A Forensic Methodology for Analyzing Nintendo 3DS Devices

Huw Read, Elizabeth Thomas, Iain Sutherland, Konstantinos Xynos, Mikhaila Burgess

Chapter 7

A FORENSIC METHODOLOGY FOR ANALYZING NINTENDO 3DS DEVICES

Huw Read, Elizabeth Thomas, Iain Sutherland, Konstantinos Xynos and Mikhaila Burgess

Abstract Handheld video game consoles have evolved much like their desktop counterparts over the years. The most recent eighth generation of game consoles are now defined not by their ability to interact online using a web browser, but by the social media facilities they now provide. This chapter describes a forensic methodology for analyzing Nintendo 3DS handheld video game consoles, demonstrating their potential for misuse and highlighting areas where evidence may reside. Empirical research has led to the formulation of a detailed methodology that can assist forensic examiners in maximizing evidence extraction while minimizing, if not preventing, the destruction of information.

Keywords: Video game consoles, Nintendo 3DS, forensic analysis methodology

1. Introduction

The 3DS, released in Japan in February 2011, is Nintendo's latest handheld platform. At the time of writing this chapter, more than 45 million units have been sold worldwide [17], making the 3DS one of the most popular eighth generation handheld video game consoles. Nintendo has upgraded the 3DS over its lifespan and has created several revisions with features such as larger screens (3DS XL), improved hardware ("new" Nintendo 3DS) and a "lite" version (2DS).

Like its predecessor, the Nintendo DS, the 3DS is Wi-Fi enabled and connects to the Internet. It has a built-in web browser, an email-like system and, as in the case of the DSi, a digital camera. The defining changes to the 3DS over its predecessors are enhanced social media, new sharing features and access to an app store from the device. Built-in functionality such as StreetPass enables the exchange of data with

other 3DS consoles in close proximity even when the console is in the sleep mode [19]. The Nintendo eShop [20] supports the downloading of software directly to the device.

The Nintendo 3DS is primarily designed for playing games, but the features mentioned above enable it to be used in many other activities that may be of interest in forensic investigations. One way to determine the 3DS customer profiles (and the types of users) is to consider the Pan European Game Information (PEGI) classifications for video games [21]. The Nintendo 3DS has two games rated as 18-year-old and 397 games rated as three-year-old. In contrast, the Sony PlayStation Vita has eighteen 18-year-old rated games and 112 3-year-old rated games [21]. The figures are similarly skewed towards the 3DS in the 7-year-old rating category. Thus, it is reasonable to conclude that, if a 3DS is seized as part of an investigation, the case would likely involve a young child. This was demonstrated in a case where the previous generation DSi was used by a ten-year-old girl to take a picture of her attacker during an assault [10]. A more recent case involved a man who encouraged two 11-year old girls to send naked pictures via the email-like service provided by the 3DS [3].

2. Related Work

The published literature suggests that the 3DS platform can be misused [3, 16]. However, there is no evidence to suggest that the Nintendo 3DS has been explored as a potential container of forensic artifacts, although it may provide information relating to misuse and user activities such as network communications. Research on other entertainment systems (described below) has shown that the forensic methods and the types of artifacts recovered depend largely on whether the system is unencrypted and whether the main storage is a hard drive. If the answer is no to either of these questions, then a forensic investigator could attempt to extract information via the native interface.

2.1 Devices with Hard Drives

Microsoft's Xbox 360 is not encrypted, but it has the non-standard XTAF filesystem. The approach proposed by Xynos et al. [28] is to carve files and perform string searches for dates and times. Filesystem drivers [26] and forensic tools [13] are also available that can simplify the analysis.

Conrad et al. [7] conducted a series of tests on a Sony PlayStation 3 to determine the optimum method for analyzing the console. Although encryption is used to protect data, the PlayStation 3 does have a standard 2.5" hard drive for storage. Conrad et al. recommend that an analyst

extract a forensically-sound duplicate of the drive and use the duplicate to perform the investigation via the native PlayStation 3 interface.

