME)) == null) && (
rawNoteName = getIntent().getStringExtra("note_name")) == null) {
            rawNoteName = "UnknownNote";
        }
```

```
@Deprecated
public static final String AUTOFILL_HINT_NAME = "name";
```

adb shell am start -a android.intent.action.VIEW "mob4mobs://note?name=test"

- adb shell -> Android Debug Bridge Shell command
- AM -> ActivityManager
- -A android.intent.action.VIEW -> Action
- "mob4mobs://note?name=test“ -> URI



SPILL THE BEANS

“Get the app to show you passwords.”

Clues

- Type the password for a note you have decrypted, and add one more character at the end.
- Reverse engineer the decryption function!

SDREN OTPYRC

“There’s one note with no stored password. Crack it!”

WHICH WAY?

Important, faster, but has a ceiling.

- Do CTFs.
- https://www.hextree.io/hextree-x-google
- Do more CTFs.
- Read about exploits.
- https://mas.owasp.org/MASVS/

Slower, but better long term.

- Write your own apps.
- Break your own apps.
- Decompile your apps.
- Scan your apps with tools like MobSF.

Credits

Photo by Anggit Rizkianto on Unsplash

Photo by Pauline Bernfeld on Unsplash

Photo by Daniel Pelaez Duque on Unsplash

THANK YOU

https://infosec.exchange/@joe_ds

https://joe-ds.github.io