Reimplementing game servers for fun and giggles

A retrospective of 10 years doing what Nintendon't

Eva Lauren Kelly (thejsa) • Trans Tech Tent @ BSides Cymru, 11th Feb 2023

Where it all started...

Nintendo DSi

- Launched in Japan in late 2008
- 16MB RAM, 256MB storage
  - Somewhat humble even by the standards of the day
  - But it offered hours on end of fun
- ~2000 games
- ~200 with online play

Image: Nicolas Nova via Flickr, May 3 2009 (Creative Commons CC BY-NC 2.0)

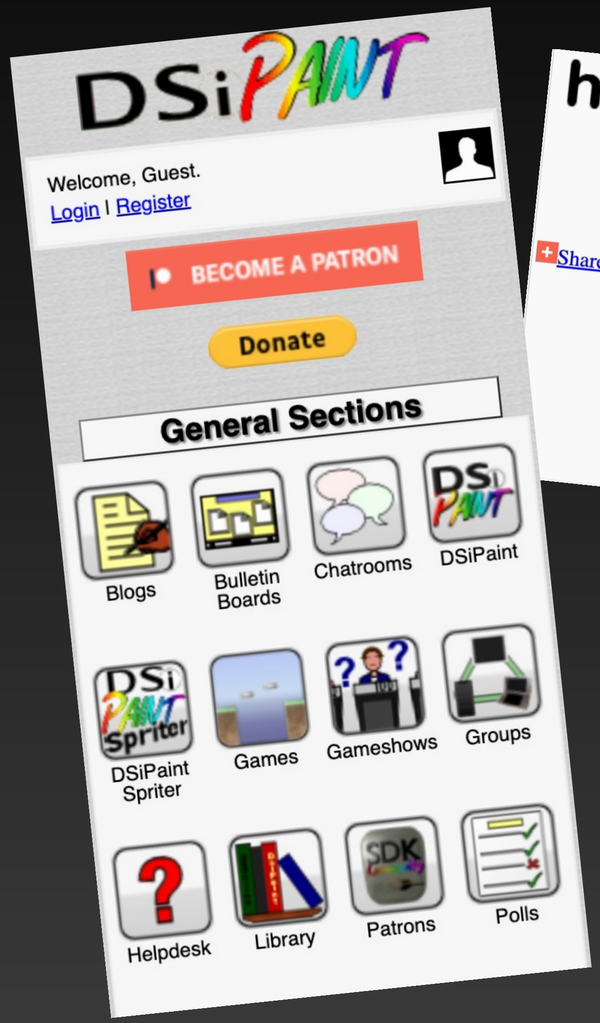
In many ways, a new kind of console

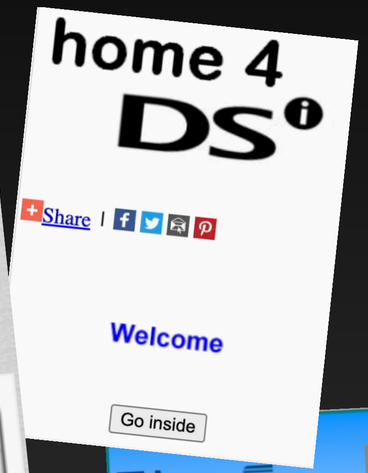
- Marketed as a truly personal device
- Designed as much for *creation*, as it was for consumption
- Surprisingly many parallels with modern smartphones

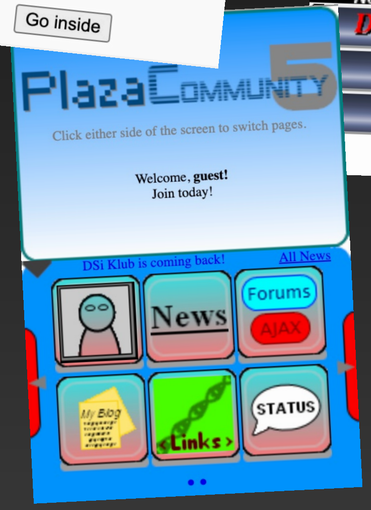
Screenshot of “Nintendo DSi Trailer” (nintendodsuk via YouTube; fair dealing)

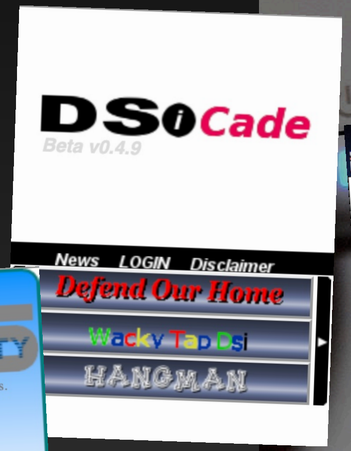
The Web in your pocket

...more or less









- A browser based on Opera 9.50 — surprisingly capable for the time :-)
- Unfortunately, a lot of these sites have been lost.
- Although the Wayback Machine preserves bits and bobs, here and there — a lot of these sites relied heavily on some kinda creative JavaScript.
- This scene probably deserves a talk to itself, in my opinion~

Image: baron valium via Flickr, Nov 1 2008 (Creative Commons CC BY-SA 2.0)

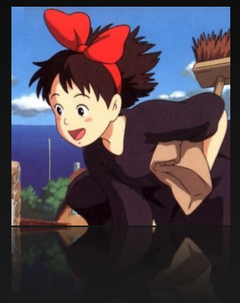
Most important of all...

- Flipnote Studio was released in 2009 for *free*
- A tool to make flipbook-style animations using the DSi touchscreen
- *Linked into an advanced online platform to share creations with the world*

Who am I?

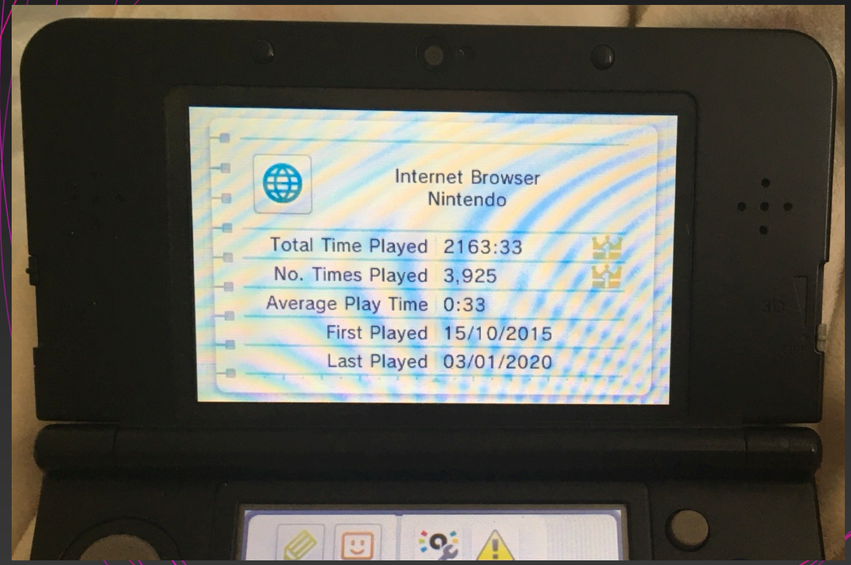
(and why has it taken so long to get to this?)

