

Running Head: VIDEO GAME DEVICE ONTOLOGY

Video Game Device Ontology

Alex Barnett

Purdue University

### Abstract

Modern video game devices more closely resemble personal computers than their primitive, specialized ancestors. Today's gaming consoles can store hundreds of gigabytes of data, connect to and browse the Internet, transmit live video and audio conversations, and much more. Should the device be modified using a 3rd party modification chip or operating system, the capabilities of the device can be expanded even further, even to the point that it is indistinguishable from a normal PC or server (from a logical standpoint). Recognizing these advances and capabilities, it is conceivable that these devices could be used to commit or assist in criminal activities, and therefore must be considered viable sources of digital evidence.

In today's average home, there are a staggering number of sources of potential digital evidence. Common sources such as PCs, cell phones, thumb drives, and PDAs have all received hundreds, if not thousands of hours of research and attention from law enforcement officials and academia alike. However, another common digital device has received almost no attention, that device being the modern video game console. These devices have come a long way since their introduction in the early 70s, when they were essentially primitive, highly-specialized embedded chip devices. Today's gaming consoles are as far removed from their ancestors as the modern PC is from the ENIAC, boasting Internet connectivity, player-to-player messaging via text and audio, onboard storage ranging from 512 MB to 250 GB, and more. These highly-complex devices are no longer relegated to simply playing video games and can be used for many activities usually associated with normal PCs. With 3rd party modifications, these devices can essentially become indistinguishable from desktop computers in behavior and function. It is therefore important to realize that these devices can be utilized as tools for committing or assisting in criminal activity, such as the storage and distribution of child pornography or online harassment, and should be treated as valid sources of evidence. Unfortunately, very little has been written regarding proper forensic examination methods for video game consoles, which may prevent law enforcement officials from discovering useful evidence held on these devices.

As with any field of digital forensics, it is important to first define the attributes that allow a device to be recognized as part of that field. Harrill and Mislán (Harrill & Mislán, 2007) include gaming devices as a sub-category in their small scale digital device ontology, but due to the growing number and complexity of these devices, a new category needs to be defined. To create a simple definition, a video game device can be any device whose primary purpose is the execution of video games, but may have other abilities as well. To give a practical example, this

definition would include the PlayStation 3, which can function as a Blu-ray player on top of its primary purpose of playing video games, but would not include the iPhone, which has a large library of game applications, but whose primary purpose is to function as a cellular phone. To further define the device, it can be given attributes from the following categories:

- **Generation.** A generation defines a time period in which gaming devices of comparable hardware are released. As of 2009, we are in the seventh generation of video game devices. From a forensic standpoint, generally only the sixth generation of devices and onward are relevant.
- **Console or Portable.** A console can be defined as a video game device that is plugged into a television or other display device and generally remains in one place. A portable game device can be defined as a gaming system that is small enough to be carried outside of the home and runs on batteries.
- **Modified or Unmodified.** A modified gaming device utilizes a 3rd party exploit (either hardware or software) to overcome the device's security restrictions and expand the capabilities of the device beyond the developer's intentions. A practical example of this would be to install the Linux operation system on a Microsoft Xbox. An unmodified console is one that utilizes factory default settings. Worth noting is that modern consoles are often issued optional operating system updates by their manufacturer, so depending on the version, unmodified consoles may have different capabilities. One practical example of this would be the Nintendo Wii 3.0 system update, which added AOSS network compatibility.

Once a device is properly categorized, its relevance to the investigation can be more accurately judged. For example, an unmodified Nintendo DS may be of little value to a case, but

a PlayStation 3 running a 3rd party operation system and utilizing a 250 GB hard drive will certainly warrant investigation. To facilitate a better understanding of these categories, the next three sections will go into further detail regarding each of the three aforementioned categories.

### *I. Generation*

The first generation of video game consoles began in 1972 with the release of the Magnavox Odyssey (Wolf, 2008). From the first generation through the fifth generation, video game devices were essentially highly-specialized embedded chip devices that did not offer much functionality beyond the execution of whatever game media they were being used to run. The only notable exception to this was the Sega Saturn, a member of the fifth generation, which could use a 1st party add-on 28.8 kbps modem to browse the Internet and send email.

