Forensic Science International: Digital Investigation 50 (2024) 301815

Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

DFRWS APAC 2024 - Selected Papers from the 4th Annual Digital Forensics Research Conference APAC

Nintendo 3DS forensics: A secondhand case study

Huw O.L. Read [a,*], Konstantinos Xynos [b], Iain Sutherland [c], Matthew Bovee [a], Clyde Tamburro [a]

[a] Norwich University, 158 Harmon Drive, Northfield, 05663, VT, USA
[b] Mycenx Consultancy Services, Stuttgart, Germany
[c] Noroff University College, Tordenskjoldsgate 9, 4612, Kristiansand S, Norway

ARTICLE INFO

Keywords:
Nintendo 3DS
Forensics analysis
Second hand study
Games console
Data recovery
MicroSD
SD card

ABSTRACT

Computer and console-based video games are an important part of the entertainment industry. Such devices may be found in evidence lockers as part of investigations, or overlooked as their intrinsic value to an investigation may not be well-understood. Modern games consoles provide network connectivity and functionality that allows a significant degree of interaction via peer-to-peer connections and/or the Internet. These gaming consoles store settings, user preferences, user information, and can capture photos, audio and video, all of which potentially contain forensic artifacts about a person of interest. Games consoles have a fixed lifespan, eventually superseded by newer models with an expanded range of capabilities. As there are significant numbers of consoles available on the secondhand market, there is clear evidence that older consoles remain in circulation even after production has ceased. What is unclear, however, is the actual extent of forensic data available within these consoles. This paper shares the results of a digital forensic case-study undertaken to assess what artifacts are retrievable based on 'real-world' dataset, particularly the aging, but popular Nintendo 3DS series. A total of 47 Nintendo 3DS/2DS handheld systems were purchased secondhand. They were forensically imaged then examined to identify what artifacts are commonly found 'in the wild' on these often overlooked systems. Results presented in this paper provide guidance to digital forensic investigators of what may be realistically obtained from these non-traditional devices.

1. Introduction

The Nintendo 3DS was released in 2011 and was discontinued in September 2020. During this time-period nearly 76 million units were sold (Nintendo, 2021b). During the lifetime of a particular device, a game console's design will often be revised several times often with new or revised features. In the case of the Nintendo 3DS six versions of the console were produced: 3DS, 3DS XL, 2DS, New 3DS, New 3DS XL, and New 2DS XL (ordered by release date). For the purposes of this paper, the term 3DS will be used to address all devices interchangeably unless otherwise noted. A review of the consoles available for purchase on sites such as ebay.com or amazon.com with the search term 'Nintendo 3DS console' will identify thousands available for sale and just as many completed sales. This is not unique to the 3DS, or even to Nintendo, many thousands of used games systems (those that have reached end-of-life production runs for example) are freely bought and sold on the secondhand market.

Existing research tends to focus on extraction methodologies, less so on what is prevalent within such devices and of tangible use to the forensic investigator. This paper provides two key perspectives. Firstly, the case-study of secondhand consoles provides an invaluable opportunity to investigate actual artifacts that are available 'in the wild' for this type of non-traditional device. A secondary concern is whether such consoles pose a cybersecurity risk to organizations or individuals, particularly children, given the family-friendly nature of the Nintendo 3DS.

2. Related work

Horsman (2019) in exploring the need for forensic artifact research, noted that investigation and research often extends long after the production of software ceases as the software is still in use. This argument applies to games consoles that remain popular years after production ceases, and where networked functionality may be maintained by enthusiasts creating third party resources after the manufacturer support ends. One example for the Nintendo 3DS is the Pretendo network which provides online functionality for certain games (Pretendo, 2021). Research on the Nintendo 3DS is also included in the most recent

* Corresponding author.
E-mail address: hread@norwich.edu (H.O.L. Read).

https://doi.org/10.1016/j.fsidi.2024.301815

Available online 18 October 2024

Interpol review of digital evidence for 2019–2022 (Reedy, 2023).