Eva Lauren Kelly
known sometimes as *thejsa*
i don't really use twitter anymore
https://www.evalauren.co.uk

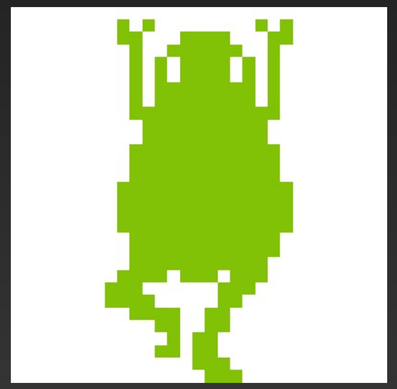


- LinkedIn: 'freelance software developer'...
- ...but really, an all-round sorceress of technological shenanigans ✨
- Born in the English Westcountry; now living and thriving in Cymru 🏴
- BSc student at Cardiff University
- Director at Trans Tech Tent
  (but I'm not wearing that hat for this talk)
- Chaotic but 'WTF in the best possible way'

- I was very much a child of the Internet...
- The DSi was often my only portal to the world throughout my middle childhood
- Its limitations inspired a wealth of creativity and wonderful communities
- Without these, I probably wouldn't be here speaking to you today



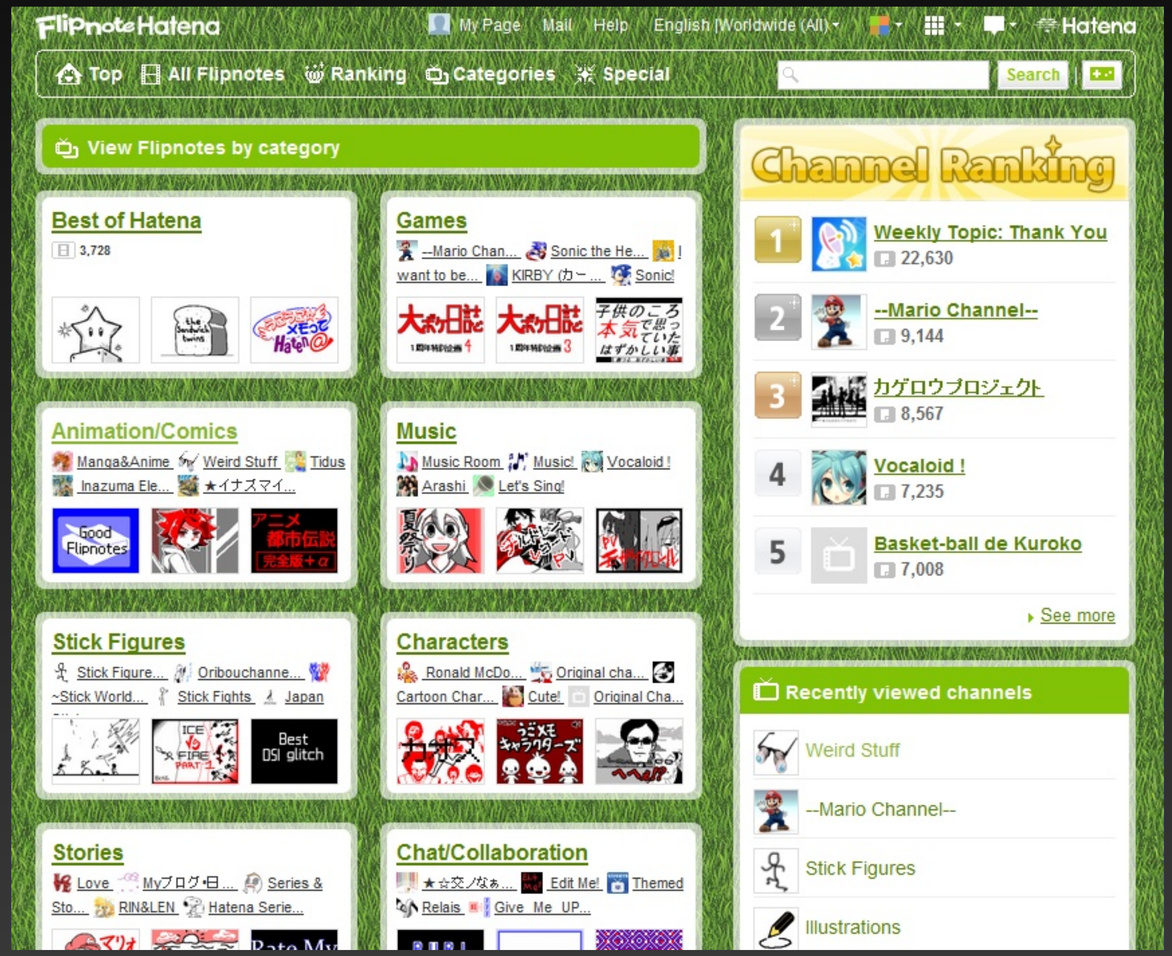
Back to Flipnote...



Flipnote Hatena

Think YouTube, but for Flipnote animations :-)

- A partnership between Nintendo and Hatena, a Japanese web services company
  - Across its lifetime, Hatena has provided microblogging, social bookmarking, photo sharing… all the fun Web 2.0 stuff
- Millions upon millions of creations from artists of all backgrounds — hosted & available free of charge



Flipnote Hatena

Think YouTube, but for Flipnote animations :-)

Flipnote Hatena has ended its service

The Flipnote Hatena website and Flipnote Hatena for Nintendo DSi ended on May 31, 2013.

We would like express our sincere gratitude to the members of the Flipnote Hatena community which began in December 2008. The service has now ended, but the memories will always remain.
Thank you all for the amazing flipnotes and for your use of the Flipnote Hatena website and Flipnote Hatena for Nintendo DSi.

Hatena Co., Ltd.

- 13th March 2013: A special Nintendo Direct Mini announced Flipnote Studio 3D for the Nintendo 3DS!
- … but Flipnote Hatena would shut down on 31st May, despite outcry from the vibrant Flipnote community
  - To be replaced with a subscription service on the new Flipnote Studio 3D
  - DSi Flipnotes would be transferred to the new platform (with an opt-out procedure)
- Flipnote Studio 3D launched in Japan in July 2013
  - …but it only made it to the rest of the world in 2015, as a limited *Club Nintendo* release…
  - …without any online sharing functionality
- What now for the Flipnote community?