The sixth generation of gaming devices began in 1998 with the release of the Sega Dreamcast. Like the Saturn, the Dreamcast also had Internet capabilities, with a notable difference being that it came with a built-in 56 kbps modem whereas the Saturn required an optional add-on card. In addition to the modem, an add-on broadband adapter was also available, further expanding the Dreamcast's capabilities. With further add-ons, such as the Dreamcast keyboard and mouse, the console could be utilized for web browsing and other associated activities.

It is important to note that these advances ushered in an age where the availability of network connectivity for gaming devices would become standard. The Nintendo Gamecube and Sony PlayStation 2, which were both released within two years of the Dreamcast, both offered optional network adapters. However, with the release of the Microsoft Xbox in November 2001, the role and capabilities of video game consoles in the home would be significantly changed.

The Microsoft Xbox was the first gaming console to be released with both a network adapter and an internal hard drive as factory default settings. Featuring an 8 GB hard drive, a 100 Mbit network card, and a custom Intel Pentium III processor, the Xbox became an attractive target for the 3rd party modification community. Utilizing various techniques to get around the console's security restrictions, the Xbox could fairly easily be made into a Linux desktop PC that was comparable to low-end PCs available at the time. As modification techniques improved, the restriction of the 8 GB hard drive was overcome so that any parallel ATA hard drive could be used. With enough time and effort, an Xbox could be upgraded to a high-capacity media center that could switch back and forth between operating systems and still be utilized for Xbox gaming.

Also worth noting is that Sony later released a 1st party add-on hard drive for the PlayStation 2, which came bundled with a combination hard drive adapter/wired network adapter. Since the release of these peripherals, the PlayStation 2 has received the same treatment as the Xbox from the modification community. While not as widespread as Xbox modification, modified PlayStation 2 consoles do exist, and can fulfill the same roles as a modified Xbox. Considering the wide availability of modification chips and the relative ease with which guides detailing the modification process can be obtained, it would be foolish to ignore any console in a situation where digital evidence is being sought.

The seventh, and current, generation of gaming devices has introduced three home-based consoles and two portable systems, all of which possess integrated networking capabilities. The Nintendo Wii, Nintendo DS, Sony PlayStation 3, and Sony PlayStation Portable all ship with built-in wireless adapters that allow them to connect to any 802.11b/g network (with some restrictions on encryption types), while the Microsoft Xbox 360 has an option add-on Wireless

adapter. The Microsoft Xbox 360 and Sony PlayStation 3 have built-in wired Ethernet connections, while the Wii has an optional add-on wired adapter. All three consoles now ship with built-in persistent storage, although the available size and implementation varies between consoles. The Xbox 360 and PlayStation 3 both utilize hard drives ranging from 20 GB to 250 GB, while the Wii utilizes a 512 MB flash chip soldered directly to the motherboard. In terms of I/O, all three consoles utilize USB 2.0 ports, and both the Wii and PlayStation 3 support Bluetooth connections. Also worth noting is the fact that the Wii and PlayStation 3 both contain slots for SD cards. As should be readily apparent by now, the line between gaming device hardware and desktop computer hardware is starting to blur.

Even left unmodified, seventh generation devices allow the user to send textual and audio messages to other players, browse the Internet, send, receive, and store images, download and watch movies, and much more. With combined sales of over one hundred million units worldwide, it is extremely likely that these devices will be encountered during the course of an investigation, and may in fact contain useful evidence.

## *II. Portable vs Console*

Portable video game devices are easily distinguishable from their home-based console counterparts, using batteries instead of relying on a power cord. While not as powerful as a console, portable game devices have made significant advances in power since their early days, and may now incorporate functions similar to PDAs.

The following are technical descriptions of forensically-relevant game devices from the current and previous generations. Note that the Nintendo Gamecube and Sega Dreamcast are omitted due to their lack of persistent storage devices.



