Forensic Investigation of the Nintendo Wii: A First Glance

Dr Benjamin Turnbull

***Abstract*—The current generation of game consoles have capacity far exceeding their predecessors, having more in common with personal computers than ever before. This work seeks to understand the Nintendo Wii, the lightest and least powerful of these, and the value in a forensic context. Specifically, this work seeks to understand what information can be obtained from the Wii console, the issues with data extraction, and the device limitations.**

***Index Terms*—Forensic analysis, Digital evidence, Game console, Nintendo Wii**

I. Introduction

NO longer merely game platforms, the seventh and current generation of gaming consoles (represented by the Microsoft Xbox 360, the Sony PlayStation 3 and the Nintendo Wii) have instead become networked media platforms capable of replacing many users need for a traditional computer system. They allow increasing connectivity, potentially offering web-browsing, email, instant messaging and Voice over IP (VoIP). This increase in capability of current generation consoles and the enlarged scope for such devices to be misused has been noted by the forensic community and has resulted in publicly released analysis guides for the Microsoft Xbox [1] and Xbox 360 [2]. The Nintendo Wii is arguably the current highest-selling console of the current wave, selling over 25 million units worldwide since [3]. However, the Wii differs in many respects to the Xbox 360 and therefore adaptation of the existing guide is not wholly appropriate. This work seeks to analyse the capability of the Nintendo Wii as a means of determining appropriate mechanisms of forensic analysis.

This work seeks to understand the Nintendo Wii from a forensic perspective; noting both the device capabilities and methods for forensically examining it in a minimally intrusive manner. The need for this arises from the increased functionality of the device and its potential use as a traditional computer workstation replacement. This work wishes to explicitly note the potential of the Nintendo Wii in both forensic analysis and as a tool for misuse.

II. Features of the Nintendo Wii of Benefit to Forensic Investigators

Of the current generation of gaming consoles, the Nintendo Wii is arguably the least attractive target for misuse, lacking the power and disk-based storage of its competitors, Microsoft Xbox 360 and Sony PlayStation 3. Notably, the lack of Hard Disk-based storage is of interest in the electronic investigation of such systems, as mechanisms for write-blocked hard disk forensic copying and analysis are therefore not possible. In addition, the Nintendo Wii has a proprietary file system that is not open to inspection, even if recovered. These device constructs pose an issue with the forensic analysis of the Wii as, unlike its rivals, forensic integrity cannot be guaranteed through the use of write protection. The result of this is less flexibility for forensic investigators.

The lack of a hard disk unit within the Wii does not imply a lack of stored data - the Nintendo Wii incorporates an onboard Samsung chip, offering 256MB of flash-based memory [4]. To augment this, an SD flash card reader is also found at the front of the unit. It is possible to remove the optional extra SD card for external analysis, but the base memory is soldered to the Wii motherboard and cannot be easily removed without desoldering the system, which has risks in itself [5].

The relatively closed proprietary system that is found within the Nintendo Wii is both beneficial and detrimental from a forensic perspective. A closed system is beneficial to forensic investigators in that it narrows the number and types of software that may be used on the device, which minimizes the forms of misuse that are possible. A closed system also ensures that certain features are active and have not been disabled, thereby ensuring that evidence collected automatically by the system remains. However, the use of a non-published Operating System and file format does not make analysis of the Wii an easy task, even for devices that may be analysed externally such as the optional SD memory card.

However, despite these hardware limitations, this device still has a large capacity and still holds potential for misuse. Features of this console of potential interest to forensic investigators include:

- Capability for wireless networking
- Email-like messaging
- Web browsing
- Online shopping through its own interface
- Automated logging of device usage

Given the limited memory, processing power and storage of the Nintendo Wii, investigators are prone to underestimate the potential for its misuse. The features described above, however, are possible to implement on even small-scale devices. Each of these features will be discussed separately, both how they are implemented within the Wii and also how they are of potential use within an investigation.

