

Forum:[Hack Forums](#)

Thread: [Noob needs a push in the right direction - reverse engineer mobile game](#)

snowball_v - April 23, 2018, 10:37 am

I am trying to do some reverse engineering on a game called "Dungeon crusher: soul hunters"
It is available on mobile and as a browser version on sites like Armorgames and Kong.

Specifically, the game has a crafting system where you combine various useless items to get more valuable ones. Many of these crafting recipes are currently unknown and nearly impossible to find with normal gameplay.

So a while ago some unknown individual somehow extracted all recipes available at the time.

His/her contribution looked like this:

Spoiler ([Click to View](#))

Code

```
ID;NameID;IconID;RecipeType;BaseChance;MaxChance;Ingredients;Result;LevelRestrictions;Disco  
veryWeight;IsHidden;IsEnabled
```

```
10;RECIPE_NAME_10;db_bottles;2;0.65;0.99;100000:15,100050:15,100100:15;L:10:(1-5);0;0;0;1
```

```
20;RECIPE_NAME_20;db_bottles;2;0.65;0.99;100150:15,100200:15,100250:15;L:10:(1-5);100;100  
00;0;1
```

```
30;RECIPE_NAME_30;db_bottles;2;0.65;0.99;100300:15,100350:15,100400:15;L:10:(2-6);200;100  
00;0;1
```

```
40;RECIPE_NAME_40;db_bottles;2;0.65;0.99;100500:15,100380:15,100600:15;L:10:(2-6);250;100  
00;0;1
```

```
50;RECIPE_NAME_50;db_bottles;2;0.65;0.99;100650:15,100700:15,100740:15;L:10:(3-6);450;100  
00;0;1
```

```
55;RECIPE_NAME_50;db_bottles;2;0.95;1;104000:5;L:10:(3-6);450;10000;0;1
```

```
60;RECIPE_NAME_50;db_bottles;2;0.95;1;104005:5;L:10:(3-6);450;10000;0;1
```

```
100;RECIPE_NAME_100;pvp_expendables_button_icon_dpc;2;0.95;1;100020:5, 100590:6,  
100190:3, 100700:5, 100730:5, 100680:3;L:80;0;10000;0;1
```

```
101;RECIPE_NAME_100;pvp_expendables_button_icon_dpc;2;0.95;1;100400:5, 100120:6,  
100110:5, 100080:5, 100560:4, 100030:5;L:80;0;20000;0;1
```

```
102;RECIPE_NAME_100;pvp_expendables_button_icon_dpc;2;0.95;1;100070:6, 100590:3,  
100580:5, 100390:6, 100030:5, 100520:5;L:80;0;20000;0;1
```

[...]

```
200;RECIPE_NAME_200;db_shards_nobg;2;0.7;0.99;100160:10, 100280:8,  
100080:10;L:30:(2-5);100;1000;0;1
```

```
201;RECIPE_NAME_201;db_shards_nobg;2;0.7;0.99;100740:5, 100690:5,  
100340:5;L:30:1;0;20000;0;1
```

```
205;RECIPE_NAME_205;db_hearts_1;2;0.75;0.99;100110:8, 100120:6,  
100130:8;L:50:(15-30);100;1000;0;1
```

```
206;RECIPE_NAME_206;db_hearts_1;2;0.75;0.99;100720:2, 100670:2,  
100320:2;L:50:(4-6);0;20000;0;1
```

```
210;RECIPE_NAME_210;db_guild_points;2;0.7;0.99;100410:15, 100070:15,  
100030:15;L:40;100;1000;0;1
```

```
300;RECIPE_NAME_300;db_heroshard_ids_16_black_dragon;2;0.8;0.99;105190:15, 100640:8,
```