Let’s do something about that...

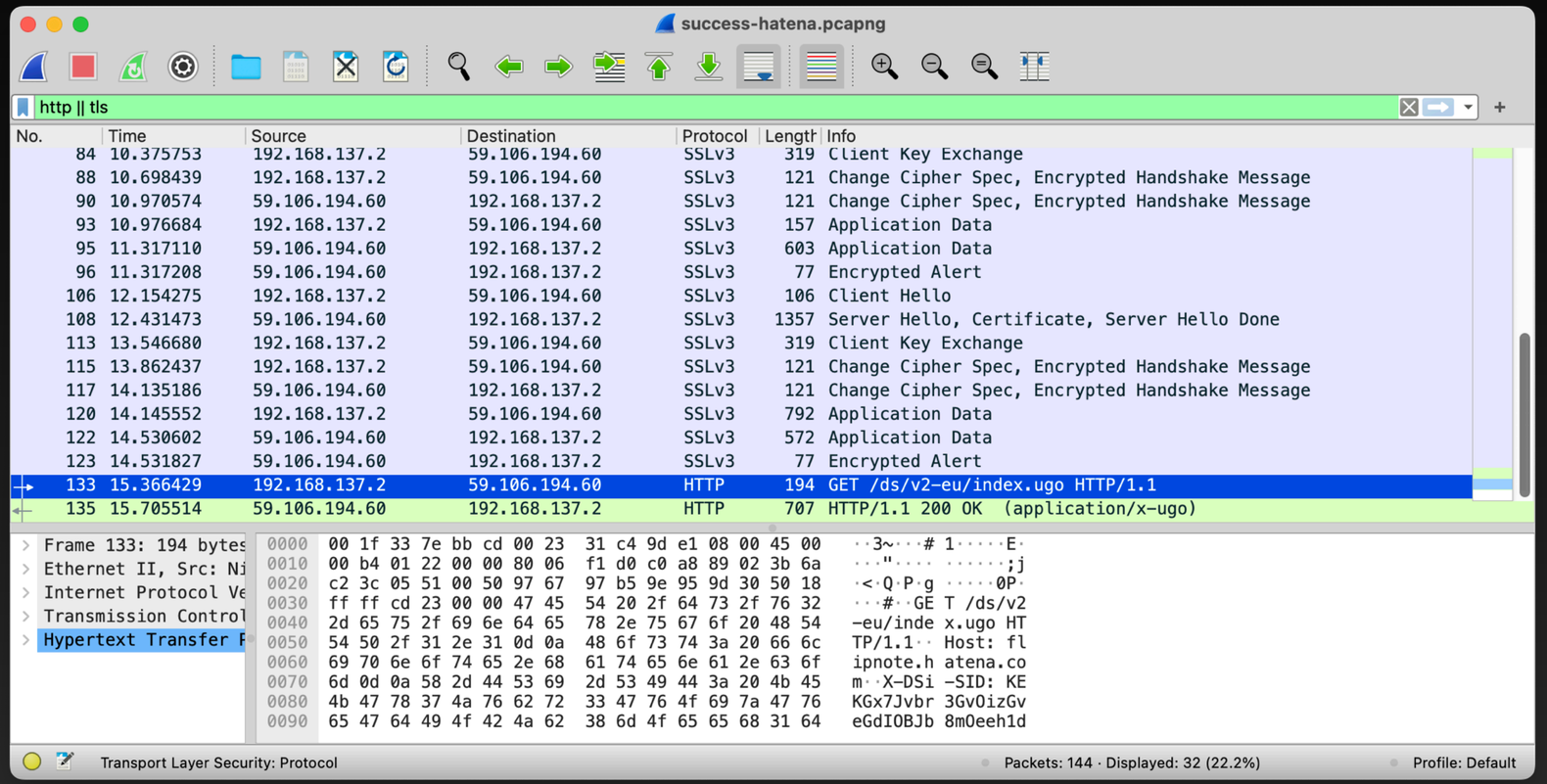
As luck would have it, earlier in 2013, a few nerds were already curious...

Flipnote Hatena had a rich web-like user interface.

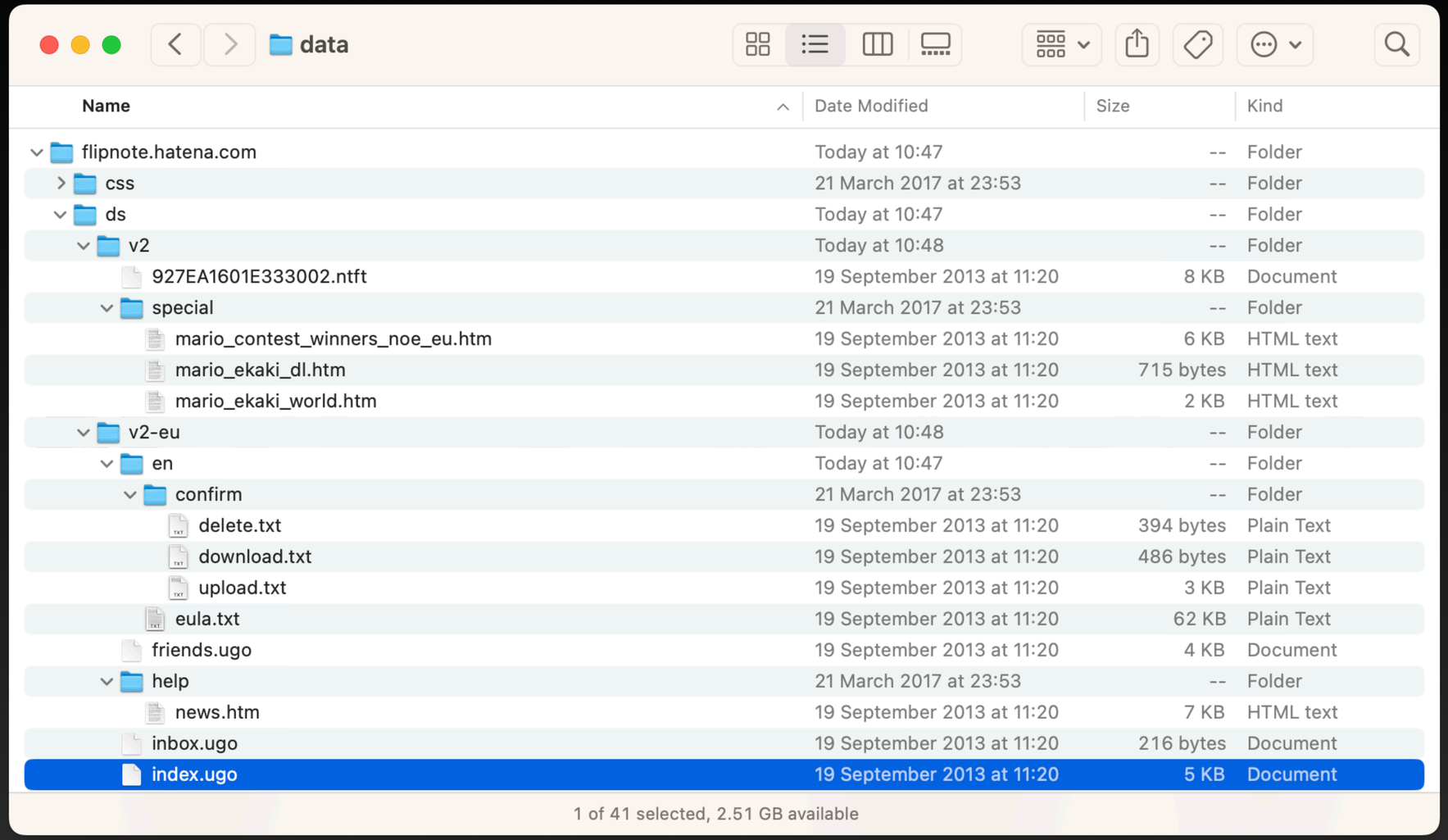
How did it work? Could we ... just ... make our own?