1) Wireless: Nintendo Wii has the ability to connect to the internet via inbuilt 802.11b/g wireless, utilising the Broadcom 4318 chipset. This is the primary form of network connectivity for the Wii although a USB-to-Ethernet device is also available

directly from Nintendo [6]. This interface is potentially of use to investigators for several reasons, one being that as a network device the MAC address may be required for elimination or confirmation on any logging mechanisms.

2) Email-like messaging: Nintendo has developed a proprietary messaging system not unlike email, both as a means of distributing news regarding system updates and features and also allowing Wii-to-Wii communications. The internal mailing system allows messages to be received to and from email addresses, but only with prior authorization. There is an obvious forensic benefit for the analysis of such communications, as it presents another form of communications and may also be used to determine links between individuals.

3) Web-Browsing: The Internet Channel is an extra third-party software purchase for the Nintendo that is a browser (developed by Opera), and the offering is fully functional from a user perspective. As the analysis of Internet usage is of obvious benefit to investigators, this may represent one of the main reasons for analyzing a Nintendo Wii. However, the software is also developed by a third-party and has a cost associated with it, and will therefore not appear on all systems.

4) Online Shopping: The Nintendo Shopping Channel is still in its infancy, but is a functioning retail system in that it allows the purchase of content with the use of a credit card. Within certain circumstances, information regarding credit card purchases may be of use within an investigation. The other tangible benefit of this system is that it has a communications stream between an individual device and a server, and it may be possible to use this as a means of synchronizing times for individual systems. This will require the active assistance of the Online Shopping Channel server administrators.

5) Automated logging: A feature unique to the Nintendo Wii console is the automated logging of the lengths of time for which the machine has been played. This information manifests itself within the Nintendo mail system but unlike other mail messages is unable to be deleted by users. Whilst the times that each game is played is not given, the total daily usage of the Nintendo Wii may be of use within a forensic investigation as a means or confirming or refuting personal statements of events or other evidence.

III. Analysis of the Nintendo Wii

The discussed lack of a hard disk or removable permanent storage mechanism for the Nintendo Wii is unique to Nintendo in the current console generation, and poses issues from a forensic perspective. The use of common forensic analysis tools such as Encase or FTK are not appropriate for this, as they potentially would be for the Microsoft Xbox 360 or Sony Playstation 3.

One mechanism for performing an extraction of all data within the system would be to have a bootable Wii disc that would be able to access and copy the data directly to a memory card. However, no such disc exists within the public domain, and given that the Nintendo is a proprietary system, such a disc would need to be manufactured by, or with the consent of Nintendo Inc.

Another viable forensic analysis process, to physically desolder and remove the onboard memory of the Nintendo Wii unit and custom build an interface to a PC workstation to extract data, was discounted. This process may be more forensically sound in the traditional sense as data is accessible in its most raw form and not subject to interpretation, but it requires a much higher skill level and access to greater resources for the investigator. In addition, the reattachment of the memory chips adds further complexity, if required. The complexity of any interpretation is also potentially an issue for what may not be a primary piece of evidence.

Therefore, this work discusses analysis of the Wii as a complex embedded device, which, although not the preferred option of analysis, represents the most applicable forensic methodology available. The aim, therefore, is to record all activity and to ensure that any alterations of a system are noted and, if possible, minimized. This may therefore require the visual recording of the process (either with the use of a video camera or direct recording method as defined by local standard operating procedure) in addition to notes on the stages taken.

For this work, the following equipment was used:

- One target Nintendo Wii
- One sensor bar - for ease of use this must be placed above or below the television as was originally set up.
- One Wiimote controller
- Cords and cables

To navigate the Wii, one Wiimote is required. In-menu navigation is conducted by pointing the Wiimote at the screen used. The 'A' button (found on the top of the Wiimote) is used to select menu items, and the 'B' button (the underneath trigger) moves one level back. The main screen may be activated at any time by the 'Home' button found on the top of the remote at the base.