Microsoft's Xbox One also contains encrypted files. An analysis of the hard drive [14] has shown that the files are contained in an NTFS filesystem, which opens the possibility of analyzing date and time entries in the MFT. However, the Sony PlayStation 4 does not have an immediately-recognizable filesystem. Forensic analysis recommendations are similar to those for the PlayStation 3: forensically image the hard drive and proceed to analyze the system via the native PlayStation 4 interface [9]. The PlayStation 4 analysis process described in [9] employed a special write blocker, VOOM Shadow 3, to write hard drive changes to an intermediate buffer that facilitated system navigation without any instabilities.

2.2 Devices without Hard Drives

The Nintendo Wii uses onboard storage that is soldered onto the motherboard. Similar to the PlayStation 4, a forensic analysis of the Wii [27] demonstrated that it is possible to recover data from the device via the user interface. However, this "live analysis" methodology has the potential to alter the data if performed incorrectly.

Desoldering the onboard memory is an option, but the high skill level needed and the potential for damage rule it out as a possible investigative method. Sutherland et al. [25] have described the analysis of an LG Smart TV entertainment system. Although a Smart TV is not a game console, the forensic analysis approach is relevant. In particular, an empirical analysis was performed via the user interface of the LG Smart TV, not unlike the methodologies used on the Wii and PlayStation 4 described above. However, as in the case of the Wii, it was difficult to extract a physical image of the onboard memory. Thus, the Smart TV analysis concentrated on what could be recovered via the user interface.

The device with the greatest similarity to the Nintendo 3DS that has been forensically analyzed and documented is the Sony PlayStation Portable (PSP) [8]. Although its updated sibling, the Sony PlayStation Vita, is technically a more direct rival to the Nintendo 3DS, at the time of this writing, no forensic research related to this device could be found. The Sony PlayStation Portable has Internet connectivity and a web browser. The browser stores artifacts on a removable, unencrypted FAT16-formatted memory stick. Conrad et al. [8] describe the process of forensically imaging the memory stick and analyzing files for web browsing artifacts, including deleted entries.

3. Forensic Value

The Nintendo 3DS can hold two types of media simultaneously, a game cartridge and an SD card. 3DS game cartridges primarily store game data, but are also used by some games to record save game data. The SD card stores images and videos taken with the camera, and applications downloaded from the eShop. Additionally, there is internal storage capacity on a NAND flash memory chip soldered onto the motherboard [11].

The closed console has several LED indicators that provide information about the system state. A blue power LED on the front of the console indicates that the device is in the standby mode. A charging LED indicates the power status and if the battery is running low. Red indicates that the device has to be charged, orange indicates that it is currently charging, while yellow indicates that the device is fully charged. Note that, if the device loses power, running applications may not be written to the device; for example, web browser history may be lost if the browser is not closed properly.

An LED on the top right of the device indicates if notifications have been received. There are four possibilities for this LED: (i) blue – SpotPass data has been received; (ii) green – StreetPass data has been received; (iii) orange – a friend's device is online; and (iv) red – the device needs to be charged. A slider on the right-hand side of the device controls wireless connectivity; the LED alongside it turns yellow when wireless is on.

Upon powering a 3DS, the last application that ran on the device is selected and the corresponding game logo is displayed on the top screen. If the notification LED is lit, a glowing dot appears on the icon of the application that received the notification.

Several features are potentially of interest to a forensic investigator. The 3DS offers Wi-Fi connectivity. The WLAN subsystem is a single-chip 802.11b/g device [12]. Connection information is easily accessible via the settings menu; this includes information about the current connection used by the device along with the MAC address. Up to three access points can be stored.

The activity log keeps a record of the applications launched on the system, including the first and most recent date that each application was used. This information is updated during a live investigation if any applications are executed, so it is important that the information is collected early in the analysis.

The 3DS incorporates a Netfront browser based on the WebKit engine, which enables images to be downloaded to the SD card [18]. The built-in

web browser has forensic significance because it provides a history of up to 32 web pages viewed by the user. However, neither date nor time information are available. It should be noted that, if a link is followed from an older web page, then a new history list is generated from that point onwards. Cached information includes the website favicon, title and URL. The web browser history can be viewed using the left and right arrows on the touch screen. A maximum of 64 bookmarks may be stored.

The camera serves as the access point for the image gallery. An investigator can use the camera to view images stored on the device, including images downloaded via the web browser. The date and time of a viewed image are displayed in the top screen. In addition, there is a note indicating where the image is stored, either on the SD card or in internal NAND memory.

