NO-INTRO FORUM

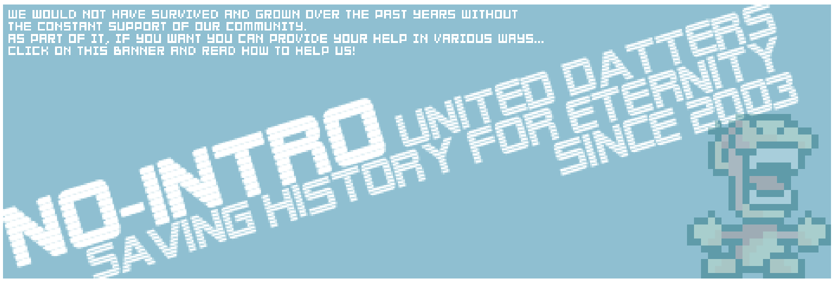
REGISTER. LOGIN. LURK. LEECH. CONTRIBUTE

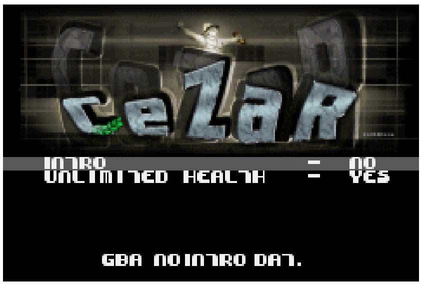
Logout [Hiccup]   **0** new messages   FAQ   Search   Members   User Control Panel

Last visit was: 28 Mar 2018 12:33   It is currently 28 Mar 2018 14:29

View unanswered posts | View active topics   View unread posts | View new posts | View your posts

Board index » Contributions » NDS*/3DS Corner   All times are UTC [DST]


WE WOULD NOT HAVE SURVIVED AND GROWN OVER THE PAST YEARS WITHOUT THE CONSTANT SUPPORT OF OUR COMMUNITY.
AS PART OF IT, IF YOU WANT YOU CAN PROVIDE YOUR HELP IN VARIOUS WAYS...
CLICK ON THIS BANNER AND READ HOW TO HELP US!
NO-INTRO
UNITED DATTERS FOR ETERNITY SINCE 2003
SAVING HISTORY



Almost all NDS cart dumps are missing data

newtopic   postreply   **Page 1 of 1**   [10 posts]

Print view   **Previous topic | Next topic**

Author   **Message**

Myria

offline

Joined: 25 Mar 2018 02:42
Posts: 18

Post subject: Almost all NDS cart dumps are missing data   **Posted:** 25 Mar 2018 07:40

About a month ago, I discovered that 99% of the Nintendo DS ROM dumps out there are missing some data. This affects almost all DS/DSi cartridge dumps out there. (DSiWare is not affected.)

In existing cartridge dumps, bytes 1000-3FFF are filled with zeros. But on the cartridges themselves, they're not zeros: that area contains the Blowfish encryption tables for the game. The Blowfish tables are derived from a table in the DS BIOS and the title ID. Thus, each game uses different data.

Unfortunately, however, the cartridge hardware has a lockout on reading this region. If you ask a retail cartridge to read this region, it will return zeros, hence existing dumps always having zeros there.

This table is needed at runtime by the cartridge, and because it is 0x1048 bytes long, it makes sense that it's simply written to the ROM and accessed by the hardware as needed. Pirate flash carts also do this for their bootstrap game, but they vary in storage location.

To explain this, I need to explain some stuff about how DS development was done. During most of game development, game developers used the title ID "NTRJ" and blank "SecurityData" (0000-2FFF) and "Segment3" (3000-3FFF). When flashing this to an official development DS flash cart, the flashing software silently injected the NTRJ security data.

Later, when Nintendo approved the title, but before final submission, Nintendo would assign the developer the title ID to use. Along with this title ID, Nintendo sent the "SecurityData", "Segment3" and "libsyscall" to use with the game. "libsyscall" was a library containing the syscall stubs. More importantly, however, libsyscall is what is encrypted in the "Secure Area" from 4000-47FF, and is the part of the ROM that pirates decrypted in their dumps. The encryption for this also depended on the title ID, so libsyscall was unique to each game.

An effect of Nintendo's design is that developers couldn't simply use pirate dumps of other companies' games on an official flash cart, because the security data is missing for whatever title ID the game had.