This work was conducted with an off-the-shelf PAL Wii system, the menus, but operations and features should be equally applicable with the NTSC console system. However, this has not been confirmed by this work, due to availability issues.

It was noted (by the researcher) that interacting with any of the 'Channels' will alter the system. Particularly, the *Wii Play Time* mail will add the amount of time spent within these channels to the total mail for that day. It is for this reason that it is recommended that analysis occur at least one day after the Wii was contained and collected to isolate this information. The alternative, with the investigator altering the data and time setting of the instrument to a time in the future, to isolate the information, is less preferable as it involves altering data potentially of use within itself. The following structure for analysis was developed to ensure that the areas potentially altered by interaction with the Wii system are examined first, before alteration occurs.

The proposed process of performing forensic analysis on a Nintendo Wii is as follows:

1) Activate external logging mechanism or recording device
2) Take out SD Card - search independently
3) Write Protect SD Card and return it
4) Turn on Wii
5) Sync controller - press A

6) Check settings
   - Determine current unit time -
   - Determine connected wireless network information (if disconnected from wireless, it is unlikely the system has been connected to the internet)
7) Check Message Board
   - Go to messaging system
   - Determine usage of the system for relevant dates
   - Any other messages of note - either internally or sent
   - Check address book
8) Check other areas
   - Determine 'Mii' players (player avatars used by the system - discussed below)
   - Check web browser
9) Check Message Board and note differences in time since stage 7.

Stage 9 is particularly relevant and may be required by specific jurisdictions, and also represents good investigative technique, in that it enables investigators to account for all changes made to the system. This would clearly define both the original and final values and allow for subsequent analysis if required.

The ordering of this process is designed to allow forensic investigators to access the potentially vulnerable areas of a system first, before these are potentially altered by access to the other areas. In particular, the Wii Message Board will be altered by such access and therefore the original data must be captured first.

Stages 1 through to 3 are self-explanatory, and therefore require little further discussion. The details for stage 1 and 2 are dependent on local legal requirements and existing processes.

A. Stage 4, 5 - Activate system

Upon start up, the user is prompted to press A to continue at the health warning page. A controller is required to do this. This brings the user to the main menu.

The main menu contains information or potential forensic value, as the features populating it may give insight into the usage of the system. It is also from this screen that all functions of the Wii are accessed. The majority of the menu icons are aligned in a grid. However, accessing any icon on the grid potentially alters the *Wii Play Time* function - a function that calculates the time the Nintendo System has been used (this is discussed further in later sections). The main screen is shown in figure 1.

B. Current Machine Disc

The first icon of the first row (top left hand corner) represents the current disc in the machine. Unless this machine has been modified, this will be empty or represent a game disc. The forensic benefits of examining this are minimal. However, it should be noted that disc information will be displayed without directly accessing the disc - the game disc has a sub-menu that will display the game title, which will not alter the *Wii Play Time* message.

Fig. 1. Wii Main Menu [7]

C. Stage 6: Check Settings

To access the system settings of the Wii, select the Wii logo on the bottom left of the screen. This gives two options; *System Settings and Data Management* [8].

The *System Settings* function has three pages of menu items. It is also from this page that the current Operating System version number may be determined, which is found in the top right-hand corner (eg. 2.1E). The Wii *System Settings* is divided into three pages, and notifications of which page is active are given in the bottom right corner of the screen. To change between *System Settings* pages, the arrows on the right and left of the screen need to be selected.

The Calendar function on the first page of *System Settings* holds the date and time for the Wii, but of course this is user-alterable. Clicking 'Calendar', gives two options, one to view and change the current time, and the other for the current date. Noting the system date and time is potentially of use for contextualizing and determining the accuracy of information gathered from the Wii Message Board.