(History of video game consoles (seventh generation), 2009)

Name	Sony PlayStation Portable/PSP Go
Categorization	Seventh-Generation Portable
CPU	Dual R4000-based MIPS clocked from 1 to 333 MHz
RAM	32-64 MB (depending on unit model)
Resolution	480x272
Networking	802.11b, Bluetooth (only on the PSP Go)
Media	UMD, Memory Stick Duo
Ports	USB, Memory Stick Duo, UMD, IrDA
Storage	Via Memory Stick Duo on most models, 16 GB flash memory (PSP Go)

Forensic viability: The PlayStation Portable may be used to access the Internet, store images and movies, and can be modified to run 3rd party operating systems (Mo, 2008).

The PSP has had several different hardware iterations: The PSP-1000, PSP-2000, PSP-3000, and the PSP Go. The 2000 and 3000 have twice the RAM of the 1000 and noticeable cosmetic differences. The PSP Go is a complete redesign and features internal storage and Bluetooth capabilities. All four units utilize the same processor.



(History of video game consoles (seventh generation), 2009)

Name	Nintendo DS/DSi
Categorization	Seventh-Generation Portable
CPU	67 MHz ARM9 and 33 MHz ARM7 (DS) 133 MHz ARM (DSi)
RAM	4 MB SRAM (DS) 16 MB (DSi)
Resolution	256x192 (Both screens)
Networking	802.11b, 802.11g (DSi)
Media	DS game card, Game Boy Advance cartridge (DS only), SD Card (DSi only)
Ports	DS game card, Game Boy Advance cartridge (DS only), SD Card (DSi only)
Storage	Nintendo DS Game Card, SD(HC) card (DSi only), 256 MB flash RAM (DSi only)

Forensic Viability: All Nintendo DS units can establish ad-hoc wireless connections to other units to utilize a P2P chat program called PictoChat. PictoChat has been used in the past by predators to lure children to them (Mathieu, 2009). The DSi incorporates an SD card reader, which may be used to hide illicit materials. The DSi also incorporates a 0.3 megapixel camera which can store images on its internal flash RAM or SD card.

The Nintendo DS has gone through four hardware iterations: The Nintendo DS, the DS Lite, the DSi, and the DSi XL.



(Xbox, 2009)

Name	Microsoft Xbox
Categorization	Sixth-Generation Console
CPU	733 MHz X86 Intel Celeron/PIII Custom Hybrid
RAM	64 MB DDR SDRAM
Networking	10/100BASE-TX Ethernet
Media	DVD-ROM, CD-ROM
Ports	Four proprietary USB 1.1, Ethernet
Storage	8 or 10 GB 3.5" IDE Hard Disk (formatted to 8 GB). FATX file system.

Forensic viability: Without modifications, little information can be retrieved from the system except text messages sent between players. However, if the device has been modified beyond factory settings with a desktop OS, it can potentially have all of the same capabilities of any normal desktop PC and should be treated as such. Also worth noting is that the only official hard drives released with the console are either 8 GB or 10 GB in size, and therefore any different-sized hard drive present in the system is a good indication that the console has been modified. Note that, by default, the system uses the FATX file system, which many forensic tools are unable to read. Burke and Craiger have written an excellent guide detailing a forensic method to examine an Xbox hard drive in a Linux environment (Burke & Craiger, 2006), which should be consulted by interested parties.

As with most modern consoles, the Xbox can be modified to run Linux (XBox-Linux, 2009). Any modified console should be treated the same as a normal desktop PC.



(PlayStation 2, 2009)

Name	Sony PlayStation 2
Categorization	Sixth-Generation Console
CPU	64-bit "Emotion Engine" clocked at 294.912 MHz
RAM	32 MB RDRAM
Networking	10/100BASE-TX Ethernet (optional)
Media	DVD-ROM, CD-ROM
Ports	Two standard USB 1.1, Proprietary controller/memory card ports, Firewire, Ethernet (optional)
Storage	40 GB 3.5" IDE Hard Disk (optional)

Forensic viability: Without modifications, little information can be retrieved from the system. However, if the device has been modified beyond factory settings, it can potentially have all of the same capabilities of any normal desktop PC and should be treated as such. Worth noting is that the only official hard drive released for this console is 40 GB in size and manufactured by Sony, and therefore any different-sized hard drive present in the system is a good indication that the console has been modified. Also worth noting is the PlayStation 2 was released on two versions: The original and the slim. The slim does not possess hard drive capabilities.