100210:10, 100590:11, 100310:9, 100700:7;L:10380:(1-3);300;5000;0;1
310;RECIPE_NAME_310;db_heroshard_lds_17_tesla;2;0.8;0.99;105190:15, 100130:8, 100730:7,
100360:8, 100700:12, 100000:10;L:10390:(1-3);300;5000;0;1
320;RECIPE_NAME_320;db_heroshard_lds_18_snow_queen;2;0.8;0.99;105190:15, 100320:8,
100690:10, 100670:11, 100190:7, 100560:10;L:10400:(1-3);300;5000;0;1
[...]
1000;RECIPE_NAME_1000;UI_loot_liquid_01;2;0.95;1;100150:5,
100250:5;L:100300:5;0;10000;0;1
1001;RECIPE_NAME_1001;UI_loot_liquid_02;2;0.95;1;100160:5,
100260:5;L:100310:5;0;10000;0;1
1002;RECIPE_NAME_1002;UI_loot_liquid_03;2;0.95;1;100170:5,
100270:5;L:100320:5;0;10000;0;1
1003;RECIPE_NAME_1003;UI_loot_liquid_04;2;0.95;1;100180:5,
100280:5;L:100330:5;0;10000;0;1
1004;RECIPE_NAME_1004;UI_loot_liquid_05;2;0.95;1;100190:5,
100290:5;L:100340:5;0;10000;0;1
1010;RECIPE_NAME_1010;UI_loot_sphere_01;2;0.95;1;100500:6, 100300:1,
100620:2;L:100650:5;0;10000;0;1
1011;RECIPE_NAME_1011;UI_loot_sphere_02;2;0.95;1;100510:6, 100310:1,
100620:2;L:100660:5;0;10000;0;1
[...]
2420;EQUIP_110229_NAME;UI_loot_w_arrow_01;2;0.75;0.99;100820:10,
105020:10;L:110229:(5-10);0;10000;0;1
2425;EQUIP_110318_NAME;UI_loot_w_spear_01;2;0.75;0.99;100660:3, 100610:1, 105090:5,
105000:1, 105020:1, 105030:1;L:110318:1;0;10000;0;1
3000;ITEM_105000_NAME;UI_loot_item_anvil;2;0.75;0.99;105090:5,
100500:1;L:105000:1;0;10000;0;1

3010;ITEM_105010_NAME;UI_loot_item_part_armor_01;2;0.75;0.99;110000:1;L:105010:1;150;100
00;0;0

3011;ITEM_105010_NAME;UI_loot_item_part_armor_01;2;0.75;0.99;110040:1;L:105010:1;150;100
00;0;0
[...]
3200;RECIPE_NAME_3200;UI_recipe_armor;2;0.75;0.99;105000:1, 105050:10, 105010:10,
100400:10, 100420:10, 100380:10;210000;0;10000;0;1
3210;RECIPE_NAME_3210;UI_recipe_boots;2;0.75;0.99;105000:1, 105050:10, 100400:15,
100420:15, 105010:10;210010;0;10000;1;0
3220;RECIPE_NAME_3220;UI_recipe_helm;2;0.75;0.99;105000:1, 105050:10, 100400:15,
100350:15, 105010:10;210020;0;10000;1;0
3230;RECIPE_NAME_3230;UI_recipe_weapon;2;0.75;0.99;105000:1, 105050:10, 105020:10,
105030:10, 105040:10;210030;0;10000;0;1
3240;ITEM_105210_NAME;UI_loot_craft_bird_01;2;0.75;0.99;100050:1, 100060:1, 100070:1,
100080:1, 100090:1;L:105210:1;0;10000;0;1
3250;ITEM_105220_NAME;UI_loot_craft_bone_01;2;0.75;0.99;100000:1, 100010:1, 100020:1,
100030:1, 100040:1;L:105220:1;0;10000;0;1
3260;ITEM_105230_NAME;UI_loot_craft_fish_01;2;0.75;0.99;100200:1, 100210:1, 100220:1,
100230:1, 100240:1;L:105230:1;0;10000;0;1
3270;ITEM_105240_NAME;UI_loot_craft_stand_01;2;0.75;0.99;100350:1, 100360:1, 100370:1,
100380:1, 100390:1;L:105240:1;0;10000;0;1
3500;ITEM_105190_NAME;db_heroshard_unknown;2;0.75;0.99;10262:5,
105180:1;L:105190:(1-3);0;10000;0;1
3501;ITEM_105190_NAME;db_heroshard_unknown;2;0.75;0.99;10280:5,

```
105180:1;L:105190:(1-3);0;10000;0;1
[...]
6000;ITEM_104000_NAME;UI_loot_event_hlw_spumpkin;2;0.75;0.99;104000:5,
110285:5;L:104001:5;0;10000;0;1
7000;ITEM_105090_NAME;UI_loot_item_ignot_2;2;0.95;1;110000:1,
105200:1;L:105090:(4-10);150;10000;0;1
7010;ITEM_105090_NAME;UI_loot_item_ignot_2;2;0.95;1;110040:1,
105200:1;L:105090:(4-10);150;10000;0;1
[...]
```

No information how this was pulled off, but it was good enough to deduce the ingredients ingame. Since then new recipes were added and they remain unknown.

What I did so far:

I produced a memory dump from the game running on windows in google chrome. And I pulled the apk file from an android phone and extracted it.

Went through the files and found some interesting stuff like png images for currently unknown content...but other than that I am a bit lost where and how to find what I am looking for.