The Nintendo eShop is used to purchase downloadable content. Information stored in the eShop could be of value because some credit card details may be saved, such as the last four digits of a credit card number and its expiration date.

The friends list contains friends who have connected locally or over the Internet using a "friend code." Users can see when their friends are online and can update their status, which is shared with others.

Until October 2013, the Swapnote message exchange service (Letter Box in some regions) could be used to exchange messages and photos with other users via the Internet using the SpotPass service. However, Nintendo terminated this service because some consumers, including minors, were posting their friend codes on Internet bulletin boards and then using Swapnote to exchange offensive material [16]. Although no new messages can be sent via SpotPass, historical data may be available on a device. Messages and pictures can still be exchanged using StreetPass (Figure 1), which requires the two devices to be in close proximity.

Unofficial cartridges (flashcarts) can offer additional functionality for the 3DS, with some cartridges providing data storage for user files. An example is Acekard 3 game cartridges that are often used for pirating software or running homebrew applications. However, the 3DS device itself supports miniSD cards, enabling users to store a range of files, including music, images and documents [22]. It is, therefore, vital to thoroughly examine game cartridges to confirm their functionality and ensure that no evidence is missed.

Several hacks have been developed that circumvent the security measures on the 3DS and allow third-party (homebrew) applications to be installed. As discussed in [23], these mechanisms could be used as new vectors to extract data from embedded systems. In the case of the

Figure 1. StreetPass service for exchanging pictures and messages.

3DS, a number of applications and game titles have been shown to be exploitable. A comprehensive list can be found in [24]. Several FTP homebrew applications have also been released [2], but at the time of this writing, they only allow access to the miniSD card, not the internal NAND flash memory.

Table 1 summarizes the 3DS device features that would be of interest in a forensic investigation. These features must be examined very carefully to ensure that the investigation is conducted in a forensically-sound manner and/or no evidence is missed.

Barriers to using standard imaging methods on a 3DS device include the lack of common interfaces (e.g., USB) and encryption of the internal NAND flash memory. Imaging a 3DS NAND chip is possible using JTAG or chip-off. JTAG guidance for forensically imaging NAND flash memory using a tool such as FTK Imager is presented in [5]; the image can be flashed back later to verify the results. Chip-off is more invasive and

Table 1. Features of interest.

Features	Reason
LEDs	Different color states indicate that data exchange has occurred
Wi-Fi	Associated access points reveal where the 3DS was used
Web Browser	Provides recent history (maximum 32 pages) and bookmarks (maximum 64 pages)
Camera	Provides access to image gallery, views of images created by the 3DS and images saved from webpages; indicates the locations of stored images (internal NAND memory and miniSD card)
eShop	Provides the last four digits of credit card numbers and their expiration dates
Friends List	Contains the list of friends (on the Internet and/or in close proximity); owners can share their status
Swapnote	Email-like service used to send text and images from the gallery; SpotPass and StreetPass services used to send text and images over the Internet and to users in close proximity, respectively
Unofficial Game Cards	May contain additional embedded media (e.g., microSD), homebrew software (potential for further communications options) and pirated software
Activity Log	Provides coarse indications of application usage patterns (e.g., pedometer indicates user perambulations)
Game Notes	Contains hand-written notes created by the user

requires the desoldering of the NAND chip. To avoid these challenges, a 3DS device can be investigated live, but this may have an impact on the state of the device (i.e., alter or even add data). The forensic analysis methodology described in the next section considers all these issues while adhering to the ACPO Good Practice Guide for Digital Evidence [4] to minimize alterations, tampering and modifications of the original evidence to the extent possible.

4. Forensic Analysis Methodology

As discussed in the previous section, the most appropriate approach for acquiring evidence from a 3DS device is via the user interface. This empirical approach ensures that investigators do not lose evidence due to unfamiliarity with the device.

The 3DS has two displays, but only the lower screen is touch-sensitive. Underneath the screen are three buttons, SELECT, HOME and START.

The most important is the HOME button, which allows a user to return to the main screen at any time. A stylus located next to the game card slot on the back of the 3DS makes it easier to interact with the device. Alternatively, a user can employ two navigational buttons: A to select an item from the menu and B to move back to the previous menu. The lower touch-sensitive screen contains applications with several built-in utilities along the top.

