BACK IN THE GAME: PRIVACY CONCERNS OF SECOND-HAND GAME CONSOLES

Exposing personal data in used games consoles

Konstantinos Xynos (PhD)

17 Dec. 2025

This presentation is not related to my current employer.

WHO AM I

Konstantinos Xynos (PhD)

I work for a large automotive company (OEM) in Germany as an IT Security Architect. A software and hardware tinkerer. I am an ex-academic. I also enjoy writing and reviewing academic papers.

Special thanks to the co-authors:

K. Xynos, H. O. L. Read, I. Sutherland and M. Bovee, "Back in the Game: Privacy Concerns of Second-Hand Game Consoles," in IEEE Security & Privacy

PROBLEM STATEMENT

Persistent Data Risks

Residual personal information often remains on second-hand consoles despite encryption and resets.

Increasing Vulnerability Over Time

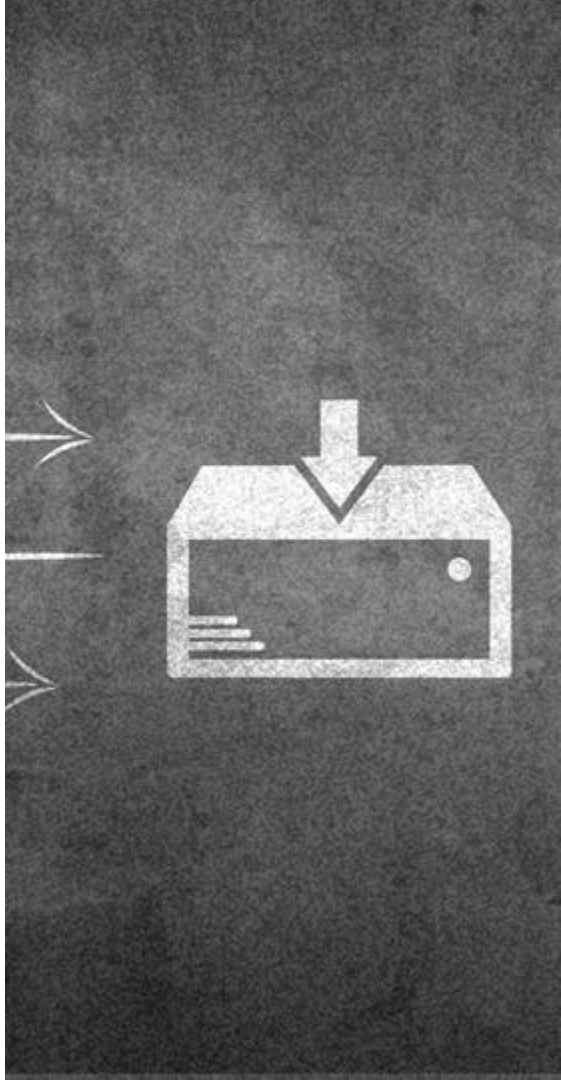
Older consoles are more prone to data breaches due to evolving exploits and forensic methods.

Misconception of Factory Reset

Factory resets do not guarantee complete data erasure, exposing consumers to privacy risks.

Need for Standardized Secure Wiping of Game Consoles

Lack of standardized secure wiping practices increases risks; research and industry support is required to provide solutions. Consumer groups and industry together with regulations like Cyber Resilience Act (EU) should pave the way.



RESEARCH OBJECTIVES

Personal Identifiable Information (PII) Exposure Investigation

Research focuses on identifying personal data exposure on used gaming consoles.

Lifecycle Privacy Risk Assessment

Our study assessed how privacy risks change across different console generations and usage periods (e.g., possible multiple owners).

Factory Reset and Encryption Analysis

Evaluating the effectiveness of factory resets and encryption in protecting user data.

Consumer and Vendor Recommendations

Providing actionable advice to reduce privacy risks when reselling consoles. Maybe even have resellers take action.