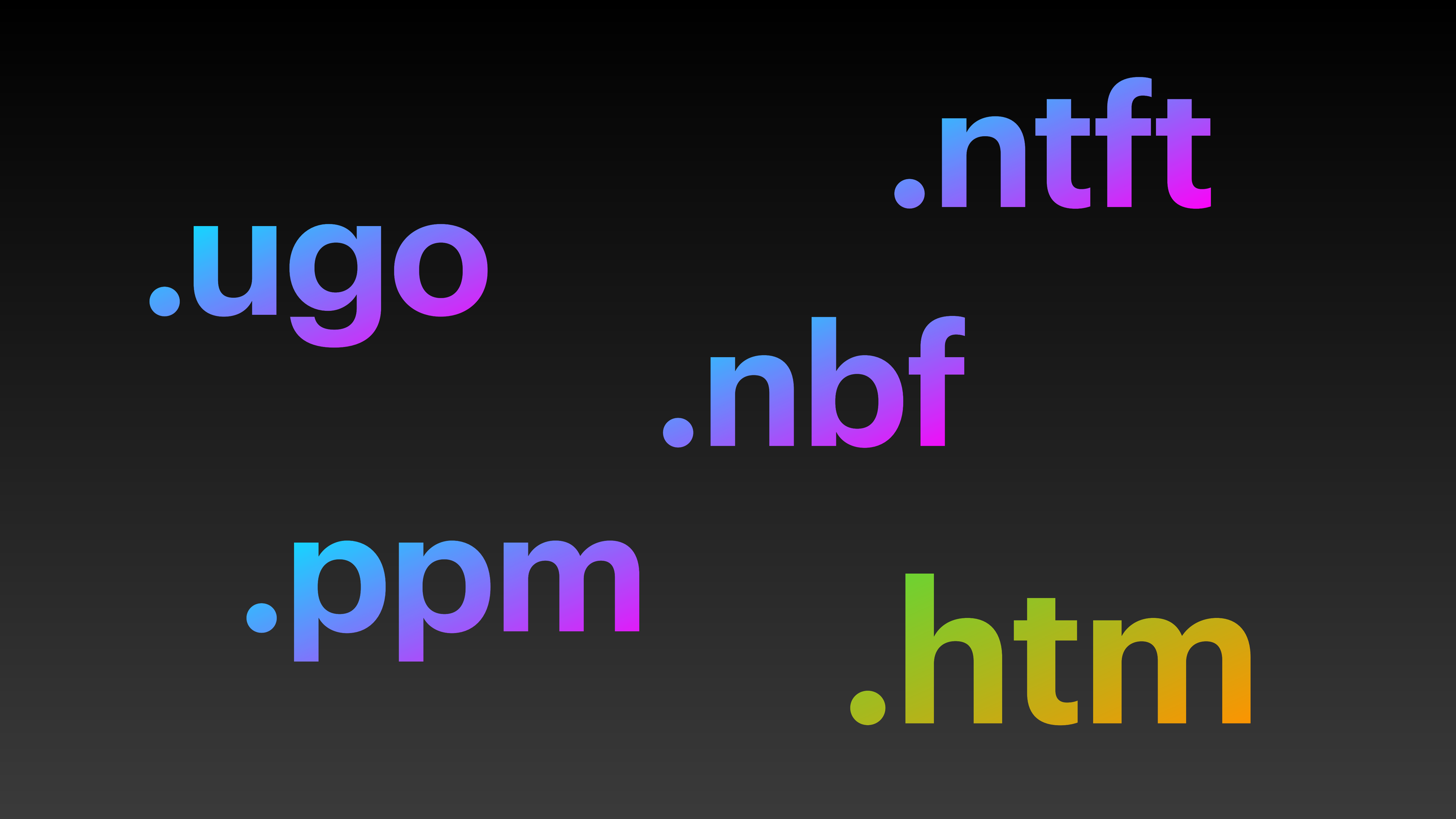
- I stumbled across a blog by a certain **Austin Burk (sudofox)**, whilst browsing on my DSi
- He'd used a tool called *Microsoft Network Monitor* to 'sniff' the packets from the DSi
- Turns out, Flipnote Hatena was *just HTTP* ... albeit with spicy files
- I got in touch!