Figure 2 presents the forensic analysis methodology for Nintendo 3DS devices. The methodology has the following steps:

- **Step 1: Start the video camera to record all interactions:** The recommended ACPO best practice [4] when examining a live device is to record the process and capture all the actions involved in the examination for later scrutiny and to provide a strong record of the procedures used in the analysis. In addition, a written record should be kept of every action performed, including its time and duration.

- **Step 2: Check the device status:** Before the SD and application cards are removed, it is important to ensure that the 3DS is actually turned off (i.e., it is not in the suspend mode). If the cards are removed when the system is in the suspend mode, then running applications are forcibly closed and potential evidence held in memory may be lost.

  The power indicator light must be checked first. If the light is blue, then the system is on. Next, the Wi-Fi indicator light on the right-side of the 3DS must be checked. If the light is amber, then the slider must be depressed to disable Wi-Fi. Following this, the console is opened – this resumes the suspended applications. Observations of interest are then recorded, following which the power button is pressed and held down to close the software and expose the power off function. This updates the activity log, but it was discovered that the log is updated even if the application card is forcibly removed. Finally, the device should be powered off.

- **Step 3: Remove, write-protect and analyze the SD card separately; clone the image to a new SD card; insert the clone:** The SD card is not encrypted and can be imaged separately using a suitable forensic tool. The card is formatted as FAT16 (up to 2 GiB) or FAT32 (up to 32 GiB). Data can be extracted via carving, which also retrieves images (including their EXIF data) that can be important depending on the case. Specifically, the following information can be extracted:

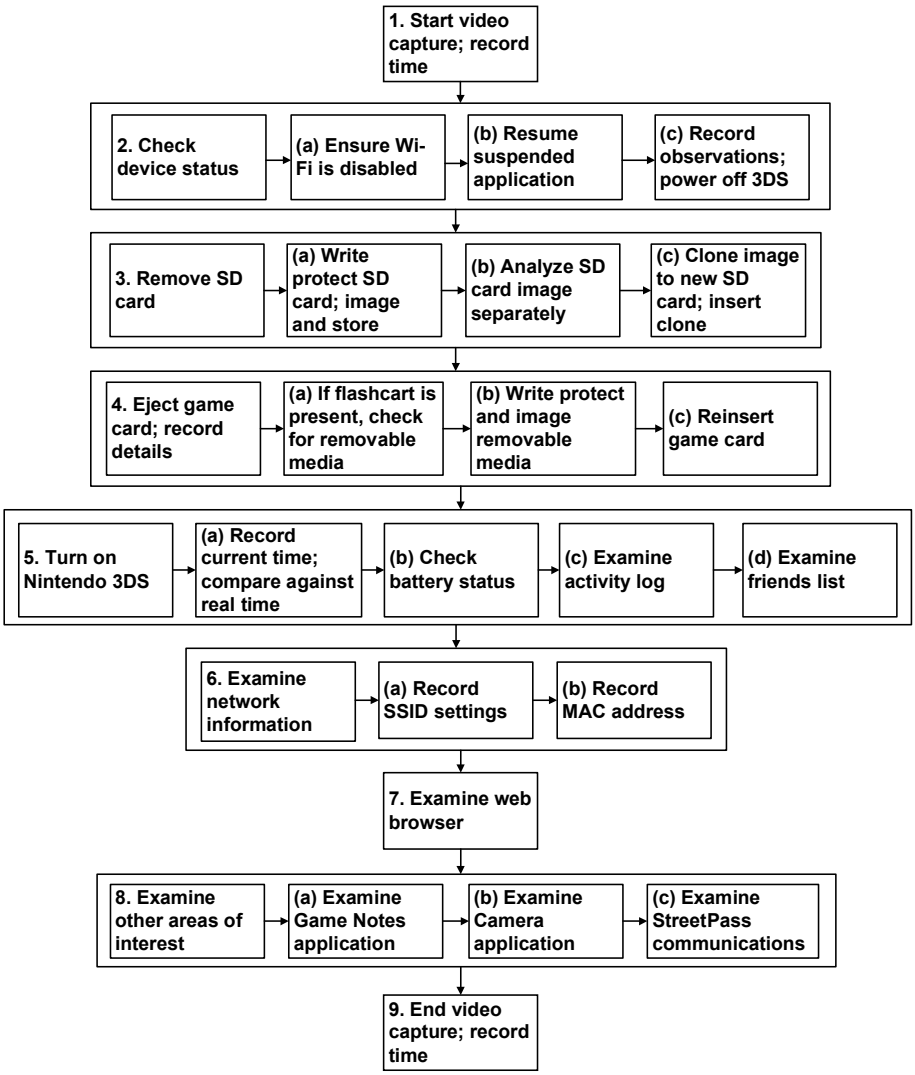

Figure 2. Forensic analysis process for Nintendo 3DS devices.