Could you point me in the right direction? I don't even know if I am on the right track with the apk file ?

V3t3r4n - April 23, 2018, 11:02 am

For Android, one of two things could be happening:

They are saving that information on a local database inside the apk. SQLite is usually the one that is used the most. Especially on Android. So you could try looking for a database file inside your extracted apk. Since you mentioned they have a browser version of the game as well, I somehow think this is very unlikely. I think you can't use this on the browser version, Although I don't know enough about browser based video games to know if this is true or not.

The other option, and the one that I find most likely is that they are saving it all server-side. So your best bet would be to install Wireshark and sniff the packets they are sending to the server, and the packets you're receiving from the server to figure out if any important information is being transmitted. (Maybe when you open the menu/shop/npc for crafting, the game might return you the various recipes that exists in the game at that moment. You can use Wireshark and limit it to just the browser, for when you're playing the game in Chrome, or just the App, if you're playing on an Android emulator. They might contain different information...? Although that's very unlikely.

If none of that works, you could start by actually reverse engineering the Android app. Though it's not a very easy thing to do. You should start by installing Android Studio, which is the Google Software used to code Android apps, and installing an appropriate SDK, which is the Android Version (You can pick from a multitude of them). Then you download the game, decompile it, try changing it's manifest (Like a main file with a bunch of rules for the app) to make it debugable (Debugging is the thing developers do to test an app), you digitally sign it yourself (There's a program that does this, and it allows you to trick Android Studio into thinking you made the app, making it debuggable), and then you run it in Android Studio and figure out what it's doing. This can be easier if the developers don't protect their code, which is unlikely. The code that will be given to you will be hard to understand, and you'll need to debug it to figure out what it does. This a very hard and tedious process. Not impossible by any means though :)

Here's an article that explains how to debug an apk in an easier to understand and step-by-step way: <https://blog.netspi.com/attacking-android-applications-with-debuggers/> . This worked for me

when I tried, although that was about 2 years ago. Hopefully not much as changed since then, and all the software mentioned there was appropriately updated to still work today.

Here's a link to Wireshark: <https://www.wireshark.org/> All-around very useful software to figure out what's being sent and received over your network. An invaluable tool when it comes to not only reverse engineering an webservice, but also for security and privacy reasons.

This post is only supposed to provide you with some direction, as you asked for. You should research everything I mentioned for yourself.

Best of Luck! ?

snowball_v - April 23, 2018, 11:30 am

Thanks, this gives me something to work with. Exactly what I was hoping for.
Others can still feel free to add hints ;)

V3t3r4n - April 24, 2018, 3:02 am

(Apr 23, 2018 11:30 AM)snowball_v Wrote: [\[CITE\]](#) Thanks, this gives me something to work with.
Exactly what I was hoping for.

Others can still feel free to add hints ;)

No problem :) Please keep us updated on your progress so far, I'm sure it would be helpful to a lot of people if you could.

BrilliantAdam - April 24, 2018, 12:06 pm

(Apr 23, 2018 11:02 AM)V3t3r4n Wrote: [\[CITE\]](#) For Android, one of two things could be happening:

They are saving that information on a local database inside the apk. SQLite is usually the one that is used the most. Especially on Android. So you could try looking for a database file inside your extracted apk. Since you mentioned they have a browser version of the game as well, I somehow think this is very unlikely. I think you can't use this on the browser version, Although I don't know enough about browser based video games to know if this is true or not.

The other option, and the one that I find most likely is that they are saving it all server-side. So your best bet would be to install Wireshark and sniff the packets they are sending to the server, and the packets you're receiving from the server to figure out if any important information is being transmitted. (Maybe when you open the menu/shop/npc for crafting, the game might return you the various recipes that exists in the game at that moment. You can use Wireshark and limit it to just the browser, for when you're playing the game in Chrome, or just the App, if you're playing on an Android emulator. They might contain different information...? Although that's very unlikely.

If none of that works, you could start by actually reverse engineering the Android app. Though it's not a very easy thing to do. You should start by installing Android Studio, which is the Google Software used to code Android apps, and installing an appropriate SDK, which is the Android Version (You can pick from a multitude of them). Then you download the game, decompile it, try changing it's manifest (Like a main file with a bunch of rules for the app) to make it debugable (Debugging is the thing developers do to test an app), you digitally sign it yourself (There's a program that does this, and it allows you to trick Android Studio into thinking you made the app, making it debuggable), and then you run it in Android Studio and figure out what it's doing. This can be easier if the developers don't protect their code, which is unlikely. The code that will be given to you will be hard to understand, and you'll need to debug it to figure out what it does. This a very hard and tedious process. Not impossible by any means though :)

This post is only supposed to provide you with some direction, as you asked for. You should research everything I mentioned for yourself.

