



DIGITAL FORENSIC RESEARCH CONFERENCE

Forensic Analysis of the Nintendo 3DS NAND

By

Mr. Gus Pessolano, Dr. Huw O. L. Read, Dr. Iain Sutherland, and Dr. Konstantinos Xynos

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2019 USA

Portland, OR (July 15th - 19th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

<https://dfrws.org>





NORWICH
UNIVERSITY®



Mr. Gus Pessolano
Dr. Huw O. L. Read
Dr. Iain Sutherland
Dr. Konstantinos Xynos

Forensic Analysis of the Nintendo 3DS NAND

\$whoami

- Graduated with a B.S in Computer Security and Information Assurance from Norwich University in December 2017
 - Deep-dove into 3DS Forensics my last semester
- Currently a Cyber Security Analyst at Vermont Electric Power Company
 - GIAC certified in Critical Infrastructure Protection (GCIP)

Why Look at the 3DS?

Nintendo Switch is Nintendo's most recently released console (2017).

- ~34.74 million units sold worldwide

New exploits have been discovered which enable a more forensically sound method of data extraction and analysis.

Released February 2011

- ~75.08 million units sold worldwide
- Nintendo's highest selling active console

Generally aimed at younger generation, statistics from ESRB for DS/DSi/3DS category

- 2587 games rated at Early Childhood/Everyone
- 38 games rated at Mature (17+)

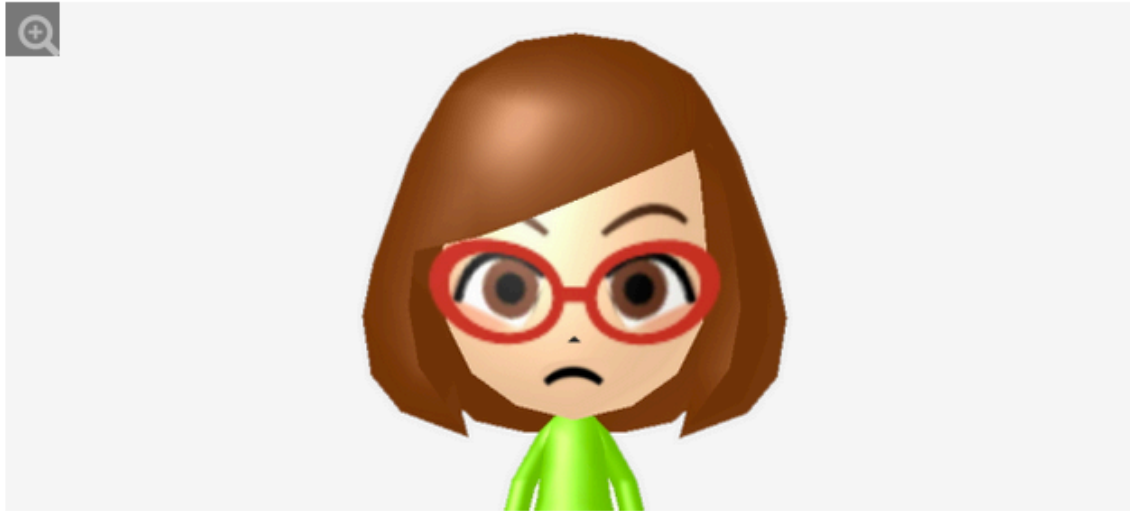
Nintendo Pulls 3DS Feature, Says Kids Were Sharing 'Offensive Material'



Stephen Totilo

Filed to: NINTENDO 10/31/13 10:51pm

91,227 🔥 12 ★ ⌵



Japanese newspaper *Mainichi* reports that charges for child pornography have also been filed against another man, aged 44, who had allegedly two girls—then aged 11 to 12—send nude photos through Swapnote, or "Itsu no Ma ni Koukan Nikki" (いつの間に交換日記) as it's called in Japan. This man, a resident of Aichi Prefecture, has allegedly confessed to the acts.

In the above articles, both *Yomiuri* and *Mainichi* note that parents had initially turned off the 3DS's internet function, but the children had turned it back on.

<http://kotaku.com/nintendo-pulls-3ds-feature-says-kids-were-sharing-off-1456565997>

Multiple Iterations



February, 2011



October, 2013



October, 2014



July, 2017

Working Towards Forensic Soundness

- The work conducted in this paper used to perform forensic acquisition of a 3DS would not be possible without the seminal work by Scires et al. (2018) and the tools created as a result of their research.
- Their paper made use of flaws discovered in the RSA signature verification of one of the boot ROMs (the ARM9 boot ROM known as “Boot9”) to cause firmware created by third parties to appear valid to the signature parser.

boot9strap vulnerability

- On May 19th, 2017, a vulnerability known as the 'boot9strap' vulnerability was published online (3ds, 2019).
- Further discoveries (Scires et al., 2018) made by analyzing the protected half of the Boot9 ROM revealed that, before the 3DS attempts to load a firmware image from the internal NAND, it will check if the device lid is closed and whether the START, SELECT and X buttons are being held. Boot9 checks if a DS cartridge is inserted and if so, attempts to load a signed firmware from it, bypassing the firmware on the NAND.