- Exif.Image.Make: Nintendo
- Exif.Image.Model: Nintendo 3DS
- Exif.Image.DateTime: 2012:01:27 13:37:00

Images downloaded via the web browser can be seen in the DCIM folder, but no information about the sources of the images is stored. Therefore, it is necessary to rely on the web browser history data.

Videos taken by a 3DS are stored in the AVI format, 3D images are stored in the MPO format and voice notes are stored in the M4A format.

Applications downloaded to the SD card from the eShop are encrypted; extensive information about the layout and file structure can be found in [1]. Experiments revealed that launching different applications known to exist on an SD card did not change the MAC (modification, access, creation) times of application files. The only times that are provided relate to the initial installations of applications on the SD card; therefore, an investigator should not rely on a timeline analysis of this nature. Furthermore, applications are stored in folders with names containing hexadecimal characters. To compile a list of applications on the SD card, an investigator would need to cross-reference the list as described in [15].

Applications that can store or process user data should be noted and appended to the end of Step 7 (described below). A clone of the SD card should be inserted into the 3DS device without write-protection. Later steps (e.g., Steps 8(a) and 8(b)) may require an investigator to export files to the SD card. Using a clone ensures that application data on the SD card can be analyzed via the console interface while maintaining the forensic integrity of the original SD card.

- **Step 4: Eject the game card; record the card details:** The game card should be formally recorded to confirm that it is a game or application. Recording and analyzing the title, type and code found on the card can confirm its functionality. If the game Cubic Ninja, in particular, is found, the presence of homebrew applications on the SD card is indicated. Investigators should cross-reference the homebrew application list available in [2] against the SD card from Step 3 to determine if other useful forensic artifacts can be found. At the time of writing this chapter, FTP servers (`ftPONY` and `ftBRONY`), a Facebook client (`fb43ds`) and a video player (`vid3o`) would be of interest to investigators. Furthermore, if an unofficial flashcart is found, there may be a removable microSD card, which should be write-protected, imaged and analyzed separately. The microSD should be cloned and the clone inserted without write-protection into the flashcart.

- **Steps 5(a), 5(b): Power on the Nintendo 3DS:** The Wi-Fi starts when the 3DS is powered up if the Wi-Fi was turned on previously. If the amber indicator light is lit on the right-side of the

3DS, then the Wi-Fi must be disabled by pushing the slider or the device must be in a Faraday cage. If the device detects that new firmware is available, then it prevents access to some areas until the update has been applied. At the top-right-hand corner is the battery icon, which indicates the battery power level using blue bars and if the device must be charged. Alongside this is the current date and time. The date and time are not updated automatically; this must be taken into account when examining timestamps retrieved from the device because they may have to be offset against the current time. The top-left-hand corner displays the connectivity status – a blue bar containing the word "Internet" indicates an active connection. The main menu displays the applications available in a grid format; these provide valuable information about the possible uses of the 3DS.

- **Step 5(c): Examine the activity log:** The activity log provides a record of recent activities on the device. Upon opening an application, a record is made in the activity log. Hence, the activity log should be one of the first items examined by an investigator.

  The activity log has two distinct views as part of the application. The first view enables a user to examine daily records of usage, which can be adjusted for daily, weekly, monthly or yearly totals. Figure 3 shows the daily view of an activity log; the analyst can scroll through and select the date on the bottom screen while the top screen defaults to a graph representation of the usage. A list view provides a different representation of the data. This view may be used, for example, to examine the results of a pedometer that indicates the numbers of steps taken by a user and the corresponding times.

  The second view in the activity log is of the software library. An analyst can navigate the application icons on the bottom screen while the top screen displays the corresponding usage. The dates of the first use and most recent use are presented, but timestamps are not provided.