2.1. Prior studies

Prior studies tend to focus on privacy concerns, highlighting information that the public are inadvertently releasing, rather than determining the prevalence of artifacts important to digital forensic examinations. The most significant studies of data remnants on devices that have been re-sold are in the form of traditional media-sources, including hard drive analyses media devices, and cellular devices. Hard drives have been well-documented (Sutherland and Jones (2008); Jones et al. (2010); Garfinkel (2012)) in literature. These previous studies highlighted the risk of disposing of improperly sanitized hard drives on the secondhand market and the ease with which the information can be recovered. The types of data recovered in their studies ranged from commercial enterprises that contained sensitive data (financial, customer information, network configuration and highly sensitive intellectual property) to personal drives, where the information could put the owners at risks of identity theft; some disks in the study contained names, addresses, bank information, volumes of communication on different email and social media platforms that had been saved on the device, scanned passports and in at least one case wedding and family history information which provided maiden names, commonly used in the UK as 'secret questions' to identify individuals. Most of disks examined in these studies contained a considerable volume of images. These were images of commercial activities, or personal family photographs. Other studies have focused on devices such as mobile phones (Glisson et al. (2016); Glisson et al. (2011); Jones et al. (2008)) and SD cards ((Szewczyk et al., 2020)) that have been re-used. It appears from a review of literature, no one has yet addressed residual data from games consoles from a forensics perspective.

2.2. Misuse and investigation of games consoles

Games consoles and their online ecosystems capture various artifacts that provide an indication of user activities and therefore consoles can feature in criminal investigations; the FBI requested information from Sony related to a PlayStation user using the console's communication functions to sell drugs (Brousil, 2019). Cobb and Flores (2015) describe how a murderer was found using evidence from an Xbox game card and gaming patterns to identify unusual patterns of behavior on the day of the murder. A college professor's murderers were found via their IP address when they connected a stolen Nintendo Switch to the Internet (AssociatedPress, 2019). Nintendo devices have featured in several criminal cases. In 2020 a US Army officer was imprisoned for sexually abusing his adopted daughter. The victim captured evidence of the attack using her Nintendo 3DS camera (Weston, 2020). Another victim in the UK used her Nintendo DSi in the same way to capture photographic evidence of her abuse (Telegraph, 2012). There are similar cases where photographic evidence relating to a case was captured using the Nintendo 3DS camera (Apellate Court of Connecticut, 2017) suggesting the Nintendo 3DS can be a useful source of photographic evidence. In one case in the UK an individual used a Nintendo 3DS to attempt to avoid detection when downloading child abuse material BBCNews (2021), suggesting web browsing may also be a useful artifact. Acquiring data on actual criminal cases involving games consoles can be challenging as noted by Sutherland et al. (2022) who explored investigations in the UK involving games consoles via a Freedom of Information request. The number of different police forces, the different approaches to the FOI request on the various games consoles and the terminology and ability to extract data (the term "DS" also refers to "Detective Sergeant", "Switch" also refers to "light switch") resulted in a complex picture although the Nintendo 3DS did appear in cases identified in the 2020 study.

2.3. Games console forensic analysis

Much of the prior work on games consoles have applied the forensic processes and procedures for extracting and interpreting artifacts from such systems. Studies have explored a range of devices including the Xbox One ((Moore et al., 2014; Khanji et al., 2016)), the Xbox360 hard drive Xynos et al. (2010) (Podhradsky et al., 2011). measured the efficacy of several tools that could manipulate an Xbox360 hard drive (Barr-Smith et al., 2021). analysed the Nintendo Switch and developed a module for Autopsy (Davies et al., 2015). performed a "first look" of a Sony Playstation 4, developing guidelines and methodologies for data extraction. Prior work on Nintendo 3DS games consoles ((Read et al., 2016; Pessolano et al., 2019)) compared the age-range classification of 3DS video games in the European (PEGI) and American (ESRB) markets, identifying a definite skew towards younger generations of players. Indeed, Nintendo stated the intended age range of the console in a support message as "People of any age can use and enjoy the Nintendo 3DS and Nintendo 3DS software" ((Nintendo, 2021a)). Both Read et al. (2016) and Pessolano et al. (2019) concluded that if a forensic investigation required the analysis of this type of device, it was likely to contain information regarding children. Xynos et al. (2023) presented a series of tools that automated the analysis of data extracted from the Nintendo 3DS to enable the investigator to easily extract and view user related data. Table 1 summarizes how many games consoles were used in each paper identified above. The focus has been on understanding these systems through decoding files and/or filesystems, thus few sample consoles were needed.

3. Contribution

A body of literature exists for extracting data in a forensically sound fashion from many games consoles (Table 1), but there does not appear to be a formal analysis of these devices from the secondhand market as there has been in prior studies (Section 2.1). This forensic case-study of a number of consoles would enable a perspective on;

- The types of evidence that can be typically recovered, given the capabilities of the device.
- Whether such artifacts identified in analysis studies (Table 1) appear 'in the wild'.
- If owners store personal data on such devices or use them purely as a gaming device.
- The relative ease with which this data can be recovered from the console, which will be of interest to forensic investigators.
- Whether proprietary binary formats only create a temporary barrier to data extraction.