One interesting point of note is that the current date and time does not adjust automatically for daylight savings, and therefore might be slow or fast by one hour. This change must also be noted for any other point at which times and dates are used, such as when determining the total time the device was used on a particular day. If the time appears anomalous, page 3 of the *System Settings* has a country option, which may assist in determining the location of time zone of the system, if this is in question.

It also may be important in some investigations to have note of the network settings for all devices within a given vicinity, and on the Nintendo Wii, this is accessed through the *System Settings*. On page two of the systems settings, the available options are *Connection Settings*, *Console Information*, and *Agreement/Contact*.

Selecting the third option, *Internet*, gives access to the three possible network configurations that the Wii can store at once [8]. This will be in a form similar to:

Connection1 - wireless
Connection2 - none
Connection 3 - none

Where each of these connections will be wireless, wired, or be inactive (none). The current profile will be highlighted with red corners. From this, forensic examination may determine

the network environment that a Wii has connected to, and if multiple environments exist, the details of each. The existence of multiple profiles may indicate that a Wii system has been moved and used at multiple locations, and if the details of wireless networks may be known, it is possible to place the Wii, and by association others, in a physical area. It is probable that the majority of connections will be wireless in nature, given that this hardware already exists. Selecting a connection will bring up the next selection of possible options:

Use this connection
Connection test
Change settings
Clear settings

Forensically, it is inadvisable to select the *Clear Settings* option. The *Change Settings* option gives the current information about the wireless connection.

The first page of settings gives the type of connection (wireless or wired) and the SSID of the connected network.

The second options page (hitting the right arrow) for a wireless network gives the security and encryption status and details required to connect. This appears similar to:

Type of Security
WEP
WPA-PSK (TKIP)
WPA-PSK (AES)
WPA2-PSK (AES)

Clicking the selected encryption type (denoted with red borders) brings up the passphrase key, although this has been masked out. The only forensic note of interest is that although masked, the length of the key is accurate. The next settings screen gives IP address information, and may appear similar to:

Auto obtain IP address?
Auto obtain DNS
Proxy

If the Wii is configured not to automatically obtain an IP address of DNS settings, the Advanced Settings will give the preconfigured information [8]. The same is also true if a proxy server has been set.

Also within the *Internet* component of the *System Settings* is the option *Console information*. This is of use within a forensic investigation if network log files are in place, and the MAC address of the system needs to be noted and logged (although the MAC address is also printed on the base of the unit). If there is a LAN adaptor connected to the Wii, its MAC address will also appear in this option, else it will be greyed out.

The *Data Management* menu indicates what information is stored on the machine, and will show the contents of the Wii memory in addition to an attached SD card, if applicable. Although viewing the SD card within this console may indicate device-centric information, independent analysis should also be attempted, as the Wii functions as a photo-viewer (*Photo Channel* on the main menu), and the SD card is the primary form of input for this.

The *Save Data* option shows all data on the Nintendo Wii or any attached Game Cube cartridges attached. When viewing the memory usage of the Nintendo from this console, anything marked 'Channels' indicates a downloaded application such as a game, the Internet Channel, or similar.

D. Stage 7: Mail and Messages

Within the Wii console, Nintendo has created a proprietary messaging system comparable to email. This system, Wii Message Board, allows communication between different Wii systems with mutual authentication. Each console has a number in the form of XXXX XXXX XXXX XXXX, which serves as this unique address. This interface is used for both external mails and for messages generated by the system. The Wii can be used to send mails directly to other Nintendo systems (requiring the unique address of the other Wii) or to email addresses, but this still requires two-party authentication to an approved whitelist.

To access the mail from the main menu, click the envelope icon in the bottom right hand corner. This is named the 'Wii Message Board', but includes all internal messages, memos as well as emails and messages from other machines. If there is a number on this icon, it represents the current 'active' messages - this does not imply that such items are unread, but that they are current.