PRIOR WORK & APPROACH

*AI generated image

In our previous work, we investigated Nintendo's 3DS consoles. We combined knowledge from the game hacking community and got access to the system via root processes and analysing the systems binary blobs.

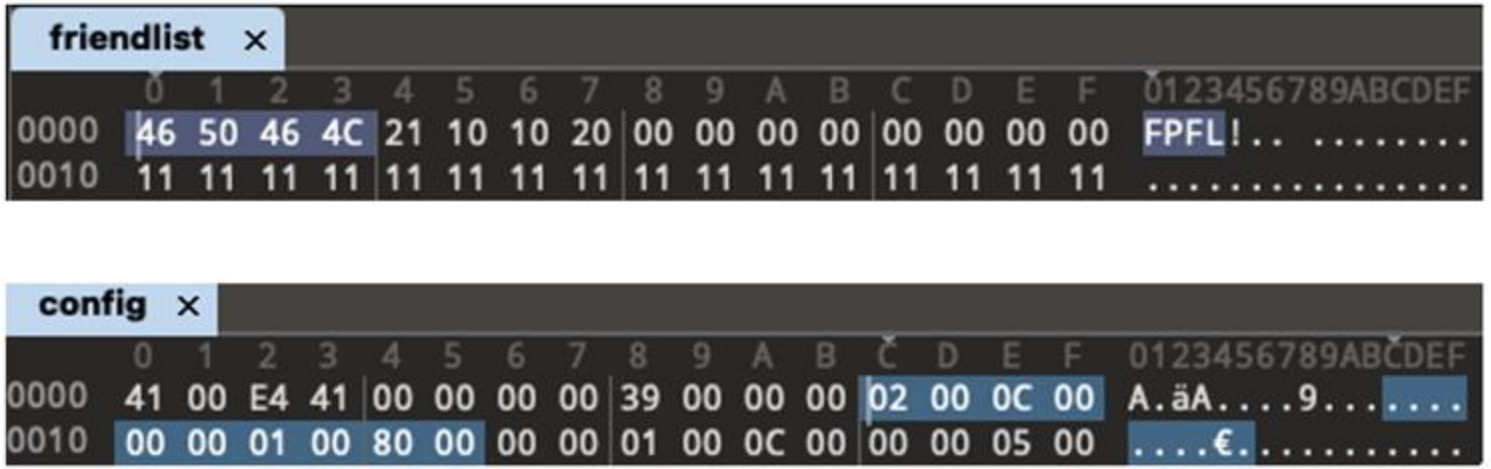
The gaming community also reversed the majority of the 3DS binary blobs. We used this knowledge to identify areas of interest.

We ended up creating custom binary parsers using the reversing knowledge found on 3dbrew.org

As part of this paper, we also expanded on that work and looked at recovering deleted data (i.e., in slack space).

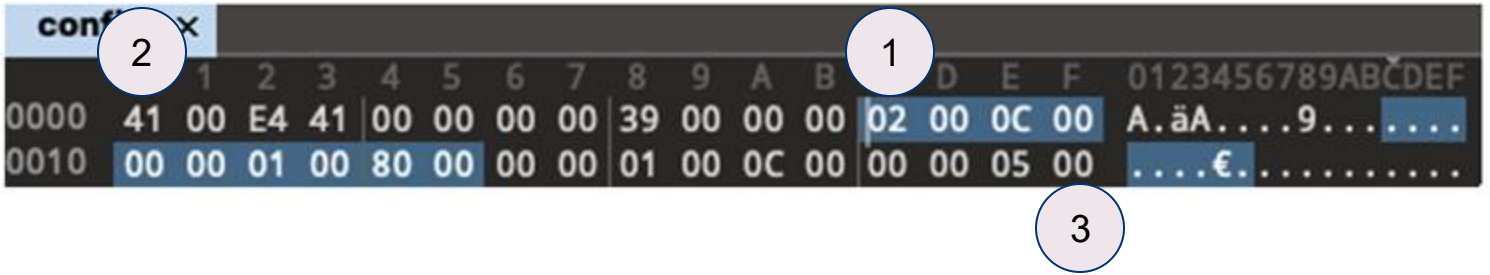
We identified parts of the binary and searched for them. From there we worked backwards to the start of the header and extracted the file in its totality. Like with any data carving process there were issues with the extraction but we still got data points.