This paper makes two contributions; firstly, it provides an overview of artifacts of interest to the forensic examiner based on analysis from a real-world dataset. Secondly, it identifies the risk posed to individuals from data contained within non-traditional devices. To the authors' knowledge, this paper is the first such formal forensic case-study across

Table 1
Quantity of samples in prior games console research.

Author	Type of Device	Quantity
This case-study	*Nintendo 3DS*	*47 used*
Xynos et al. (2010)	Xbox 360	1 unknown
Podhradsky et al. (2011)	Xbox 360	2 used
Moore et al. (2014)	Xbox 360	2 used
Davies et al. (2015)	Playstation 4	1 new
Khanji et al. (2016)	Xbox One, Playstation 4	1 each, unknown
Read et al. (2016)	Nintendo 3DS	1 unknown
Pessolano et al. (2019)	Nintendo 3DS	1 new, 3 used
Barr-Smith et al. (2021)	Nintendo Switch	1 new, 2 used
Xynos et al. (2023)	Nintendo 3DS	1 new

the domain of games consoles (Table 1). This research provides the results of analyzing 47 randomly sourced used consoles. This will assist in determining where an investigator should focus their efforts in an investigation.

4. Methodology

This study followed best practice as proposed byGlisson et al. (2016) and Garfinkel (2012) regarding the need for relevant advice and approval on the appropriate legal and ethical processes required to run a study of this type where data is collected from devices that refer to living individuals. The authors sought and received IRB approval for this research.

4.1. Console acquisition

The research followed forensic best practice with the consoles (both the physical devices and their extractions) securely stored pre- and post-imaging. Extracted data was assessed with encrypted channels and as the game consoles were purchased in the USA all data was also stored and processed in the USA. A total of 47 Nintendo 3DS handheld games consoles were purchased on the secondhand market from various sources over several months. Following the methodology described in Sutherland and Jones (2008), Jones et al. (2008, 2010) the consoles were blind purchased to confirm that the researchers analyzing the consoles had no information on provenance, ensuring no bias was introduced into the study. All purchasing decisions were made by staff who were not involved in the analysis. The range of different consoles purchased for the study are shown in Table 2. Examples are shown in Fig. 1.

4.2. Data acquisition and further analysis

The Nintendo 3DS contains two storage media of interest to this study. The first is the NAND chip soldered onto the motherboard, the second is the SD card, or microSD on those with the "new" moniker (henceforth microSD). If the microSD card was supplied with the console, it was connected through a write blocker (Cellebrite Memory Card Reader, model #A-CRD-01-005) and a physical image was taken in the Expert Witness Disk Image Format (EWF) using Exterro's FTK Imager. The acquisition of the NAND was less-straightforward; the method presented by Pessolano et al. (2019) was used to create a forensic copy of the NAND, verified by SHA hashes. For identification and record keeping purposes the NAND and microSD images were renamed to match the serial number of the console; e.g. SW123456789.bin (NAND), SW123456789.E01 (microSD). Both NAND and microSD extractions were kept in the same folder and stored on an encrypted server. With regards to analysis, a two-step approach was deployed. Firstly, a data-carving process took place using Exterro FTK 7.1 on the internal memory (NAND) and, if present, the microSD card. The authors sought to identify pictures, audio, and video from the data carving process (larger than 20 kb), in a manner similar to Pessolano et al. (2019) initial experiments. Of particular interest were any files that could conceivably be used to identify an individual, rather than content captured from playing video games (i.e. screenshots etc.). Secondly, a detailed analysis of files on the NAND took place. This was made possible due to the prior work by Xynos et al. (2023) who developed a suite of tools for decoding and extracting artifacts from the Nintendo 3DS devices. In their paper, 16 tools were developed and made available to the authors for the purpose of this research. These tools could decode information that would otherwise be unavailable in Exterro's FTK; though the filesystem was recognized (the NAND is FAT16), the file types were not. The decoded information on the NAND for each of the 47 devices was captured as text files and compared for artifacts. Furthermore, the authors were able to extend the functionality of the Xynos toolset (Xynos et al., 2023) by decoding an additional structure, the "meet.dat" file which contains the data collected by the StreetPass function and used by StreetPass Mii Plaza. StreetPass passively communicates with other consoles within close proximity and shares the Mii character information. Of particular interest to the forensic investigator is that the data structure containing the Miis received from other consoles also contains the Mii creator's MAC Address, their name (may be an alias), their System's ID, the device the Mii was originally created on (Wii, DS, 3DS, or Wii U/Switch), and the time the Mii was created on the originator's console (seconds since January 1st, 2010). This file exists within the 'sysdata/000XXXXX/00000000' on the NAND, where 'XXXXX" represents the region; 00020218 (US), 00020228 (EU) or 00020208 (JP), for example on a console from the USA this value would be: 'sysdata/00020218/00000000'. The first entry is the Owner's Mii data (at offset 0x04). Then the remainder of the Mii database starts with the magic bytes (MTDB, 0x4D 54 44 42 at offset 0x70) followed by 2 unknown bytes and then 2 bytes starting at offset 0x76 denoting the total number of entries held. The first entry is set as zero and if the list is empty then the bytes are set to (0xFF FF). The maximum number of entries is 1000, or 999 (0xE7 03) since the index starts from zero (0). Then there is an initial short lookup table of all the stored Mii characters. The Mii ID (4 bytes), MAC address (6 bytes) and 2x unknown 2 byte values make up the 14 bytes (0xE) entries up until offset 0x3727 (14119). Then there are 8 bytes of unknown data. We now reach offset 0x3730h (14128) where the shared Mii characters [30] are stored in 264 bytes (0x108). The data in these structures are known and include, but not limited to, which device (3DS, Wii, Switch etc) was used to create the Mii, System ID, Mii ID, MAC Address, Country, State, Day and Month of Birthday of the Mii, when the Mii was created. This information is summarized in Table 3. The game hacking community has detailed some of their findings on gbatemp.net and demonstrated them with applications that jump to specific offsets modifying the meet.dat file to unlock achievements. This is significantly past the offsets of Mii characters and is outside the scope of this paper.