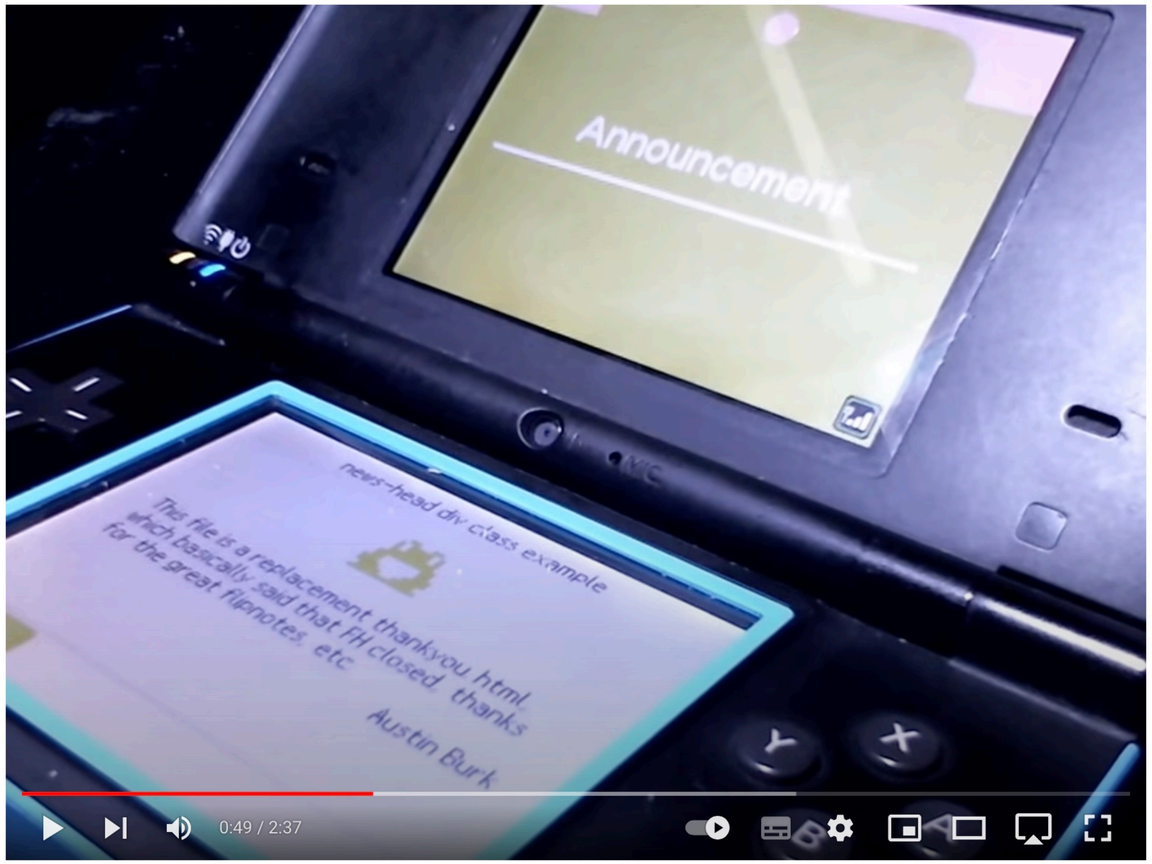

Fiddler



Yes, I know this is Wireshark... I couldn't find the Fiddler captures in their original format in time for the talk, unfortunately


data
Name
Date Modified
Size
Kind
flipnote.hatena.com Today at 10:47 -- Folder
css 21 March 2017 at 23:53 -- Folder
ds Today at 10:47 -- Folder
v2 Today at 10:48 -- Folder
927EA1601E333002.ntft 19 September 2013 at 11:20 8 KB Document
special 21 March 2017 at 23:53 -- Folder
mario_contest_winners_noe_eu.htm 19 September 2013 at 11:20 6 KB HTML text
mario_ekaki_dl.htm 19 September 2013 at 11:20 715 bytes HTML text
mario_ekaki_world.htm 19 September 2013 at 11:20 2 KB HTML text
v2-eu Today at 10:48 -- Folder
en Today at 10:47 -- Folder
confirm 21 March 2017 at 23:53 -- Folder
delete.txt 19 September 2013 at 11:20 394 bytes Plain Text
download.txt 19 September 2013 at 11:20 486 bytes Plain Text
upload.txt 19 September 2013 at 11:20 3 KB Plain Text
eula.txt 19 September 2013 at 11:20 62 KB Plain Text
friends.ugo 19 September 2013 at 11:20 4 KB Document
help 21 March 2017 at 23:53 -- Folder
news.htm 19 September 2013 at 11:20 7 KB HTML text
inbox.ugo 19 September 2013 at 11:20 216 bytes Document
index.ugo 19 September 2013 at 11:20 5 KB Document
1 of 41 selected, 2.51 GB available


.ntft
.ugo
.nbf
.ppm
.htm



Sudofox's Flipnote Server: Test 1

Sudofox
1.13K subscribers

Subscribed | 37 | Share | Clip

2,058 views 14 Sept 2013
A few weeks ago, I found out that Flipnote Hatena had closed its doors back in May (2013). Ever since then, for a little while each day, I've reverse-engineered Flipnote Hatena and Flipnote Studio. I now have a basic, working, wireframe flipnote site running on my

Sudomemo

Sudomemo is the place to share flipbook animations - called Flipnotes - created and posted from Flipnote Studio on the Nintendo DSi and 3DS.

Learn how to Join!

Sign in | Help Center

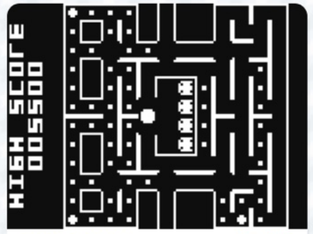
This week's topic is:
Slapstick Comedy
Have a laugh!