Clicking the 'Wii Message Board' icon brings up the mail function, which is a list of recent messages and mails. To view individual mail messages, click them with the Wiimote.

The left and right sides of this screen have '-' and '+' buttons respectively, and these cycle through each day's messages. The 'active' messages are denoted with a flashing red and yellow dot. To search messages more effectively, the calendar icon (bottom left corner of the screen) may be useful.

To view the address book, click the second icon from the left along the bottom of the screen. This allows the creation of new messages. Within the resulting message, the right-hand side shows others who have been messaged. This is potentially of use forensically as a communications channel requiring mutual authentication.

Apart from messages written by other Nintendo users, the mail function of the Wii stores messages and information from the system itself. The most common of these is entitled: *Today's Play History*. These messages record daily machine usage, and typically read similarly to:

News Channel
00:01
Wii Play
00:27
Total Play Time
00:28

These messages do not state the player or a time of day. However, there is potential forensic benefit in that an investigator may see the total amount of time the device was used, and a breakdown of the different areas. It may possibly be used as a means of corroborating events, statements or other information. The other advantage, from a forensic perspective, is that unlike messages, *Today's Play History* messages cannot be deleted.

E. Stage 8: Mii Channel

The second icon along the top row of the Wii main menu represents the Mii Channel. Mii's are person-based avatars that give interactivity in some games. The appearance of each Mii is customizable, with the intention that users will create Mii profiles that resemble themselves [8]. The forensic benefits of examining this information are minimal, however it may give a forensic investigator insight into the number and details of users who have interacted with the system. One case in the UK saw a man discover an unfaithful wife through the addition of another Mii character [9]. In addition, in the previous section, it was noted that the address book would allow users to link with a Mii, and this area may give more information about the character. However, interaction with the Mii Channel does alter the Nintendo system - notably the *Wii Play Time* message. Therefore, any channel-based interaction must occur after these settings have been accessed and recorded.

To access the Mii channel, click the Mii icon, and then click 'Start'. The main Wii screen shows all Mii characters that have been developed by users of the system. To view them in more detail, click the whistle icon in the bottom right corner, which will line up the Mii characters. By selecting them individually with the cursor, the name can be seen. When complete, the top left icon leaves the Mii Channel.

IV. Other Areas of Interest

Beyond the channels discussed already, the main console of the Wii may look different than that given in figure 1. Any purchases made at the Wii Shop Channel are also reflected on the main menu on different icons. Many of these will be purchased games or free extras developed by Nintendo. The mere existence of these channels does give some insight into the use of the system - the presence of the Forecast Channel, the News Channel and the Internet Channel all indicate that the system has connected to the Internet at some point and some of these may provide additional relevant information of investigative interest. However, each of these is not part of the standard set. As with the use of any channels, any access or interaction will alter the *Wii Play Time* messages, and this needs to be noted and accounted for.

A. Internet Channel

From a forensic perspective, such a device is both an issue and a potential source of electronic evidence. The forensic disadvantage of a web browser is the capabilities added to the device increase both the range and possibilities of misuse, but also provides another source of potential evidence.

The implementation of the Wii web browser, called the *Internet Channel*, (accessible from the main menu) has two potential issues from a forensic perspective; a lack of Internet user history and a lack of information in the Internet Favourites component.

The Wii Internet Channel lack of a user Internet history is of forensic issue as there is no permanent record maintained of a browsing session. This notable feature omission may be put down to the lack of permanent hard disk space available to store such information, but the forensic implication is frustrating - representing one less source of information for examination.