Table 2
Consoles purchased by version.

3DS	3DS XL	2DS	New 3DS	New 3DS XL	New 3DS XL
7	11	8	1	13	7
11.9 %	23.4 %	17 %	2.1 %	27.7 %	14.9 %

5. Results

A total of 47 secondhand consoles were analyzed in this case-study. Of these, 36 (76.5 %) had a microSD card present. The 3DS is capable of storing digital photographs, video, and audio on both the internal NAND and the microSD card. It will default to the microSD if one is present unless it is at capacity and overflows onto the NAND. Table 4 provides a summary of how many devices contained artifacts (as opposed to video game-related recordings or appearing empty). 'Per Console' identifies if a Nintendo 3DS had photo, video or audio data on any of its storage (i.e. NAND and microSD, if present). 'Internal NAND' and 'microSD' provide a detailed breakdown of how often such data was found on that type of storage.

Characterizing this dataset further proved to be rather subjective; therefore each console was analyzed by a lead reviewer, and later confirmed by a second. In this fashion the categories identified in Table 5 began to emerge.

Of particular interest to the authors (and we hope, the community) is any information that may be deemed of a more personal nature. In particular, the following broad categories emerged:

- *Home:* Evidence that identifies the inside of what appears to be someone's private residence, including rooms of the house (bedroom, kitchen, bathroom, etc.).

Fig. 1. 3DS Family (clockwise, from top left), 3DS, 3DS XL, New 3DS, New 2DS XL, New 3DS XL, 2DS.

Table 3
Section MTDB of the meet.dat structures and artifacts.

meet.dat offset (hex)	Length (bytes)	Description
0x70	4	0x4D 54 44 42 ("MTDB" Magic)
0x74	2	Unknown
0x76	2	Number of entries (0xFF FF for no entries). Max. of 1000.
0x78	4	Mii ID
0x7B	6	Mac Address of Mii's Creator
0x80	4	Unknown
The 0x0D bytes from 0x78 to 0x84 represent one Mii lookup. This structure is repeated 0x3E8 times		
0x3728	8	Unknown
0x3730	264	Mii character entry

There are a maximum of 0x03E8 Mii characters, unused entries have null values 0xFF7F.

Table 4
Personal data artifacts found.

Storage [n = total]	Photos	Videos	Audio
Per Console [47]	32 (68.1 %)	17 (36.2 %)	24 (51.1 %)
Internal NAND [47]	11 (23.4 %)	0 (0 %)	1 (2.13 %)
microSD [36]	28 (77.8 %)	17 (47.2 %)	24 (66.7 %)

Table 5
Artifacts within specific categories.