The final submissions to Nintendo were named ".srl" and contained the security data and libsyscall. (They did not, however, contain the post-DSi RSA signature; more on that later.) What pirates call the ".nds" format Nintendo calls ".srl".

Download "0663 - Barbie in the 12 Dancing Princesses (USA)" and "x085 - Contra 4 (Europe) (Proto)" to see this in action. Both games were made by WayForward, better known for their Shantae series. If you look at the headers for the two ROMs, you might notice that the title ID is the same - AIPE. It appears that during Contra 4's development, WayForward used the security data they had from Nintendo for their previous Barbie game in Contra 4 until they got Contra 4's security data. (At that time, they switched to the assigned ID, YCTE.)

But if you look lower in the Contra 4 prototype dump, you'll see that 1000-3FFF is filled in! That is the missing security data for Barbie in the 12 Dancing Princesses. In fact, if you copy 1000-3FFF from the Contra 4 prototype, stick it into the Barbie dump, encrypt 4000-47FF, and flash it to an official Nintendo dev flash cartridge, it will run! And it'll run on a DSi, too. So this is the first "proper" dump of Barbie in the 12 Dancing Princesses (using the numbering datomatic uses):

Name: 0663 - Barbie in the 12 Dancing Princesses (USA).nds
Serial: AIPE
Size: 8388608
CRC32: 0B526238
MD5: E15E004B4BEDC642D885E13A303659A9

I argue that proper dumps of DS games should *always* have the "Secure Area" (4000-47FF) be encrypted, because that is their native format and how they're stored in the ROM. It's what the header's secure area CRC is matching. Also, always storing encrypted avoids problems like Dragon Quest 5 having a strange secure area. The objection that then emulators would not be able to decrypt the Secure Area without a DS BIOS dump would be moot if we managed to get the "SecurityData" into the dump: that's enough information to decrypt the Secure Area.

The ROM images within Wii U Virtual Console DS releases came from the .srl files submitted to Nintendo by the developers, not scene dumps. This means that they also contain the "SecurityData" and have an encrypted "Secure Area". So some of these are in fact "proper" dumps, and here's one:

Name: 5171 - Brain Age - Train Your Brain in Minutes a Day! (USA) (Rev 1)
Serial: ANDE
Size: 16777216
CRC32: 3987710F
MD5: 619BA7892DF9AE64FE5DDA864743631F

Not all of them are "proper", though. DS Virtual Console games from 2008 and later do not have the RSA signature data in them. I believe that this is because DS Virtual Console game images are the ones submitted to Nintendo by developers, not the final ones written to the game carts. The solution for those is simple: copy the "SecurityData", "Segment3" and "Secure Area" to the scene dump and you get a proper image:

Name: 4926 - Picross 3D (USA) (En,Fr,Es).nds
Serial: C6PE
Size: 67108864
CRC32: CBB410EA
MD5: 9619F555722141203F18D27DC15DFAC8

I don't know how we can dump this data for every cartridge. The cartridges are returning zero for this area, after all!

Some experiments with an IS-CTR-BOX (3DS dev system, which supports flashing NTR/TWL/CTR flash carts) and an official flash cart show that the IS-CTR-BOX's flashing software knows how to dump the "SecurityData" from official flash carts. Whether this works with retail cartridges is unknown, and admittedly, probably unlikely to work (except perhaps with WarioWare DIY? TBD). It's worth a shot, but I lack the hardware knowledge to log the cartridge protocol between an IS-CTR-BOX and a flash cart.

It would be nice if we could just generate this "SecurityData". After all, we know the Blowfish algorithm and source tables. The problem is that Nintendo put extra data in there. The 0x1048-byte Blowfish table is stored in 0x1600-0x1647 and 0x1C00-0x2BFF, but the rest (0x1000-0x15FF, 0x1648-0x1BFF, 0x2BFF-0x2FFF) is unknown. If you zero these areas, games will work fine when flashed to an official dev flash cart, suggesting that they're unused. Nintendo may have filled these unused areas with random data as chaff.

My biggest question is whether anyone cares. Do we care if data unimportant to running the games is missing?

Top

profile pm quote

Hiccup

online

Datter

Joined: 09 Oct 2015 11:29
Posts: 232

Post subject: Re: Almost all NDS cart dumps are missing data

Posted: 25 Mar 2018 11:47

Good work.