Popular This Month

Kanük×× ★ 827

CerealBowl ★ 846


J.A.STAFF ★ 560

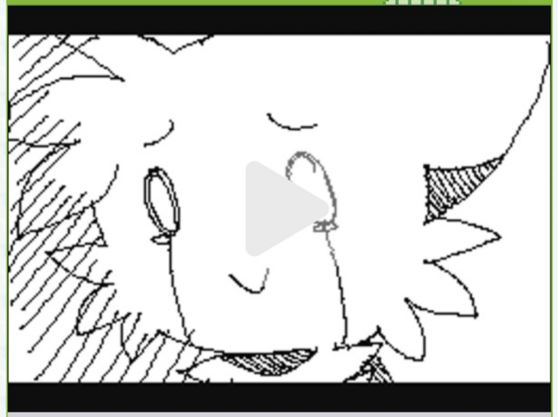


RETROMAN ★ 443

Flipnote Hatena Archive
Browse Now

Join the Sudomemo Discord!
discord.gg/sudomemo

Flipnote Spotlight



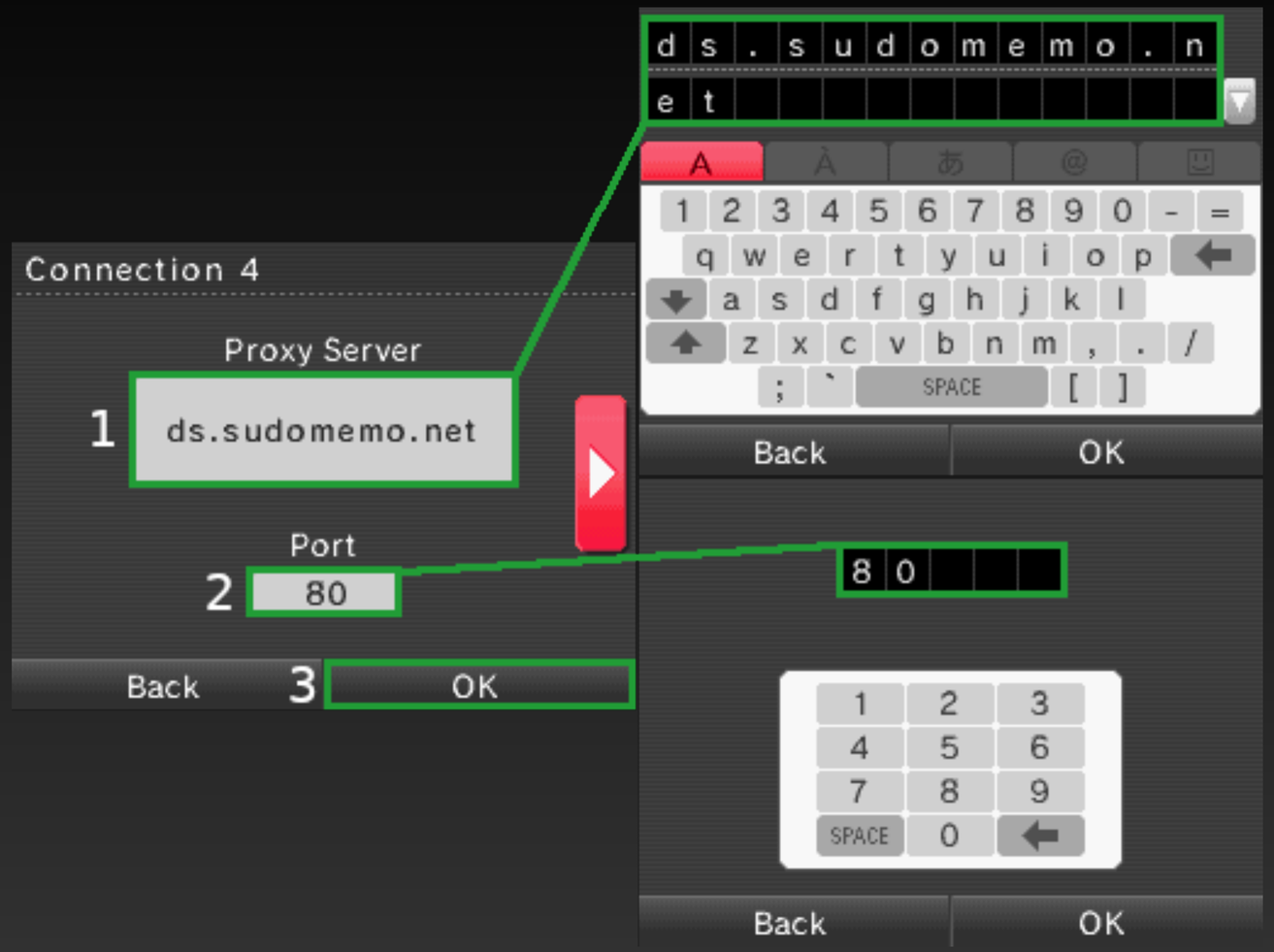
7,475 views

We need your help! Want to help us preserve Flipnote history? Get a cool exclusive theme, Sudomemo Plus, a special trophy, and color stars when you donate to the Flipnote Archive Ko-Fi!
https://t.co/vSQ6zqEpXSpic.twitter.com/Bo6p3VGP6H

— Flipnote Archive (@FlipnoteArchive) June 1, 2022

Trending Creators

1 Mizuka



- Fronting the web server with a reverse proxy
- Configured to forward ‘flipnote.hatena.com' to Sudomemo’s backend
- This works easily mostly by luck — Flipnote Studio sends full URIs in the HTTP GET
- This was enough for a long time...

SSL Shenanigans

- Years later, suddenly, the DSi stopped connecting to Sudomemo
- Turns out, there were *encrypted communications* before the main one
- These HTTPS requests handled authentication
  - Challenge-response, to prevent against spoofing someone else's DSi
- Up until now, these requests had been going through to Nintendo/Hatena as ever (so that Hatena could serve the shutdown info)...
  - But they eventually pulled the plug

What can we do?
The Wiimmfi option

- The Wiimmfi project was launched in the wake of Nintendo shutting down online play services for the Nintendo DS and Wii families — these were powered by GameSpy, who ceased operations in 2014
- Wiimmfi had solved the auth & matchmaking servers requiring SSL for Nintendo DS games by providing a patching tool; this simply changed ‘https’ -> ‘http’ (and the auth server hostname, for ease)
- Unfortunately, this meant users had to dump games and run them on a flashcart
  - Flash carts are increasingly hard to get, can be of dubious quality, and even banned in some countries
  - Plus, in practice, most people would end up just downloading ROMs someone else had patched…
- This wasn’t an option for Nintendo DSi; the only alternative, installing custom firmware, would be unpalatable to a large number of users
  - It’s fiddly, carries perceived risks, and looks too much like ‘hacking’ for many
  - Japanese users in particular seemed particularly averse to this sort of solution, for cultural reasons

The next best thing: exploiting Flipnote Studio

ugopwn

- shutterbug2000 found a way to exploit the PPM parser to gain arbitrary code execution
- Only worked on the USA version of Flipnote Studio, at first
  - Leaked before it was fully cooked
  - fincs and WinterMute of devkitPro reverse engineered it, and got it working for other regions
- A payload which patched the binary in-memory to change the server URLs and disable HTTPS was developed for Sudomemo supporters
  - Much improved, but it was still fiddly and sometimes unreliable

The panacea: nds-constrain't

Exploiting a vulnerability in the SSL library

- shutterbug2000 was not to be deterred, and started exploring the SSL libraries in Flipnote Studio
- We discovered that it didn't verify the Basic Constraints field on intermediate certificates...
- ...which wouldn't help us, if Nintendo hadn't signed a client certificate installed on *every Wii* with the same CA as they used to authenticate online play on Nintendo DS games(!)

Using nds-constrain't

- By using the Wii Shop client certificate (shared between all Wiis) and its private key, we could sign any certificate we want
  - As long as we include it in the chain back up to Nintendo's CA
- This meant changing the DNS settings on the console to a server we controlled was all users needed
- With a reverse proxy server to Wiimmfi, this also entirely removed the need to patch games for online play on the DS

https://github.com/Flipnote-Collective/flipnote-studio-docs/wiki

A collaborative effort between lots of hackers in the Flipnote community

What about Flipnote Studio 3D?