Category	Photo	Video	Audio
Home	23 (48.9 %)	12 (25.5 %)	0 (0.0 %)
Public location	7 (14.9 %)	1 (2.1 %)	0 (0.0 %)
Vehicle	8 (17 %)	3 (6.4 %)	0 (0.0 %)
Adult	22 (46.8 %)	8 (17.0 %)	7 (14.9 %)
Child	27 (57.5 %)	13 (27.7 %)	17 (36.2 %)
Names	4 (8.5 %)	7 (14.89 %)	3 (6.4 %)

- *Public Location:* Media that could lead to someone's geographic location being revealed, either directly due to an address or recognizable location, or via Open-Source Intelligence (OSINT) techniques. May include clear background audio indicating a public location.
- *Vehicle:* Data indicating a vehicle travel (interior photos or video taken from a car) or information related to travel. Including audio suggesting vehicle travel.
- *Adult/Child:* Media that would identify someone who appears to belong to a particular age category, what they look or sound like.
- *Names:* Identifiable names are either spoken in video/audio tracks or visible in photos.

The data extracted from the consoles ranged from minimal, with limited configuration data, to more comprehensive and potentially private information that would allow someone to identify multiple individuals. Key information found on the consoles is summarized in Table 6. Captured data included network credentials (SSID and plaintext password) for connected networks, avatar information (Mii avatars with information about individuals the console may have interacted with),

Table 6
Types of information recovered in the study. *Each device is capable of storing up to three SSID/Password entries.

Type of Artifact Recovered	Quantity [47]
Username as recorded in the console	27 (57.4 %)
Partial Date of Birth as captured in the console	31 (66 %)
User(s) avatars, on the 3DS known as a Mii	9 (19.1 %)
Email addresses (parental contact email)	1 (2.1 %)
Wireless configuration (Password information)*	20 (42.5 %)
Blocklist	0 (0.0 %)
Mac Address	16 (66 %)
Consoles with one or more SSID/Passwords*	13 (28 %)
Location (Country, State)	29 (61.7 %)
Web Browser/History	4 (8.5 %)
Gameplay information	16 (34 %)
Meet.dat file contains Mii from StreetPass	9 (19.2 %)
GameNote images	13 (28 %)
Timestamps associated with game playing	16 (34.1 %)
Pedometer information (steps, date & time)	27 (57.4 %)

owner's name, game play activity (duration of play and dates for the first and last play of a game), parental security settings and contact emails and which country and state were selected during setup of the console by the user (i.e. owner). Of all the types that could be found with the toolset from Xynos et al. (2023), only the *blocklist* artifact was not found across all the samples. The blocklist is a data structure that stores users "blocked" by the console's owner; this merely suggests that very few (or none!) ever block communication with other users.

The consoles record the user's county selection. In the USA, the state is recorded and the console will then allocate the state's capital. Therefore, the level of granularity is limited to the state. This is still concerning when combined with the photos on the console and landmarks that would facilitate OSINT efforts. The locations recorded in the sample set are shown in Fig. 2. In the sample set, 29 consoles (61.7 %) contained location (country and state) information. In particular, the following were identified: 15 unique American states, Washington D.C., Berlin (Germany), and Anguilla (British Overseas Territories).

6. Artifacts discovered

Artifacts found across the games console dataset were in one of two categories. The first is of a more personal nature (i.e. photograph/video/audio) which could conceivably be used to identify an individual. The second is of a more technical nature (i.e. usage logs, network data such as MAC addresses and WiFi information) which could be used to identify games console usage.

6.1. Artifacts of a personal nature

The camera and microphone features were frequently used, 32 (68.1 %) consoles exhibited photographs, 17 (36.2 %) exhibited videos, and 24 (51.1 %) contained audio that were recorded using the system (Table 4). Nine (9) consoles had over 500 images and of those five (5) had over 1000 images. Six (6) consoles had over 10 videos and of those three (3) had over 50. Likewise, eight (8) consoles had over 10 audio clips and of these four (4) had over 30. Some images across the dataset were of a personal nature. This is to be expected given the consoles are mainly used by children; there were examples of children taking pictures of themselves, other family members, and pets. A small number of images could have been considered of a private and personal nature, that an owner would wish to sanitize before disposing of the console. Images, video, and audio included recordings of the inside and outside of the family home providing some additional location information and the ability to identify landmarks, vehicles parked outside the home with license plates clearly visible, school banners with the name (and location) of the school visible, the owner's gaming interests (types of games and how long they played each one), children and babies at play in a relaxed home setting, conversations between children, recordings of parents/guardians, recognizable names of children obtained via photo, video, audio samples. Read et al. (2016) and Pessolano et al. (2019) suggested that, as 3DS consoles had many games designed for a younger audience, they were more likely to hold data about children. The results in Table 5 appear to corroborate this claim, with more data about children present than adults in the Photo, Video, and Audio categories.