- **Step 5(d): Examine the friends list:** The friends list contains friends' names, friend codes, whether friends are online or not, and a user-editable message of up to 16 characters that can be broadcast to everyone in the friends list.

- **Step 6: Examine network information:** Networking information can be found under the Settings menu. Upon selecting

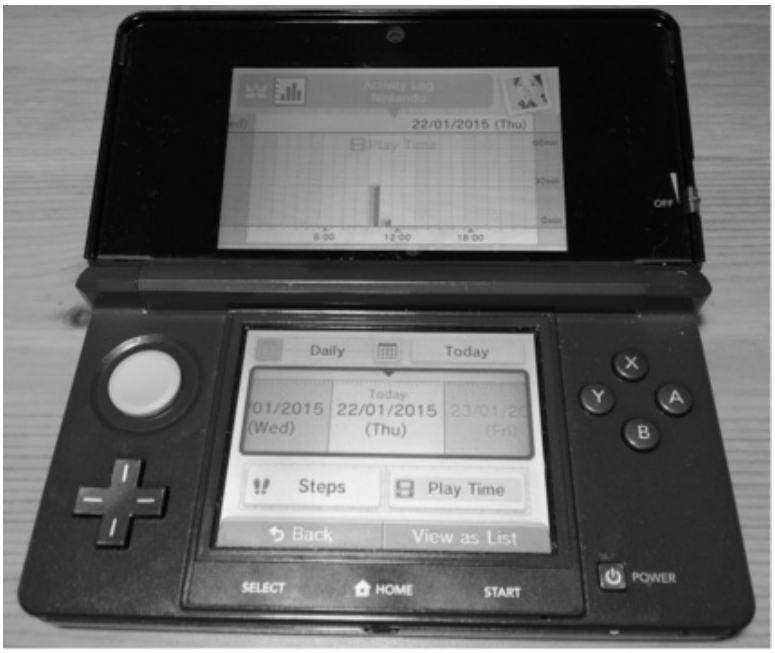

Figure 3. Daily view of activity log events.

Internet Settings, the new menu contains the items: Connection Settings, SpotPass, Nintendo DS Connections, Other Information.

Upon selecting Connection Settings, a list of three possible connections are displayed. If the Connection has "None" written alongside it, no connection is established. However, if it has an entry such as "Connection 1: mySSID," then a connection is established. A lock symbol indicates the security status of the connection.

To obtain the MAC address of the device, it is necessary to access Internet Settings and select Other Information. The MAC address may be needed during an investigation to confirm or eliminate that the device was used to perform certain actions.

- **Step 7: Examine the web browser:** The 3DS web browser appears in the top-right-hand corner of the touch screen. When the browser is opened, the last page viewed is the first to open. From this point on, the left arrow at the bottom of the screen can be used to navigate through previously-viewed pages. Clicking on the Menu button provides access to the bookmarks list and an "i" icon provides page information, including the address (i.e., URL).

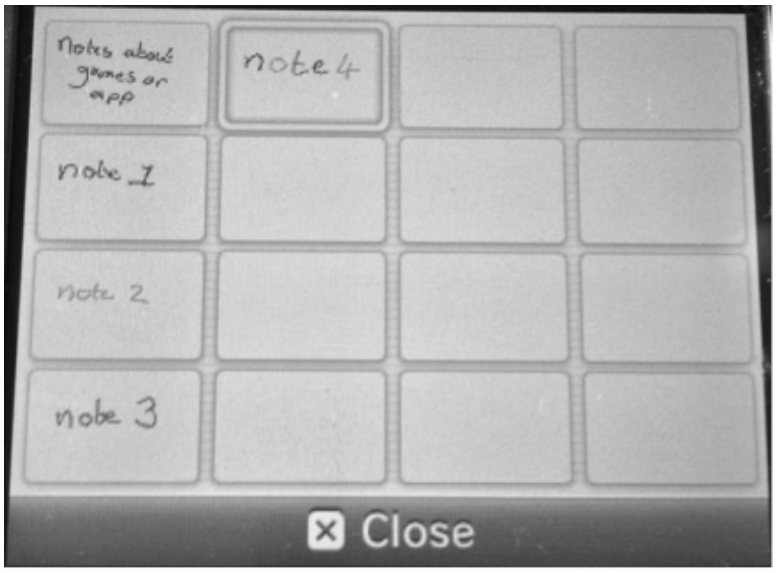

Figure 4. Game Notes application with handwritten messages.