Impossible combination?



X button

START+SELECT button

Power button

Sleep switch activated
(lid closed)

Magnets



DS Flashcarts

- Unofficial game cartridges, known colloquially as flashcarts (as they are user-writable) are commonly associated with software piracy.
- In this case, we can flash these flashcarts with a 'malicious' firmware that will allow us to boot custom software we placed onto the 3DS micro SD card, completely circumventing a normal boot process.



‘Unpatchable’

- As confirmed in McClintic et al. (2018), the trust in the 3DS is the boot ROM which is burned into the System-on-Chip (SoC) during the manufacturing.
- Fixing the issue consists of changing the SoC at the factory for all future revisions of the hardware.
 - Improbable, as 3DS successor has been released.
- This is significant as the vulnerability has existed in all Nintendo 3DS manufactured to date.

Preparing to Dump the NAND

- A reflashable cartridge is prepared with the ntrboot files.
- The original microSD/SD card in the console is forensically imaged and set aside.
- A new microSD/SD is prepared with the following tools:
 - a. boot9strap (Scires, 2017b) which enables Boot9 code execution
 - b. decrypt9WIP (decrypt9, 2017) which performs the actual dumping of NAND and the system's encryption key.

Dumping the NAND with Decrypt9

- Backup of the internal NAND via SysNAND Options - > SysNAND Backup/Restore - > NAND Backup. This creates two files, the NAND.bin and a NAND.bin.sha (SHA256 value).
- Verification of the NAND dump via SysNAND Options - > SysNAND Backup/Restore - > Validate NAND Dump.
- Backup of the unique encryption key (XOR) needed to decrypt the NAND dump via XORpad Generator Options - > CTRNAND Padgen, nand.fat16.xorpad.

```
Decrypt9WIP (2017/06/07)
=====
XORpad Generator Options
Ticket/Titlekey Options
SysNAND Options
EmuNAND Options
Content Decryptor Options
[Gamecart Dumper Options]
NDS Flashcart Options
Maintenance Options
=====
A: Choose
SELECT: Unmount SD Card
START: Reboot / [++] Poweroff

Work directory: /files9
Game directory: /files9/D9Game
SD card: 43878MB/59485MB & no EmuNAND
```

Assuring Forensic Soundness

- The NAND.bin.sha file contains the SHA256 value of the 3DS NAND image.
- The NAND.bin file can be hashed separately on an investigator's workstation, and the hash values will match.
- The NAND was dumped several times and consistently generated the same SHA256 value (as long as the console has not been booted).

Impact of Booting the 3DS

- 1.7% of the files were updated
 - Activity and feed aware apps
 - AccessData FTK's KFF used to verify pre- and post-states.
- To ensure integrity, it is recommended to practice this method on another console first, before trying it live.

Decrypting the NAND

- The NAND.bin file actually contains two partitions, the backwards-compatible DSi partition and the 3DS partition.
- The 3DS partition (CTR NAND) contains the artifacts of interest to an examiner.
- NAND.bin is XOR'd with console-unique key

Decrypting the NAND

- This may be achieved using a dedicated XORing application, like 3DSFAT16Tool (3DSFAT16tool).
- Produces a decrypted version in a raw, uncompressed format, FAT16.
- Image easily recognized by many forensic tools

```
3DSFAT16tool [-d|-i] [NAND] [FAT16] [XORPAD]
```

```
-d    Dump FAT16 from NAND file
```

```
-i    Inject FAT16 to NAND file
```

```
NAND    -> your NAND backup, dump via Decrypt9, GW launcher.dat or rxTools
```

```
FAT16   -> the FAT16 image, must exist for injecting, will be created/overwritten for dumping
```

```
XORPAD  -> NAND XORPAD, generate using Decrypt9 or rxTools
```

Example:

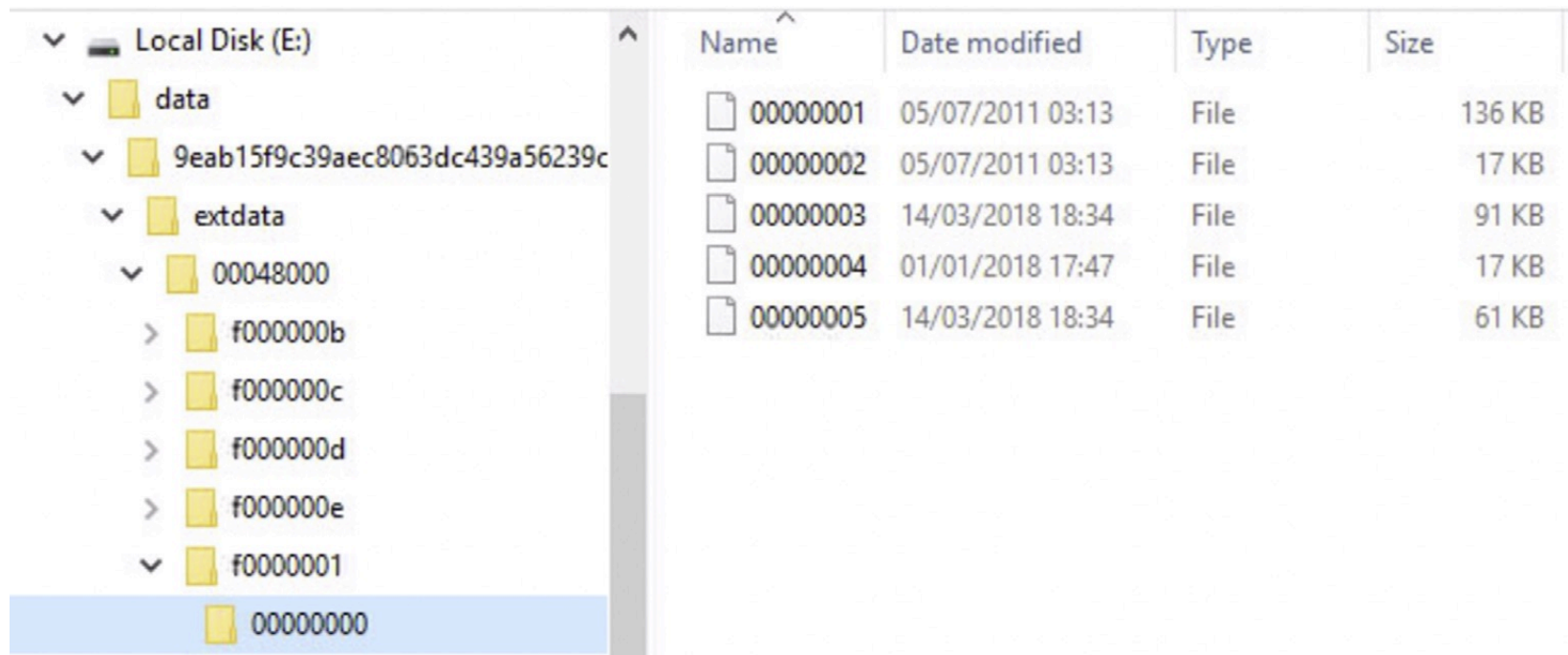
```
3DSFAT16tool -d NAND.bin NAND.fat16.bin NAND.fat16.xorpad
```



extdata

The extdata (or extra data) folder stores additional, arbitrary data for an application (3dbrew, 2015b).

extdata File System Structure



Name	Date modified	Type	Size
00000001	05/07/2011 03:13	File	136 KB
00000002	05/07/2011 03:13	File	17 KB
00000003	14/03/2018 18:34	File	91 KB
00000004	01/01/2018 17:47	File	17 KB
00000005	14/03/2018 18:34	File	61 KB

extdata File Structure

- Within each application's 00000000 folder there are two files 00000001 and 00000002 which are part of the core operating system.
- The time stamps of these files are static, and will never update.
- If present, 00000003 and above are created by a user's actions and have a timestamp reflecting when the action occurred.

Artifacts of Interest

- Camera app
- Sound app
- Internet Browser
- Config services
- Friends app
- MicroSD Management app
- Titles.db

Camera app - f00000001

- The 00000003 file is created after the camera app has been used and remains even if all pictures have been deleted. The timestamp of 00000003 is updated when a picture is taken or when a picture is deleted.
- If present, 00000005 and above contain embedded pictures (one per file - n.b. “3D” images appear as two embedded files, slightly off-center from each other) in JPEG format (i.e, file header 0xFFD8FFE1).
- FTK successfully carved all the images taken.

Camera app - f00000001

- Using ExifTool (Harvey, 2019) a wealth of metadata was obtained.
- Within the “ExifIFD” group, create date and date/time original tags provided the creation date of the image.
- Within the Nintendo group, time stamp and a tag labelled “internal serial number” were obtained.

Camera app - f00000001

- The images were then deleted using the camera application's delete function.
- Another NAND image was obtained and put through a second file carve.
- FTK was able to carve out all the deleted pictures.

Sound app – f00000002

- Files 000000003 and above contain sound recordings made by the built-in microphone. They are in the m4a format (i.e., file header 0x66747970).
- PhotoRec was able to extract the m4a files. The sound clips were then deleted, and the console re-imaged. PhotoRec was able to recover all the deleted audio files.