6.2. Artifacts of a technical nature

Many of the consoles retained their WiFi settings. Twenty (20) SSIDs were recoverable, nineteen (19) plaintext passwords were recoverable for these SSIDs. One (1) SSID was not protected, no password was present. Of the 47 consoles in the dataset, 7 had one SSID set, 5 had two SSIDs set, 1 had three SSIDs set. WiFi password patterns included family surname, locations, favorite sports group, and affiliations. The following were also recovered: parental control email addresses that contain parents first name and surname, and partial dates of birth (month/year) entered into the system (via Mii avatars). Mii characters shared from other consoles (as part of StreetPass Mii Plaza) contained the MAC address and Mii created time from the originating console, providing evidence of games systems in close proximity to one another.

Fig. 2. Extracted state information, # of consoles.

7. Discussion and impact

This work represents a study of the 'real-world' artifacts found on these secondhand consoles with the aim of informing digital forensic investigations. To the authors' knowledge this is the first such case-study on game consoles. Furthermore, secondhand markets are the best option from both an environmental and the user's financial perspective. However, security and the presence of personal data, as is often the case, is an afterthought. These consoles may have been used for an extended period. Users may not recall all the information they added into a console. The presence of a microSD memory card in a games console with old photos and information may be forgotten. Users need to be reminded of the potential risks especially where consoles are used by those under 18 years of age. Overall, it is reasonable to argue that the amount and nature of information present in the consoles and on SD cards can present a security risk. This has been highlighted in previous studies on residual data on SD Cards (Szewczyk et al., 2020). Elements in the information gathered in this case-study may be considered innocuous, but the aggregation of data can support a forensic investigation. The consoles contain coordinates providing information on the registered location. In some cases, this may be a location with a small population size, as in the case of the consoles from Anguilla. These islands have a population of just over 15,000 people, so if the user was a local it might be possible to locate the owner of the device. In other cases, if the location information is augmented by OSINT an exact location may be found. One example from this study, a video taken by a child from a moving car enabled an exact address to be located using landmarks. In a further example, where the aggregate data was examined, it was possible to determine that the Nintendo 3DS was registered in the continental USA. The analysis from analyzing photographic evidence indicated it was most likely owned by a young girl, leading to identification of the state, the school she attended, and the address of the school with relative ease. Names appearing in photographs recorded in the console suggest potential names for the girl and/or siblings, who were also present in photographs on the device. If pictures have been deleted from an SD card, but not erased/wiped, they can be recovered using freely available tools that require a limited skill level (e.g. PhotoRec). These present a wealth of information depending on the content of the media as outlined above. The process of accessing the console NAND, while complicated, is a publicly available technique (Pessolano et al., 2019). In this study the tools described in Xynos et al. (2023) were used to automate the recovery of the data. Knowing such artifacts commonly appear in real-word data will enable an analyst to expand their investigation to include such non-traditional devices which would otherwise be overlooked.

8. Conclusions

Over 76 million Nintendo 3DS consoles were produced and they can still be found for sale in secondhand markets and have been demonstrably seized as evidence (Sutherland et al., 2022). The nature of a portable games console is that it is carried on the person and mainly used by one user. Some games even encourage the user to keep the device with them, for instance, coins for steps made, having Streetpass enabled to capture new Mii characters all lead to rewarding the owners with game achievements. This case-study demonstrates an indication of the actual type and number of artifacts left behind on used consoles. It is possible to find significant amounts of artifacts relating to personal data remaining on consoles and their microSDs. Furthermore, this should serve as a reminder of cybersecurity best-practices to organizations, of the consoles examined 13 (28 %) had recoverable SSID and passwords allowing a would-be attacker access onto a network. This research highlights types of forensic artifacts, observed 'in the wild', from non-traditional devices that an investigator may utilize during an investigation. The findings, in Section 5, suggest that depending on the type of crime these consoles can provide useful artifacts through photographic and video material, network credentials, personal notes, web browser history, friend interactions, and gameplay timing and periods amounting to a considerable trove of personal information.

Future work

Future work includes modifying the toolset to further decode artifacts from the extracted files. This study could also be extended to include a larger number of Nintendo 3DS consoles covering several different continents to further explore artifacts from a national perspective. Additional studies on different game consoles may support the findings in this paper. We also propose that digital forensics researchers should consider other non-traditional devices.