The Bookmarks item contains a maximum of 64 entries. A bookmark can be opened for editing, which displays the complete website URL. The web browser design poses a challenge to forensic investigators because no permanent record of the browser history is recorded; only the most recent 32 pages can be viewed. Other information can be confirmed via the web browser, such as the current network connection and proxy settings. The menu contains a setting tab, which displays information as follows:

- Connection Type: Wireless LAN (Connection 1)
- Connection (SSID): mySSID
- Security: WPA2-PSK (AES)

In addition, the user can use the menu to delete the history, cookies and save data.

- **Step 8(a): Examine the Game Notes application:** As shown in Figure 4, Game Notes supports handwritten notes made by users. Date/time information is not stored by a 3DS device, but a user may write the time on the note itself. The application stores the handwritten messages in onboard memory. However, export functions are provided that enable an investigator to save notes of

interest such as pictures on the SD card by default and in internal memory if the SD card unavailable. Timestamp data associated with an exported picture reflects the creation date of the image, not the creation date of the Game Notes entry. Exporting images in this manner leaves the original Game Note entries intact.

- **Step 8(b): Examine the Camera application:** The camera icon enables the viewing of photos and videos. These images can be stored on the device or the SD card, but all the images are viewed in chronological order from left to right, with date markers separating the images. By clicking on an image, the date/time at which the image was taken is displayed, along with the image storage location.
- **Step 8(c): Examine StreetPass communications:** Mii characters (Nintendo avatars) from other 3DS consoles can be transferred when the consoles are in close proximity to each other. The number of times the Miis have met is displayed alongside an indicator of the software used (e.g., "met via StreetPass"). A Mii creator can register information to be transferred with the Mii, including the nickname, Mii's birthday, creator, StreetPass hits and plaza population. A coarse timestamp indicates when the Mii was linked to the 3DS device (e.g., "3 hours ago" or "4 days ago").

5. Conclusions

The phrase "End of the Age of Nintendo Forensics" was coined by Carvey [6] to emphasize that forensic investigators must have detailed knowledge about the systems and files they analyze and that they should not merely rely on digital forensic tools. We are currently in the "New Age of Nintendo Forensics," where game consoles – both desktop and handheld – can contain significant amounts of digital evidence about user actions and possible criminal activity. This is especially true of the eighth generation of game consoles that provide advanced Internet functionality and applications, including web browsers, email and social media.

This chapter has highlighted cases in which Nintendo handheld consoles have provided evidence of illegal activity and has identified areas on the devices where data relevant to forensic investigations may be stored. The forensic analysis methodology for Nintendo 3DS devices was developed using empirical research. The methodology maximizes data retrieval and minimizes evidence loss or corruption; this is important because certain sequences of events can trigger the modification of forensically-relevant data.

Unfortunately, retrieving a dump of the internal device memory is difficult without hardware modifications and analyzing the dump is extremely difficult due to encryption. Future research should focus on these problems. For example, if an FTP server could run with root privileges, it may be possible to obtain and analyze a logical image of the files stored in the internal NAND memory. Analyzing and understanding the raw files that store data could reveal valuable artifacts pertaining to user communications. If Linux tools (e.g., `dd`) compiled for use on a 3DS are available, it may be possible to obtain unencrypted images of internal NAND memory. Existing forensic techniques such as file carving could then be used to identify and recover deleted data and temporary files.

References

[1] 3DBrew, Title Data Structure (`3dbrew.org/wiki/Title_Data_Structure`), 2014.

[2] 3DBrew, Homebrew Applications (`www.3dbrew.org/wiki/Homebrew_Applications`), 2016.

[3] B. Ashcroft, Accused child predator allegedly used Nintendo's Swapnote service, *Kotaku* (`kotaku.com/child-predators-were-using-nintendos-swapnote-service-1459304126`), November 6, 2013.

[4] Association of Chief Police Officers, Good Practice Guide for Digital Evidence, London, United Kingdom, 2012.

[5] Ate0Eight, DIY 3DS XL NAND Dumping-R/W pt. 1 (`www.youtube.com/watch?v=n5Aa88HCK6g`), 2013.