Whilst accessible from the main menu of the Internet Channel, the Favourites implementation for the Wii is specifically designed for television screens, and this may be one reason why the Favourites themselves do not explicitly state the URL they link to. Instead, each of the Favourites shows a thumbnail of the page as it appeared at the last visit, and the title of that page. There is no way, from within the Wii menu, to ascertain the page linked to. However, the use of an external analysis machine may be used to determine the Wii favourite links, and there are two methods of doing this. The first method is to perform an internet search on the link title, and compare the results with the thumbnail of the favourite on the Wii system. This is potentially inaccurate, especially given the ability for users to rename the favourite links. The other, more reliable method, takes a greater amount of technical skill, and involves connecting the target Nintendo Wii to a network and clicking the favourite link. If the network communications is monitored, either through the use of a wireless network traffic sniffer such as Kismet [10], or through a wired component, using an application such as Wireshark Network Analyzer [11], the interaction to and from the system may be made known. Within Wireshark, the Nintendo device is identified as 'Nintendo_XX:XX:XX, where the X's denote the last six digits of the MAC address.

It should be noted, however, that the Internet Channel is not a standard component of the Wii system and that it must be bought separately. Therefore, this stage may not be applicable in many systems. Also, as with other aspects of the Nintendo menu system, access to the Internet Channel will alter the *Wii Play Time*.

B. Forecast Channel

of the second row of the main menu, and has only limited forensic value. It allows, at a higher granularity than the *Systems settings* menu, to determine if a geographic location is of importance to the users of the system, but has little other interest within an investigation.

C. Wii Shop Channel

Although the Wii Shop could be potentially useful within a forensic investigation, the lack of stored customer data or sales history diminishes its potential use.

All purchased from the Wii Shop Channel are accessible directly from the main menu, but the shop itself has little information beyond this. It may be assumed, however, that Nintendo Co Ltd would maintain a sales history for each user, which may include payment method and details (such as credit card number and expiry), as well as IP address and other significant factors.

D. News Channel and Photo Channel

The News Channel is a primarily text-based new service that provides categories and lists of headlines from which you can access a full news article. It has very little forensic value.

The Photo channel is an image viewing application, and although it states that it does not alter files, it is not of forensic interest within itself. However, the existence of the Photo Channel may increase the potential forensic value of any SD memory cards that may be within the vicinity, as these may have been used to view images through the Wii.

One last consideration is that the System Settings also has a *Restore Factory Settings* option. There are two points of note for forensic analysts; first, the selection of this during an analysis of the machine will restore the machine to its factory defaults, and therefore will destroy any evidence contained on the system. The second point of interest is that the possibility that a device has been reset before analysis has occurred, and a lack of data (even data that cannot be manually deleted) may not imply that this data has not existed in the past. However, this deletion is an all-or-nothing mechanism, and data cannot be selectively removed.

V. Third Party Modifications

Compared with workstation PCs, consoles are considered more of a closed system. As consoles are generally unable to run arbitrary code, they are hence capable of less forms of misuse than PC systems. However, the use of third party hardware modifications, or "mod-chips" on different consoles has allowed features beyond the original manufacturer's design and often intention.

The installation and use of mod-chips may facilitate illegal acts (such as the copying and play of unauthorized or backup games), and this discussion is beyond the scope of this work, but investigators may encounter such systems in the field and therefore an understanding of how such systems are altered from their original state is of value. In particular, whether the above information is still accurate on a modified system, and whether featured such as the logging of Wii interaction will still occur. In addition, mod-chips for some consoles allow for the operation of unsigned code, which vastly increases the types and number of applications which may be run on the console, whish in turn increases the potential for that device's misuse and issues in any resulting analysis.

There are several competing brands of mod-chip for the Nintendo Wii, although anecdotally all of these work in a similar manner. Wii-ModChips.com (2007) state that, rather than modifying the Nintendo system, the mod-chip is physically attached to the DVD drive, and intercepts calls to the main unit. There are two benefits of this; to allow for the bypass of internal checks on the validation of the disc, and more recently, to allow for the running of unsigned code [12], [13].