Declaration of competing interest

The authors are not aware of any conflicts of interest.

Acknowledgements

The authors would also like to acknowledge the following support and contribution to this project: Ignacio 'Inaki' Lopez for his insights in reversing binary formats and data structures.

Student project work by Mr. Paul Bierro and Ms. Trang Do, Julia Munroe and Kathleen Covino.

Assistance of Norwich University Office of Academic Research.

Ethical approval for this project was via Norwich University Institutional Review Board.

This material is based upon work supported by the National Science Foundation under Grant #1754014. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

This material is based upon work supported by the National Security Agency under Grant #H98230-19-1-0152. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Security Agency.

References

Apellate Court of Connecticut, 2017. State V. Purcell, 166 A.3d 883, 174 Conn. App., vol. 401. https://cite.case.law/a3d/166/883/, 15-07-2024.

AssociatedPress, 2019. Police Trace Stolen Nintendo System to Suspects in Slaying. https://apnews.com/general-news-40e5422678dc6bb89362616e6ef86781, 15-07-2024.

Barr-Smith, F., Farrant, T., Leonard-Lagarde, B., Rigby, D., Rigby, S., Sibley-Calder, F., 2021. Dead man's switch: forensic autopsy of the nintendo switch. Forensic Sci. Int.: Digit. Invest. 36, 301110 https://doi.org/10.1016/j.fsidi.2021.301110. URL: https://www.sciencedirect.com/science/article/pii/S2666281721000044. dFRWS 2021 EU - Selected Papers and Extended Abstracts of the Eighth Annual DFRWS Europe Conference.

BBCNews, 2021. Special Olympics Winner Caught with Abuse Images for Second Time. https://www.bbc.com/news/uk-scotland-tayside-central-58383718, 15-07-2024.

Brousil, B., 2019. Affidavit in Support of Search Warrant. URL: https://ia803105.us.archive.org/26/items/playstationseachwarrantapplication/PlayStation-Seach-Warrant-Application.pdf, 15-07-2024.

Cobb, G., Flores, M., 2015. A Murder Case with No Body. https://www.tdcaa.com/journal/a-murder-case-with-no-body/, 15-07-2024.

Davies, M., Read, H., Xynos, K., Sutherland, I., 2015. Forensic analysis of a sony playstation 4: a first look. Digit. Invest. 12, S81–S89. https://doi.org/10.1016/j.diin.2015.01.013. URL: https://www.sciencedirect.com/science/article/pii/S1742287615000146. dFRWS 2015 Europe.

Garfinkel, S., 2012. Lessons learned writing digital forensics tools and managing a 30tb digital evidence corpus. Digit. Invest. 9, S80–S89. https://doi.org/10.1016/j.diin.2012.05.002. URL: https://www.sciencedirect.com/science/article/pii/S1742287612000278 (the Proceedings of the Twelfth Annual DFRWS Conference).

Glisson, W.B., Storer, T., Blyth, A., Grispos, G., Campbell, M., 2016. In-the-wild residual data research and privacy. Journal of Digital Forensics, Security and Law 11. https://doi.org/10.15394/jdfsl.2016.1371. URL: https://commons.erau.edu/jdfsl/vol11/iss1/1.

Glisson, W.B., Storer, T., Mayall, G., Moug, Iainand, Grispos, G., 2011. Electronic retention: what does your mobile phone reveal about you? Int. J. Inf. Secur. 10, S337–S349. https://doi.org/10.1007/s10207-011-0144-3.

Horsman, G., 2019. Raiders of the lost artefacts: championing the need for digital forensics research. Forensic Sci. Int.: Reports 1, 100003. https://doi.org/10.1016/j.fsir.2019.100003. URL: https://www.sciencedirect.com/science/article/pii/S2665910719300039.

Jones, A., Valli, C., Dardick, G., Sutherland, I., Dabibi, G., Davies, G., 2010. The 2009 analysis of information remaining on disks offered for sale on the second hand market. Journal of Digital Forensics, Security and Law. https://doi.org/10.15394/jdfsl.2010.1083.

Jones, A., Valli, C., Sutherland, I., 2008. Analysis of Information Remaining on Hand Held Devices Offered for Sale on the Second Hand Market, vol. 3. ECU Publications. https://doi.org/10.15394/jdfsl.2008.1041.