[6] H. Carvey, The age of "Nintendo forensics" ..., Windows Incident Response (`windowsir.blogspot.no/2005/12/age-of-nintendo-forensics.html`), December 22, 2005.

[7] S. Conrad, G. Dorn and P. Craiger, Forensic analysis of a PlayStation 3 console, in *Advanced in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 65–76, 2010.

[8] S. Conrad, C. Rodriguez, C. Marberry and P. Craiger, Forensic analysis of the Sony PlayStation Portable, in *Advances in Digital Forensics V*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 119–129, 2009.

[9] M. Davies, H. Read, K. Xynos and I. Sutherland, Forensic analysis of a Sony PlayStation 4: A first look, *Digital Investigation*, vol. 12(S1), pp. S81–S89, 2015.

[10] C. Hanlon, Quick-thinking girl, 10, traps paedophile by using her games console to take picture of him molesting her, *Daily Mail*, March 28, 2012.

[11] iFixit, Nintendo 3DS Teardown, San Luis Obispo, California (www.ifixit.com/Teardown/Nintendo+3DS+Teardown/5029), 2016.

[12] IHS Technology, Nintendo 3DS Carries $100.71 Bill of Materials, IHS iSuppli Physical Teardown Reveals, Press Release, Engelwood, Colorado, March 28, 2011.

[13] Magnet Forensics, Magnet Forensics releases Internet Evidence Finder v6.3, Waterloo, Canada (www.magnetforensics.com/magnet-forensics-releases-internet-evidence-finder-v6-3), February 5, 2014.

[14] J. Moore, I. Baggili, A. Marrington and A. Rodrigues, Preliminary forensic analysis of the Xbox One, *Digital Investigation*, vol. 11(S2), pp. S57–S65, 2014.

[15] Mtheall, List of Application Identifiers (mtheall.com/~mtheall/tmdlist.php), 2014.

[16] Nintendo, Notice about Service for Nintendo 3DS Software Swapnote, Redmond, Washington (www.nintendo.com/whatsnew/detail/UHQZFP2Jxcll_Vm-PsZpxNIK5920bRRK), October 31, 2013.

[17] Nintendo, Hardware and Software Sales Units, Kyoto, Japan (www.nintendo.co.jp/ir/en/sales/hard_soft/index.html), 2016.

[18] Nintendo, Internet Browser Specifications for Nintendo 3DS, Redmond, Washington (www.nintendo.com/3ds/internetbrowser/specs), 2016.

[19] Nintendo, Welcome to StreetPass: What is StreetPass? Frankfurt, Germany (www.nintendo.co.uk/Nintendo-3DS/StreetPass/What-is-StreetPass-/What-is-StreetPass--827701.html), 2016.

[20] Nintendo, What is Nintendo eShop? Redmond, Washington (www.nintendo.com/eshop/what-is-eshop), 2016.

[21] Pan European Game Information, Search a Game, Brussels, Belgium (www.pegi.info/en/index/id/509), 2016.

[22] R4town.com, Acekard 3 Card for Nintendo 3DS and DSi (r4town.com/products/Acekard-3-card-for-Nintendo-3DS-and-DSi.html), 2016.

[23] H. Read, I. Sutherland, K. Xynos and F. Roarson, Locking out the investigator: The need to circumvent security in embedded systems, *Information Security Journal: A Global Perspective*, vol. 24(1-3), pp. 39–47, 2015.

[24] smea, The Homebrew Launcher (`smealum.github.io/3ds`), 2016.

[25] I. Sutherland, K. Xynos, H. Read, A. Jones and T. Drange, A forensic overview of the LG Smart TV, *Proceedings of the Twelfth Australian Digital Forensics Conference*, pp. 102–108, 2014.

[26] I. Tepper, A set of tools for working with the Xbox 360 (`code.google.com/p/x360`), 2016.

[27] B. Turnbull, Forensic investigation of the Nintendo Wii: A first glance, *Small Scale Digital Device Forensics Journal*, vol. 2(1), pp. 1–7, 2008.

[28] K. Xynos, S. Harries, I. Sutherland, G. Davies and A. Blyth, Xbox 360: A digital forensic investigation of the hard disk drive, *Digital Investigation*, vol. 6(3-4), pp. 104–111, 2010.