The execution of unsigned code is of potential interest from a forensic perspective, as it increases the applications for the Nintendo system, and therefore the misuses that it is capable of when compared with a system able to only run signed code. In practice, there are few public projects porting applications and systems to the Nintendo Wii; there is an active WiiLi project seeking to port Linux to the Wii [14], but this has not yet released an operational system. However, should a Linux system be released for the Nintendo Wii, it will open up the number of ways in which the system may be of interest within an investigation and the forms of electronic evidence that can be gathered from it.

There is currently no simple method to determine whether a Nintendo Wii has been installed with a third-party mod-chip without physically opening the unit and searching for the chip [15]. Physically opening the system is not a trivial task, requiring the use of a Tri-wing screwdriver [4]. Alternatively, the presence of back up, non-legitimate or overseas Nintendo Wii games in the vicinity of a seized machine may indicate the presence of a mod-chipped system.

As a means of determining how a Nintendo system is affected by the presence of a mod-chip, the researcher installed one of the more popular brands, the WiiKey [16], and spent time using the system to determine if the presence of the chip would alter the information above. After physically installing the mod-chip, the system was tested to ensure that it still played original legitimate discs. This was confirmed, as was each of the processes described earlier in this work. As expected, all of these processes verified as before the mod-chip was installed. From the main menu, the system would still play legitimate discs, but the backed up disc was not recognized. To load this, another bootable DVD was required containing a 'setup disc'. This disc was recognized by the Wii as a Gamecube game, and when loaded, booted into a homebrew options menu.

Once activated, the mod-chip allows games to run as if they were original, and all features (such as use logging) still occurs. This allays the original fears held that the use of a mod-chip may bypass these systems. However, the system appears to operate as normal. The only potential issue is that the mod-chip will allow the construction of homebrew code - the setup disc was, by its very nature, unsigned and unauthorized. Therefore, there is the possibility that the potential pool of applications that may be run directly from the Wii console will expand, and may therefore include more methods of performing misuse. Although any system running as an external disc will appear as a game on the *Total Play* counter, a system such as the proposed WiiLi Linux port may bypass the Nintendo Operating System entirely, which would require a different structure for analysis.

VI. Conclusion and Further Work

This work has aimed to provide an insight into the Nintendo Wii as a source of potential digital evidence, and to provide a methodology for its investigation. Further research may determine less intrusive methods to analyzing the Nintendo Wii, but it is likely that all possible methods will involve some form of interaction with the device. The use of a closed, proprietary system and lack of permanent, accessible storage necessitate that all analysis must be conducted through the underlying operating system, which interprets the data within memory. However, this work has identified several areas of potential research, which could not be completed within the scope of this project. Specifically, the two current major communications mechanisms; messaging and internet usage, will need further exploration as they are updated and potentially

expanded over time. Ninendo's email and messaging system may be expanded to other systems over time, and the use of an obvious whitelisting process may be of forensic interest for heavy Wii users - all email addresses must exist on a server controlled by Nintendo. Such analysis would require cooperation from the server operators, but would be able to provide new or corroborating information.

It should also be noted that whilst the hardware of the Nintendo Wii is static, the addition of an internet connection has allowed the periodic upgrading of the Operating System and firmware. Therefore, it is possible that changes may occur in the system over time. Additionally, this work only analysed one mod-chip device, and the structure and firmware of these devices may also alter over time as the technology and understanding of the system increases.

One area that has been identified within this work is the extent that the addition of third party mod-chips potentially alters the investigative environment. This issue is not unique to the Nintendo Wii and is potentially exists for all modern gaming consoles and systems. The associated issue of having a modified system is that it opens the scope of the system, which potentially increases investigative avenues for the Nintendo Wii as a source of digital evidence.

It also may be possible to use the same systems that are being used to unlock the Nintendo Wii to develop a means of accessing and extracting the contents of the onboard memory. The use of existing exploits that allow the execution of unsigned code could allow a means of accessing the memory directly, which could then be copied for forensic analysis on a separate system. Such a system would also require interpretation of any raw dump of the memory.