Khanji, S., Jabir, R., Iqbal, F., Marrington, A., 2016. Forensic analysis of xbox one and playstation 4 gaming consoles. In: 2016 IEEE International Workshop on Information Forensics and Security (WIFS), pp. 1–6. https://doi.org/10.1109/WIFS.2016.7823917.

Moore, J., Baggili, I., Marrington, A., Rodrigues, A., 2014. Preliminary forensic analysis of the xbox one. Digit. Invest. 11, S57–S65. https://doi.org/10.1016/j.diin.2014.05.014. URL: https://www.sciencedirect.com/science/article/pii/S1742287614000577. fourteenth Annual DFRWS Conference).

Nintendo, 2021a. For Which Age Ranges Is the Nintendo 3DS System Recommended? — nintendo.Co.uk. https://www.nintendo.co.uk/Support/Nintendo-3DS-2DS/FAQ/Safety/For-which-age-ranges-is-the-Nintendo-3DS-system-recommended-/For-which-age-ranges-is-the-Nintendo-3DS-system-recommended-244139.html, 15-07-2024.

Nintendo, 2021b. IR Information : Sales Data - Dedicated Video Game Sales Units — nintendo.co.Jp. https://www.nintendo.co.jp/ir/en/finance/hard_soft/index.html, 15-07-2024.

Pessolano, G., Read, H.O., Sutherland, I., Xynos, K., 2019. Forensic analysis of the nintendo 3ds nand. Digit. Invest. 29, S61–S70. https://doi.org/10.1016/j.diin.2019.04.015. URL: https://www.sciencedirect.com/science/article/pii/S1742287619301641.

Podhradsky, A.L., D'Ovidio, R., Casey, C., 2011. A practitioners guide to the forensic investigation of xbox 360 gaming consoles. In: Annual ADFSL Conference on Digital Forensics, Security and Law 9. URL: https://commons.erau.edu/adfsl/2011/wednesday/9.

Pretendo, 2021. Game Servers Recreated. https://pretendo.network, 15-07-2024.

Read, H., Thomas, E., Sutherland, I., Xynos, K., Burgess, M., 2016. A forensic methodology for analyzing nintendo 3ds devices. In: Peterson, G., Shenoi, S. (Eds.), Advances in Digital Forensics XII. Springer International Publishing, Cham, pp. 127–143.

Reedy, P., 2023. Interpol review of digital evidence for 2019–2022. Forensic Sci. Int.: Synergy 6, 100313. https://doi.org/10.1016/j.fsisyn.2022.100313. URL: https://www.sciencedirect.com/science/article/pii/S2589871X22000985.

Sutherland, I., Jones, A., 2008. Indstrial espionage from residual data: risks and countermeasures. In: 6th Australian Digital Forensics Conference Edith Cowan University. https://doi.org/10.4225/75/57b2771540cc2.

Sutherland, I., Read, H., Xynos, K., 2022. An analysis of the prevalence of game consoles in criminal investigations in the United Kingdom. In: European Conference on Cyber Warfare and Security, vol. 21, pp. 289–295. https://doi.org/10.34190/eccws.21.1.497.

Szewczyk, P., Sansurooah, K., Williams, P., 2020. An Australian Longitudinal Study into Remnant Data Recovered from Second-Hand Memory Cards, pp. 542–559. https://doi.org/10.4018/978-1-7998-3025-2.ch035.

Telegraph, 2012. Paedophile Caught after Victim Takes Picture Using Nintendo Game — telegraph.Co.uk. https://www.telegraph.co.uk/news/uknews/crime/9171452/Paedophile-caught-after-victim-takes-picture-using-Nintendo-game.html, 15-07-2024.

Weston, A., 2020. N.C. Army Soldier Sentenced to Life for Sexual Abuse of Adopted Daughter. https://wcti12.com/news/state-news/nc-army-soldier-sentenced-to-life-for-sexual-abuse-of-adopted-daughter, 15-07-2024.

Xynos, K., Harries, S., Sutherland, I., Davies, G., Blyth, A., 2010. Xbox 360: a digital forensic investigation of the hard disk drive. Digit. Invest. 6, 104–111. https://doi.org/10.1016/j.diin.2010.02.004. URL: https://www.sciencedirect.com/science/article/pii/S1742287610000125. embedded Systems Forensics: Smart Phones, GPS Devices, and Gaming Consoles).

Xynos, K., Read, H., Sutherland, I., Bovee, M., Do, T., 2023. Nintendo 3DS Forensic Examination Tools. Springer, Nature Switzerland, Cham, pp. 55–70. https://doi.org/10.1007/978-3-031-42991-0_4.