I think its important to preserve this data 😋.
But that's just me.

Top

profile pm edit quote

Myria

offline

Joined: 25 Mar 2018 02:42
Posts: 18

Post subject: Re: Almost all NDS cart dumps are missing data

Posted: 26 Mar 2018 17:44

> **Hiccup wrote:**
>
> Good work.
>
> I think its important to preserve this data 😋.
> But that's just me.

We don't know how to dump the data right now, and even if we did, we'd have to re-dump every game in the library.

Top

profile pm quote

z.g

offline

Datter

Joined: 25 May 2008 12:13
Posts: 186

Post subject: Re: Almost all NDS cart dumps are missing data

Posted: 26 Mar 2018 19:32

some speculations while i have fresh impressions.

> **Myria wrote:**
>
> Not all of them are "proper", though. DS Virtual Console games from 2008 and later do not have the RSA signature data in them. I believe that this is because DS Virtual Console game images are the ones submitted to Nintendo by developers, not the final ones written to the game carts.

> **Myria wrote:**
>
> The 0x1048-byte Blowfish table is stored in 0x1600-0x1647 and 0x1C00-0x2BFF

this is the weakest point. i'm 100% sure, that blowfish table stored in the cart, but we steel don't have at least one 100% confirmed good dump. as you proofed itself, vc dumps is not final. so we can be sure that nintendo only add rsa signature. blowfish table divided into two parts without any reason. possible this not changed in retail cart, but who knows? possible explanation that they do this for "security". and as official flash carts is not mass product its not problem, and on retail cart it placed in another place continuously.

> **Myria wrote:**
>
> An effect of Nintendo's design is that developers couldn't simply use pirate dumps of other companies' games on an official flash cart, because the security data is missing for whatever title ID the game had.

strange statement. by design this system was before first pirate dumps, and then pirate dumps appeared — generate blowfish table was not a big problem.

> **Myria wrote:**
>
> And it'll run on a DSi, too.

how is this relevant to topic?

> **Myria wrote:**
>
> Also, always storing encrypted avoids problems like Dragon Quest 5 having a strange secure area.

i'm also for leaving only encrypted versions of roms, but what is wrong with dq5? i know that this and one another game is release instead rom target, but accurate decrypting not cause any problem for me.

> **Myria wrote:**
>
> except perhaps with WarioWare DIY?

what is with warioware diy? i know it use nand, and any evidence, that 0x1000-0x3fff area can be dumped from such carts exsits?

> **Myria wrote:**
>
> My biggest question is whether anyone cares. Do we care if data unimportant to running the games is missing?

for me — any data important, but if it practically undumpable and its existance not critical for preservation — it is not thing that make great concern.

!

Top

profile pm quote

Myria

offline

Joined: 25 Mar 2018 02:42
Posts: 18

Post subject: Re: Almost all NDS cart dumps are missing data

Posted: 27 Mar 2018 08:28

> **z.g wrote:**
>
> this is the weakest point. i'm 100% sure, that blowfish table stored in the cart, but we steel don't have at least one 100% confirmed good dump. as you proofed itself, vc dumps is not final. so we can be sure that nintendo only add rsa signature. blowfish table divided into two parts without any reason. possible this not changed in retail cart, but who knows? possible explanation that they do this for "security". and as official flash carts is not mass product its not problem, and on retail cart it placed in another place continuously.

I'm just going on what is probably true: it is more likely that the data is in 1000-2FFF than that it is in some other format, just because it's the simplest answer that matches available information.

> **z.g wrote:**
>
> strange statement. by design this system was before first pirate dumps, and then pirate dumps appeared — generate blowfish table was not a big problem.

I just mean that it's possible that Nintendo knew that dumping the Blowfish tables was difficult and factored that into the design. This is just speculation based on available information.

> **z.g wrote:**
>
> how is this relevant to topic?

That it runs on DSi when flashed this way means that the cartridge is accurate enough to pass the extra DSi protections.

> **z.g wrote:**

> i'm also for leaving only encrypted versions of roms, but what is wrong with dq5? i know that this and one another game is release instead rom target, but accurate decrypting not cause any problem for me.

Dragon Quest 5 has an invalid "Secure Area" (4000-47FF) by the usual definitions. If you "decrypt" it, you're actually destroying it.