Although outside of the scope of this work, Nintendo's wireless remote controller, colloquially termed the 'wiimote', has some measure of inbuilt memory that may hold the Mii avatars. It is not known whether this memory may be made available for the storage of other information, but investigating this possibility may be a future direction for research. In addition, accessing and interpreting this memory may also be of use to forensic investigators, if it is found that any information may be stored in these devices.

This research has aimed to provide an introduction into the analysis of the Nintendo Wii, noting the possibilities of evidence, how it may be extracted, and the limitations potentially imposed. In doing so, recommendations have been one outcome of this work, but the individual circumstances and the forensic examiner are obviously of importance in the interpretation of these. As can be seen by this research and similar guides and discussion, game machines are no longer isolated, single use machines, but are rapidly merging with other areas of computing, and hence have the possibility of being involved in forensic examinations.

REFERENCES

[1] P.K. Burke and P. Craiger, *Xbox Forensics*, Journal of Digital Forensic Practice, vol. 1, no. 4, 2006, pp. 275-282.

[2] E. Door, et al., *Investigating the Microsoft Xbox 360*, Book Investigating the Microsoft Xbox 360, Series Investigating the Microsoft Xbox 360, ed., Editor ed.êds., SEARCH - The National Consortium for Justice Information and Statistics, 2006, pp.

[3] VG Charts, *Hardware Comparison Charts*, 2007; http://www.vgchartz.com/hwcomps.php.

[4] B. Detwiler, *Cracking open the Nintendo Wii*, 2006; http://content.techrepublic.com.com/2346-10877_11-38683.html.

[5] S.Y. Willassen, *Forensic analysis of Mobile Phone Internal Memory*, Proc. 1st IFIP WG 11.9 Workshop on Digital Evidence, Springer Publishing, 2005.

[6] Nintendo Co. Ltd, *Nintendo Customer Service - Wii LAN Adapter*, 2007; http://www.nintendo.com/consumer/systems/wii/en_na/acc/wiiLAN.jsp.

[7] FrequencyCast UK, *http://www.frequencycast.co.uk/images/wii_02.jpg*, Book http://www.frequencycast.co.uk/images/wii_02.jpg, Series http://www.frequencycast.co.uk/images/wii_02.jpg, ed., Editor ed.êds., 2007, pp.

[8] Nintendo Co. Ltd, *Wii Operations Manual: Channels and Setting*, Self Published, copy available at http://www.nintendo.com/consumer/downloads/WiiChEng.pdf 2006.

[9] GoNintendo.com, *Wii have caught you cheating on your husband*, 2007; http://gonintendo.com/?p=29938.

[10] M. Kershaw, *Kismet Readme - Kismet 2007-01-R1*, 2007; http://www.kismetwireless.net/documentation.shtml.

[11] A. Orebaugh, et al., *Wireshark & Ethereal Network Protocol Analyzer Toolkit* (Jay Beale's Open Source Security), Syngress Publishing, 2006.

[12] Bushing, *Console Hacking: State of the Wii*, Book Console Hacking: State of the Wii, Series Console Hacking: State of the Wii, ed., Editor ed.êds., 2007, pp.

[13] A. Bradner, *Interview with a Wii Hacker*, 2008; http://www.atomicmpc.com.au/article.asp?SCID=14&CIID=102079&p=1.

[14] n.a., *WiiLii Project Page*, 2007; http://www.wiili.org/index.php/Main_Page.

[15] Wiikey, *Wiikey Installation Manual*, 2007; http://www.wiikey.cn/images/installWiiKey.pdf.

[16] Wii-ModChips.com, *Compare Wii ModChips: Nintendo Wii*, 2007; http://www.wii-modchips.com/compare.htm.

Dr. Benjamin Turnbull Benjamin Turnbull is currently employed as a Post-Doctorate Research Fellow working at the Defence and Systems Institute, at the University of South Australia. His research interests are primarily in the field of forensic computing and electronic evidence.