Best of Luck! ?

Thanks so much ! i found this reply very helpful to me too . I'm trying to crack Empires And Allies (by Zynga) . Wish me some luck =) i'm going to follow ur steps , but i have only a one problem . All critical information are encrypted in the HTTP REQUEST and even RESPONSE (i use Burpsuite to interrupt requests on fb gameroom) , Variety of Md5 , Sha1 , Base64 .. and so on are used . I tried to look at the code using (dnSpy) , and i can find many many files called (Hash , HashAssembly , Encryption , .. etc) and many algorithms in c# that i can't identify at all and can't find the main line which controls the whole encryption traffic . Any help / Advice would be greatly appreciated . Warm Regards =)

snowball_v - April 25, 2018, 12:18 pm

So what I did among other things was using il2cppdumper.

It produced a dump file with some interesting information, among other things entries like these:

Code // Namespace: TM.ClickerCore.Models.Craft

public class CraftRecipeEntry : ClickerConfigEntry // TypeDefIndex: 4604

```
{
// Fields
private string <NameID>k__BackingField; // 0x10
private string <IconID>k__BackingField; // 0x14
private RecipeType <Type>k__BackingField; // 0x18
private float <BaseChance>k__BackingField; // 0x1C
private float <MaxChance>k__BackingField; // 0x20
private List`1<Tuple`2<int, int>> <Ingredients>k__BackingField; // 0x24
private LootFormat <Result>k__BackingField; // 0x28
private int <LevelRestrictions>k__BackingField; // 0x2C
private int <DiscoveryWeight>k__BackingField; // 0x30
```

// Methods

```
public void .ctor(); // 0x1105850
public string get_NameID(); // 0x1105858
private void set_NameID(string value); // 0x1105860
public string get_IconID(); // 0x1105868
private void set_IconID(string value); // 0x1105870
public RecipeType get_Type(); // 0x1105878
private void set_Type(RecipeType value); // 0x1105880
public float get_BaseChance(); // 0x1105888
private void set_BaseChance(float value); // 0x1105890
public float get_MaxChance(); // 0x1105898
private void set_MaxChance(float value); // 0x11058A0
public List`1<Tuple`2<int, int>> get_Ingredients(); // 0x11058A8
private void set_Ingredients(List`1<Tuple`2<int, int>> value); // 0x11058B0
public LootFormat get_Result(); // 0x11058B8
private void set_Result(LootFormat value); // 0x11058C0
public int get_LevelRestrictions(); // 0x11058C8
private void set_LevelRestrictions(int value); // 0x11058D0
public int get_DiscoveryWeight(); // 0x11058D8
private void set_DiscoveryWeight(int value); // 0x11058E0
public static CraftRecipeEntry ParseFromTable(string[] row, string[] header, string[] validHeader); // 0x11058E8
```

```
private static List<Tuple<int, int>> ParseIngredients(string value); // 0x1105CB8  
}
```

What can I do with it? I can look up what is in the offsets in global-metadata, but I can not make any sense of it from looking at the file in a hexeditor.

I have to admit, maybe I need more than a gentle push in the right direction ?

V3t3r4n - April 26, 2018, 1:21 am

(Apr 24, 2018 12:06 PM)BrilliantAdam Wrote: [\[CITE\]](#) Thanks so much ! i found this reply very helpful to me too . I'm trying to crack Empires And Allies (by Zynga) . Wish me some luck =) i'm going to follow ur steps , but i have only a one problem . All critical information are encrypted in the HTTP REQUEST and even RESPONSE (i use Burpsuite to interrupt requests on fb gameroom) , Variety of Md5 , Sha1 , Base64 .. and so on are used . I tried to look at the code using (dnSpy) , and i can find many many files called (Hash , HashAssembly , Encryption , .. etc) and many algorithms in c# that i can't identify at all and can't find the main line which controls the whole encryption traffic . Any help / Advice would be greatly appreciated . Warm Regards =)

(Apr 25, 2018 12:18 PM)snowball_v Wrote: [\[CITE\]](#) So what I did among other things was using il2cppdumper.