> **z.g wrote:**
>
> what is with warioware diy? i know it use nand, and any evidence, that 0x1000-0x3fff area can be dumped from such carts exsits?

I ordered WarioWare DIY from eBay so I could check it. I don't know yet. I was going to see whether the IS-CTR-BOX will think it's a flash cart.

> **z.g wrote:**
>
> for me — any data important, but if it practically undumpable and its existance not critical for preservation — it is not thing that make great concern.

If I do manage to find a way to dump 1000-3FFF, would it be worthwhile to redump every DS game in existence?

By the way, I believe that there is a second "Security Data" area on DSi games. I have a TWL flash cart coming in the mail that I'll use to test theories.

!

Top profile pm quote

z.g **Post subject:** Re: Almost all NDS cart dumps are missing data **Posted:** 27 Mar 2018 12:05

offline

Datter

Joined: 25 May 2008 12:13
Posts: 186

> **Myria wrote:**
>
> I'm just going on what is probably true: it is more likely that the data is in 1000-2FFF than that it is in some other format, just because it's the simplest answer that matches available information.

yes, i also think so, but everything that we have is indirect evidence, before we get dump from retail cart we cant' be 100% sure.

> **Myria wrote:**
>
> That it runs on DSi when flashed this way means that the cartridge is accurate enough to pass the extra DSi protections.

dsi protections based only on rsa signing, that easy dumpable and not relevant to this topic.

> **Myria wrote:**
>
> Dragon Quest 5 has an invalid "Secure Area" (4000-47FF) by the usual definitions. If you "decrypt" it, you're actually destroying it.

no.

> **Myria wrote:**
>
> I ordered WarioWare DIY from eBay so I could check it. I don't know yet. I was going to see whether the IS-CTR-BOX will think it's a flash cart.

i own "jam with the band" and "face training" this is another games that use nand. read nand data commands works only in real save area, but address used from rom start. when i tried read data before save cart became busy forever.

> **Myria wrote:**

> If I do manage to find a way to dump 1000-3FFF, would it be worthwhile to redump every DS game in existence?

yes.

> **Myria wrote:**
>
> By the way, I believe that there is a second "Security Data" area on DSi games. I have a TWL flash cart coming in the mail that I'll use to test theories.

yes. we had very hot private discussion here about this 5 or 6 years ago. rom_header.LTD.sbin used to fill this area in twl sdk.

!

Top profile pm quote

Collecter

offline

Joined: 25 Nov 2016 17:09
Posts: 133

Post subject: Re: Almost all NDS cart dumps are missing data **Posted:** 27 Mar 2018 18:34

Preserving everything is good and all but just imagine redumping everything again in 2018 xD

!

Top profile pm quote

Hiccup

online

Datter

Joined: 09 Oct 2015 11:29
Posts: 232

Post subject: Re: Almost all NDS cart dumps are missing data **Posted:** 27 Mar 2018 19:40

A lot of the people who made the original redumps may be still around,still have their carts and be willing to redump again, especially if there is a straightforward way to do it (like a new version of wooddumper or GodMode9).

!

Top profile pm edit quote

Myria

offline

Joined: 25 Mar 2018 02:42
Posts: 18

Post subject: Re: Almost all NDS cart dumps are missing data **Posted:** 28 Mar 2018 08:43

Are there any Virtual Console releases of DSi-enhanced games?

!

Top profile pm quote

Hiccup

online

Datter

Joined: 09 Oct 2015 11:29
Posts: 232

Post subject: Re: Almost all NDS cart dumps are missing data **Posted:** 28 Mar 2018 12:33

I checked the Wikipedia lists of NDS VC games against a Datomatic search for "ndsi enhanced" and it appears that there are no dsi enhanced VC games.

!

Top profile pm edit quote

Display posts from previous: All posts ▼ Sort by Post time ▼ Ascending ▼ Go

new topic post reply **Page 1 of 1** [10 posts]

Board index » **Contributions** » **NDS*/3DS Corner** All times are UTC [DST]

Who is online

Users browsing this forum: **Hiccup** and 0 guests

You **can** post new topics in this forum
You **can** reply to topics in this forum
You **can** edit your posts in this forum
You **cannot** delete your posts in this forum
You **can** post attachments in this forum