It’s a Kind of Magic



(Top) friendlist file is identified by its “magic number”, i.e. *FPFL*. (Bottom) The 3DS’ config file is identified by a “byte sequence”, i.e. *0x02 00 0C 00 00 00 01 00 80 00*.

It’s a Kind of Magic - Data Carving example



Basic example of carving out data from slack space:

1) Find the magic number (or sequence) **highlighted section*
2) Move to the start (x number of bytes)
3) Extract size of the file that we had observed (this is an error prone process)

Questions ?

EXPLOITS AND DIGITAL FORENSICS

Digital forensic research on games consoles tend to follow an approach similar to the following:

1. Games console is released, “first look” research emerges identifying artifacts typically from the device’s user interface

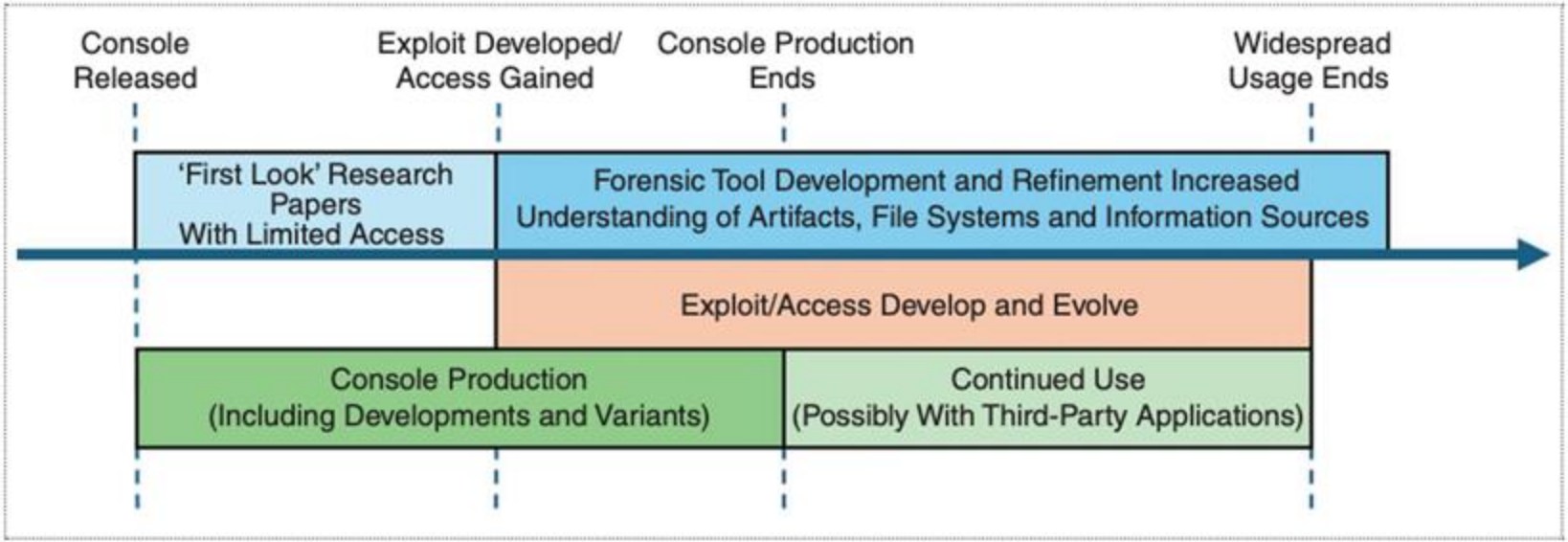
1. Once vulnerabilities have been found and exploits have been released, forensic researchers assess the impact of exploits and assess whether they improve existing forensic methodologies

Consoles that have had forensics research incorporating exploits are mentioned in the table.