It produced a dump file with some interesting information, among other things entries like these:

Code // Namespace: TM.ClickerCore.Models.Craft

public class CraftRecipeEntry : ClickerConfigEntry // TypeDefIndex: 4604

```
{  
    // Fields  
    private string <NameID>k__BackingField; // 0x10  
    private string <IconID>k__BackingField; // 0x14  
    private RecipeType <Type>k__BackingField; // 0x18  
    private float <BaseChance>k__BackingField; // 0x1C  
    private float <MaxChance>k__BackingField; // 0x20  
    private List<Tuple<int, int>> <Ingredients>k__BackingField; // 0x24  
    private LootFormat <Result>k__BackingField; // 0x28  
    private int <LevelRestrictions>k__BackingField; // 0x2C  
    private int <DiscoveryWeight>k__BackingField; // 0x30
```

// Methods

```
public void .ctor(); // 0x1105850  
public string get_NameID(); // 0x1105858  
private void set_NameID(string value); // 0x1105860  
public string get_IconID(); // 0x1105868  
private void set_IconID(string value); // 0x1105870  
public RecipeType get_Type(); // 0x1105878  
private void set_Type(RecipeType value); // 0x1105880  
public float get_BaseChance(); // 0x1105888  
private void set_BaseChance(float value); // 0x1105890  
public float get_MaxChance(); // 0x1105898  
private void set_MaxChance(float value); // 0x11058A0  
public List<Tuple<int, int>> get_Ingredients(); // 0x11058A8  
private void set_Ingredients(List<Tuple<int, int>> value); // 0x11058B0  
public LootFormat get_Result(); // 0x11058B8  
private void set_Result(LootFormat value); // 0x11058C0  
public int get_LevelRestrictions(); // 0x11058C8  
private void set_LevelRestrictions(int value); // 0x11058D0  
public int get_DiscoveryWeight(); // 0x11058D8  
private void set_DiscoveryWeight(int value); // 0x11058E0  
public static CraftRecipeEntry ParseFromTable(string[] row, string[] header, string[] validHeader); //
```

0x11058E8

```
private static List<Tuple<int, int>> ParseIngredients(string value); // 0x1105CB8
}
```

What can I do with it? I can look up what is in the offsets in global-metadata, but I can not make any sense of it from looking at the file in a hexeditor.

I have to admit, maybe I need more than a gentle push in the right direction ?

To the both of you, this has apparently gotten into C# (Or at least .NET) Reverse Engineering/Debugging. My desktop work environment is Linux (Solus), and to be able to help you guys with any sort of specifics would take an initial setup that I'm not willing to go through.

I suggest both of you to maybe try posting your more specific issues over at the [Visual Basic and .NET Framework](#) or the [C# Programming Language](#) sections.

Try to go into as much detail about what you already did, what you're trying to do, and what exactly it is that you are trying to get (Maybe a little bit on how the game works, because you have to remember the people trying to help you might not know a single thing about it).

Good luck :)

And to snowball_v specifically: Where you able to find anything at all through Wireshark?

BrilliantAdam - April 26, 2018, 3:10 am

(Apr 26, 2018 01:21 AM)V3t3r4n Wrote: [\[CITE\]](#) To the both of you, this has apparently gotten into C# (Or at least .NET) Reverse Engineering/Debugging. My desktop work environment is Linux (Solus), and to be able to help you guys with any sort of specifics would take an initial setup that I'm not willing to go through.

Try to go into as much detail about what you already did, what you're trying to do, and what exactly it is that you are trying to get (Maybe a little bit on how the game works, because you have to remember the people trying to help you might not know a single thing about it).

Good luck :)

And to snowball_v specifically: Where you able to find anything at all through Wireshark?

Thanks for your reply , sir

I was refreshing the website many times to see if u replied =)

snowball_v - April 26, 2018, 11:24 am

(Apr 26, 2018 01:21 AM)V3t3r4n Wrote: [\[CITE\]](#) And to snowball_v specifically: Where you able to find anything at all through Wireshark?It's the same problem: I don't know what to look for. I sure can isolate the packets related to checking a craft result, but have no idea what to do with them.

But in the end, I hardly think that what I am looking for (see initial post, i described it to the best of my ability) is transmitted here.

V3t3r4n - April 27, 2018, 12:48 am

(Apr 26, 2018 03:10 AM)BrilliantAdam Wrote: [\[CITE\]](#) Thanks for your reply , sir

I was refreshing the website many times to see if u replied =)

Well, sorry for keeping you waiting for so long :) I don't engage on activity on HF as much these days.

Hope you're able to find what you're looking for for, good luck!

(Apr 26, 2018 11:24 AM)snowball_v Wrote: [\[CITE\]](#) It's the same problem: I don't know what to look for. I sure can isolate the packets related to checking a craft result, but have no idea what to do with them.

But in the end, I hardly think that what I am looking for (see initial post, i described it to the best of my ability) is transmitted here.

Can you post some snippets of those packets contents? That way I can have a look at it myself.