Internet browser - 000200bb

- A file carve after browsing the web does not reveal any images of the web pages visited.
- This suggests the 3DS does not keep a local webcache like desktop web browsers.
- However, it is possible to extract the bookmarks and the history.

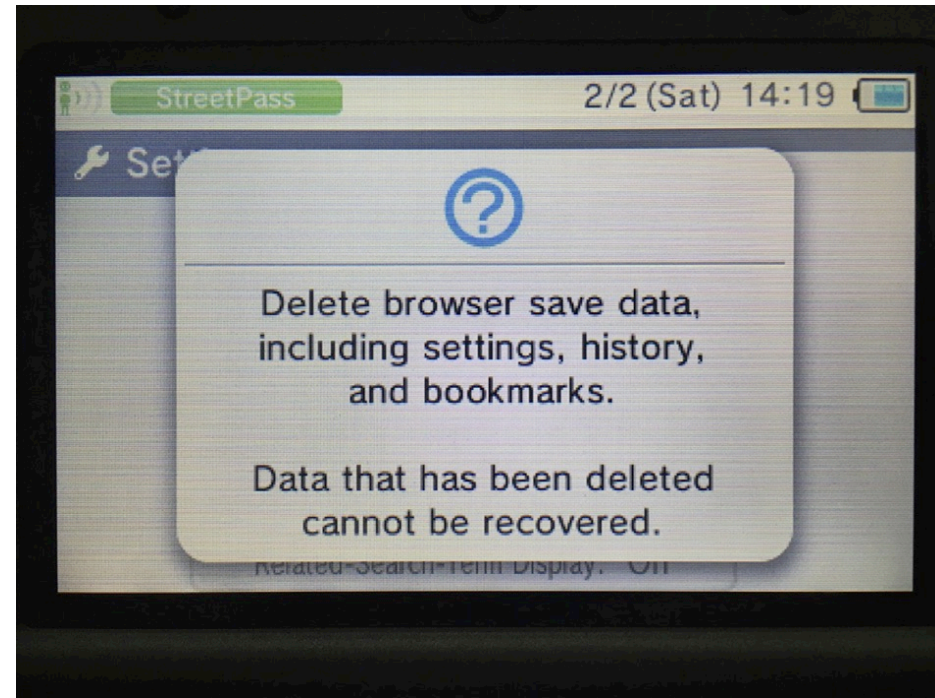
Internet browser - 000200bb

Bookmark structure.

Length (hex)	Description
8	Timestamp, number of milliseconds since epoch (Jan. 1st, 2000). Default bookmarks are zeroed out.
4	Unknown
1	Counter. The byte increments the bookmark entry. First value is 0x00.
1	Unknown
1	Appears to have the value 0x01 if a default bookmark, 0x00 if a user added bookmark.
1	Unknown, always 0x01
200	Unknown, has data for default bookmarks, zeroed for user-generated.
400	URL (null-padded)
200	Bookmark name

Internet browser - 000200bb

- History has similar structure to bookmarks, limit of 99 entries on new 3DS systems.
- Built-in reset functionality does not scrub data. All bookmarks and history entries were recoverable.



Config Services - 00010017

- After an investigation of the WiFi configuration entries, it was discovered that **WiFi SSIDs and their passwords are stored in plaintext**. An investigator may search for the start of the embedded config file with 0x4100E44100, noting the offset.
- The 3DS was added to three access points, two of the entries were erased, the console was re-imaged. **One of entries was recoverable; the others could not be found** (neither by explicitly searching for the known SSID nor the known password).

Friends - 00010032

- Analyzing this file with strings yielded the names and publicly displayed messages of all friends that have been added on the console.
- In addition the 3DS console's Serial number, username, and public message were all viewable.

microSD management - 00020241

- The microSD Management application is specific to the New Nintendo 3DS line of 3DS consoles only.
- The application temporarily turns the New Nintendo 3DS into a device that can be accessed by a SMB network connection.
- No system/NAND files can be accessed in this manner, only files stored on the console's microSD card

microSD management - 00020241

- Analyzing this file with the strings reveals the following:
 - SSID of any network stored within the console.
 - The name the device is given when joining the network
 - The device's required login name and PIN.
 - The name of the workgroup on the console's respective network.

title.db

- On the root of the decrypted NAND disk image is a folder dbs or databases. Within this folder is several files, one of which is the title.db file.
- This file contains a list of all of the installed pieces of software present on the device.
- This can be helpful in knowing exactly what software was installed on the console, without having to live boot the console to check.

Additional Analysis

- Restoring a NAND dump is Forensically sound
 - Analysts can use Native apps to interpret data, as in Read et al. (2016)
- Impact of System Erase
 - Does not zero out NAND
 - Does not generate new XOR key
 - We were able to recover “deleted” JPEG files

Questions?