One could say that, exploitation of a console is inevitable.

CONSOLE	RELEASE YEAR	EXPLOIT USED
Xbox	2001	Ndure
Wii	2006	BannerBomb
3DS	2011	ntrboot
Switch	2017	Fusée Gelée

LIFECYCLE OF GAMES ARTIFACTS



METHODOLOGY

Ethical and Legal Compliance
Institutional Review Board approval ensured ethical handling of potentially sensitive data during the research.

Blind Sourcing for Unbiased Sampling

The study used blind sourcing to collect second-hand consoles, ensuring unbiased and representative data sampling.

Forensic Tools and Exploits

Custom forensic tools and exploits like ntrboot and Fusée Gelée were employed to analyze Nintendo 3DS and Switch consoles respectively.

Data Decryption and Analysis

Decryption and signature-based file carving techniques allowed recovery and analysis of deleted files and personal information (PII).

Case Study

Analyzed two console families, Nintendo 3DS and Nintendo Switch

METHODOLOGY

a) New Nintendo 3DS XL exploited by ntrboot

b) Nintendo Switch exploited by Fusée Gelée

Questions ?

CASE STUDY 1: NINTENDO 3DS

Original Recovery:
Corpus of 47 Nintendo 3DS consoles created.

Developed tools extracted information from decrypted file system.

Extended Recovery:
Same corpus of 47 Nintendo 3DS consoles used.

Toolset extended to ignore filesystem, focus on byte sequences and magic numbers.

Identified deleted (*not yet overwritten*) data.

Artifacts indicate historical owners of devices.

ARTIFACT	ORIGINAL RECOVERY	EXTENDED RECOVERY
Username	57.4% (27)	93.6% (44)
Date of Birth	66% (31)	93.6% (44)
Email	2.1% (1)	6.4% (3)
Location	61.7% (29)	93.6% (44)
Mii from StreetPass	19.2% (9)	36.2% (17)
Friends list	2.1% (1)	31.9% (15)
Wi-Fi Config	20	50

CASE STUDY 2: NINTENDO SWITCH

Toolset developed by Barr-Smith et Al. (2021), tested against consoles with artificial datasets.

We performed analysis against 9 consoles purchased on second-hand market to determine if there is real risk to the consumer.

Data we recovered in table (to the right).

ARTIFACT	RECOVERY RATE
Wi-Fi SSID & Password	33.3% (3)
Email Address	44.4% (4)
Photos	55.6% (5)
User details (PII)	33.3% (3)

CONCLUSION

Privacy Risks of Residual Data

Residual personal information on used game consoles poses significant privacy risks to consumers. Poorly implemented encryption (unique persistent encryption keys) can expose residual data in future instances. Remove external media (SD cards etc.)

Lessons Learned

Limited lessons learned from the manufacturer since they reused the same architectural process for both consoles (similar filesystem and encryption techniques).

Limitations of Factory Resets

Factory reset is not enough to securely erase all personal data from consoles.

Need for Advanced Security Measures

New proactive and standardized solutions are needed to ensure secure data erasure on consoles. Manufacturers could provide independent assurance of how their devices could be sanitized before reselling to boost consumer confidence.

Direction for Future Research

Further studies should explore other console types and standardized data protection methods. In the end, consumer's data should also be considered and removed.

Thank you !

Any Questions ?

References

K. Xynos, H. O. L. Read, I. Sutherland and M. Bovee, "Back in the Game: Privacy Concerns of Second-Hand Game Consoles," in IEEE Security & Privacy, doi: 10.1109/MSEC.2025.3553038.

Frederick Barr-Smith, Thomas Farrant, Benjamin Leonard-Lagarde, Danny Rigby, Sash Rigby, Frederick Sibley-Calder, Dead Man's Switch: Forensic Autopsy of the Nintendo Switch, Forensic Science International: Digital Investigation, Volume 36, Supplement, 2021.

*Some images created using Microsoft’s Copilot, slides 1-4,14-16