Flipnote Studio 3D

- Japanese exclusive until 2015
- No online service when it finally did make it abroad
  - Though community websites, subreddits, etc had some success in making up for the gap
- Flipnotes from Flipnote Hatena now only available within the 3DS app
  - No browsing or search; you had to know the 16-digit FSID for a creator
  - These were shared online, but the experience still left much to be desired
- We can do better than this!

New challenges

- Flipnote Studio 3D, like most other software on the 3DS by that point, encrypts all traffic with TLS
  - They didn’t make the same mistake with the SSL library as on the DSi
- This stops us easily snooping on what’s happening
- But, unlike the DSi, the 3DS has a proper operating system
- With custom firmware and patches, we can just ask the SSL sysmodule not to validate certs anywhere on the system

charlesproxy.com

Charles

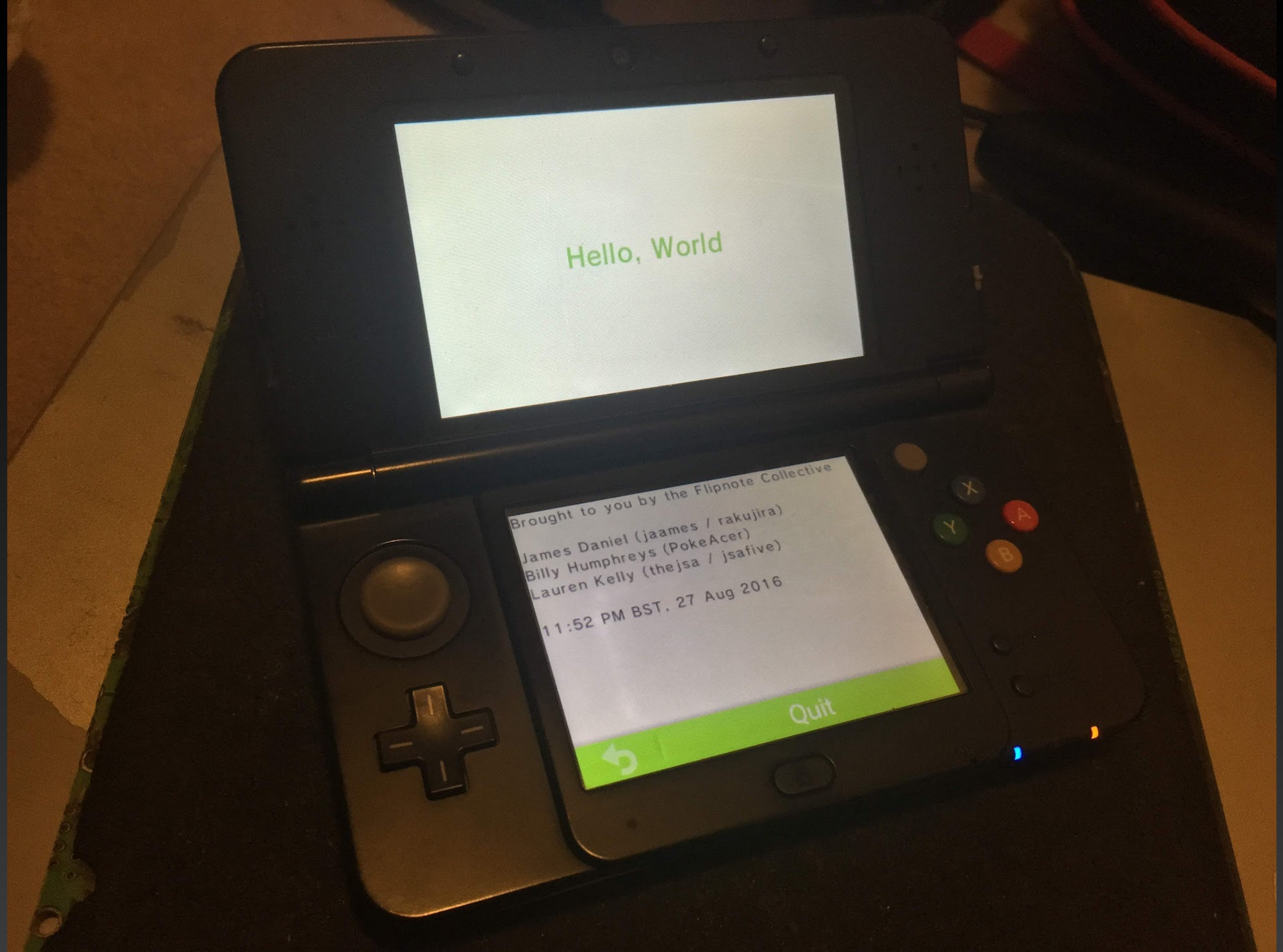
WEB DEBUGGING PROXY

v 4.6.3 Loading Preferences

Plus ça change, plus c’est la même chose

And now it’s *all* HTML

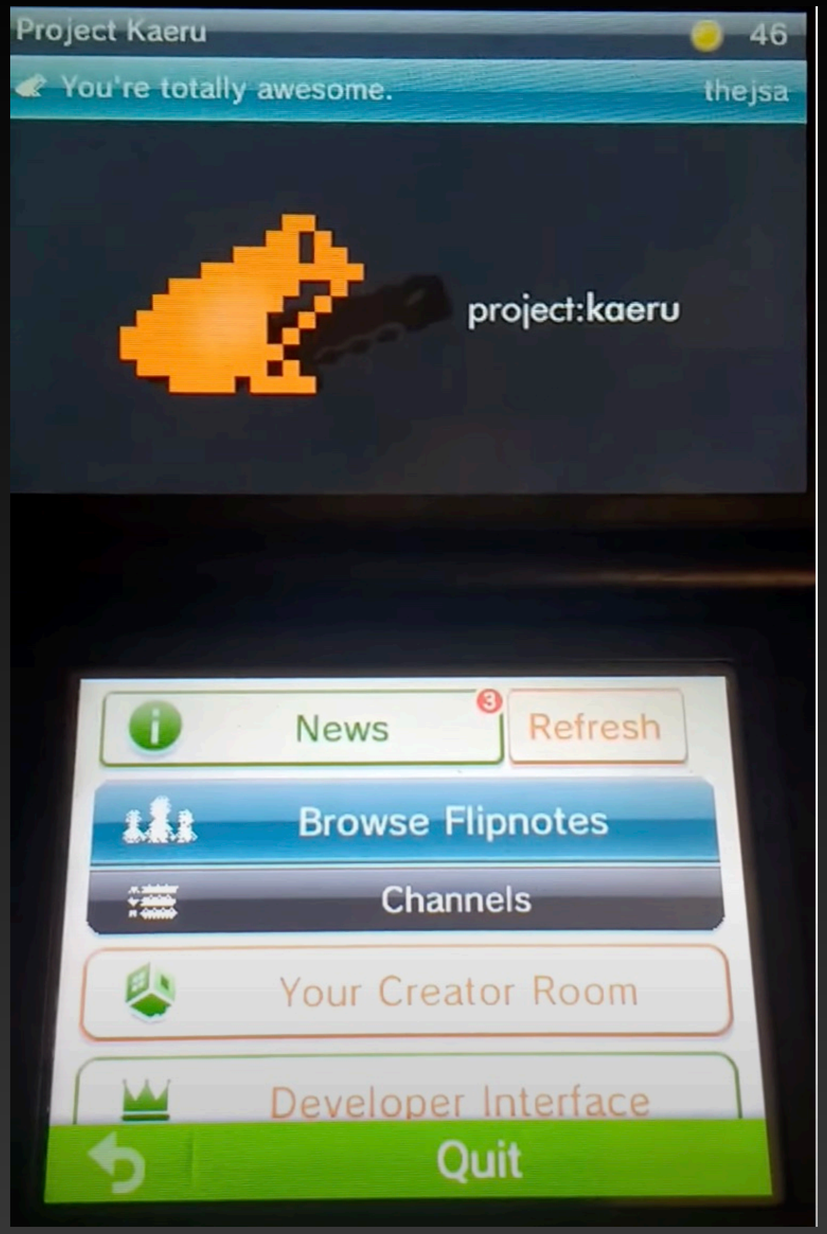
- Although Nintendo stripped all of the main online functionality from the global release of Flipnote Studio 3D, they preserved access to Flipnotes in the DSi Library
  - This worked like a stripped back version of Flipnote Gallery World
- Now that we were able to intercept the traffic, it turned out to be even less custom and weird than the DSi
  - HTML+CSS — even standard GIF images! — but many custom elements
- Much easier to work with than Flipnote Studio DSi’s weird binary formats


Hello, World
Brought to you by the Flipnote Collective
James Daniel (jaames / rakujira)
Billy Humphreys (PokeAcer)
Lauren Kelly (thejsa / jsafive)
11:52 PM BST, 27 Aug 2016
Quit
X
Y
A
B

‘Hello world’ becomes Kaeru World

Building an online service for Flipnote Studio 3D almost from scratch

- With our newfound knowledge, the Flipnote Collective (which sort of morphed and duplicated into what’s now Kaeru Team) set out to give users outside of Japan the online service for FS3D they were promised
- Starting point: sniffing Flipnote Gallery World on a Japanese 3DS to gather data on the custom elements
- We also carried out some static analysis on the 3DS game
  - Decompilation in IDA and, later, Ghidra
  - Just running the `strings` command(!)

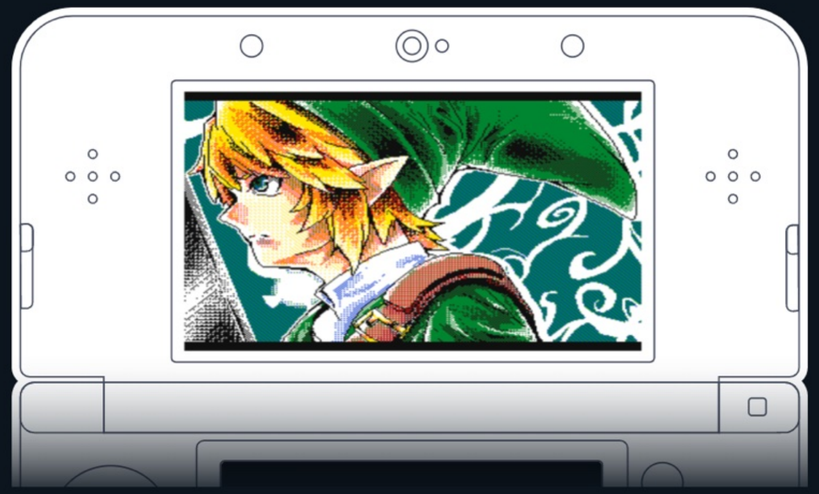

Project Kaeru
46
You're totally awesome.
thejsa
project:kaeru
News
3
Refresh
Browse Flipnotes
Channels
Your Creator Room
Developer Interface
Quit


Welcome back, KT.Lauren!
Kaeru Gallery
Star
3
2.4k
Users
3.3k
Flipnotes
3.5k
Comments
Created by Kaeru Team
Copyright © 2021
Lauren (jsa)
Creator's Room
Upload a Flipnote
Latest Flipnotes
View all...
Quit
X
Y
A
B
START

Kaeru Gallery

An online community for sharing animations from Flipnote Studio 3D, available worldwide on 3DS.

Connect your 3DS



4.4k Flipnotes

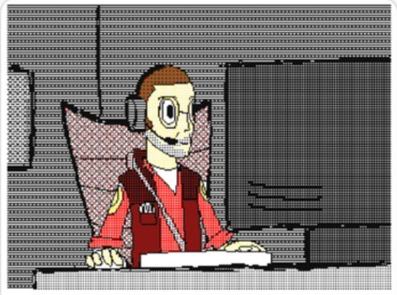
3.1k Users

4.2k Comments

Created by Kaeru Team

Top Flipnotes

See more...



sniper gaming
dq38

First FNS3D MV!
dq38

Spin-off

OTGW Toxic MV
Lame Kirby

Kaeru DSi Library

Access a wealth of Flipnotes from the DSi Flipnote Hatena service, right from within your browser.

Try it now »

Powered by Archive.org

Reflections

- Kaeru Gallery (originally known as ‘Project Kaeru’ and ‘Kaeru World’) had a higher barrier to entry than DSi Flipnote services like Sudomemo
- But it grew to be a tight-knit, friendly community, and a launching point for other exciting things
- Work by jaames and others on Flipnote.js enabled web-based playback
  - Later used by the Flipnote Archive project led by Sudomemo
  - 44 million Flipnotes from the DSi Library scraped from their (open!) S3 bucket; indexed and made viewable online
  - Bringing the work of 1.2 million creators back to life

https://github.com/Flipnote-Collective/flipnote-studio-3d-docs/wiki

Further developments

Acknowledgements

- jaames
- Billy Humphreys
- Austin Burk (sudofox)
- shutterbug2000
- Joshua Wickings (JoshuaDoes)
- InvoxiPlayGames
- Meemo
- Simon Aarons
- Khangaroo
- eta
- Many others I’ve no doubt missed

Contact:
https://www.evalauren.co.uk/
eva@evalauren.co.uk
Fedi: @eval@glauca.space