Like the Xbox, Linux has been made to run on modified PlayStation 2s (PlayStation 2 Linux Community, 2009). Again, this renders the system essentially no different from a normal desktop PC, and should be treated as such during examination.



(History of video game consoles (seventh generation), 2009)

Name	Nintendo Wii
Categorization	Seventh-Generation Console
CPU	729 MHz PowerPC based IBM "Broadway"
RAM	24 MB "internal" 1T-SRAM integrated into graphics package 64 MB "external" GDDR3 SDRAM 3 MB GPU frame buffer memory
Networking	802.11b/g, 10/100 Ethernet (optional)
Media	Wii optical disk, SD Card
Ports	Bluetooth, Wii optical disk port, SD Card reader, two USB 2.0 ports, Ethernet (optional)
Storage	512 MB Flash memory, SD card (up to 32 GB)

Forensic viability: Little is known regarding what logs the Wii stores. It can utilize a first-party Opera-based web browser, but at this point it is unknown what, if any, records of browsing history are stored. However, bookmarks are retained, and may be worth noting. The Wii also retains a basic, daily log of system usage, and also keeps a contact list of added friends, as well as the messages those friends have sent. Also worth noting is that images may be sent over the player messaging system, which are then saved to the system flash storage or to an external SD card. As is true of most modern consoles, various distributions of Linux have been ported to the system (Wii Linux, 2009), meaning that it could be utilized in the same way as any desktop PC and should be treated as such.

Due to the closed nature of the system, forensic examination is difficult, but not impossible (Turnbull, 2008). As Turnbull describes, provided that a video recording device is

present, information such as player-to-player messages, system clock information, network connection settings, and other information previously mentioned above can be collected in a forensically sound manner. However, this approach is far from ideal due to its manual nature and chance of evidence modification. One potential solution to this problem has come out of the Wii homebrew software community in the form of an application that dumps the contents of the Wii's persistent memory to an inserted SD card (Wii FileSystem Dumper v1, 2008). However, further research into the Wii's file system structure will be required before this tool's usefulness can be determined.



(History of video game consoles (seventh generation), 2009)

Name	Microsoft Xbox 360
Categorization	Seventh-Generation Console
CPU	3.2 GHz IBM PowerPC tri-core codenamed "Xenon"
RAM	512 MB GDDR3 @ 700 MHz shared between CPU & GPU 10 MB EDRAM GPU frame buffer memory
Networking	802.11b/g (optional), 10/100 Ethernet
Media	CD, DVD, HD-DVD (optional)
Ports	3 USB 2.0, IrDA, Ethernet, 2.4 GHz ISM band radio, memory card slots
Storage	20, 60, 120, or 250 GB 2.5" SATA Hard Drive (swappable)

Forensic viability: The Xbox 360 may store large amounts of digital media on its hard drive. Also, textual and audio messages sent between players via the Xbox LIVE online system may be of interest. Worth noting is that messages sent via the Xbox LIVE service are retained on Microsoft's servers and are accessible from any console that the profile is logged into, so letters of preservation are advisable in the event that such information is deemed potential evidence.

Again, Linux can be run on the Xbox 360 (Wiki/Main Page, 2009), and it should therefore be examined carefully.



(History of video game consoles (seventh generation), 2009)

Name	Sony PlayStation 3
Categorization	Seventh-Generation Console
CPU	Cell Broadband Engine (3.2 GHz POWER-based PPE with seven 3.2 GHz SPEs)
RAM	256 MB XDR @ 3.2 GHz, 256 MB GDDR3 @ 700 MHz
Networking	10BASE-T/100BASE-TX/1000BASE-T Ethernet, 802.11 b/g
Media	Blu-Ray Disc, DVD, CD
Ports	Bluetooth 2.0, 4 USB 2.0 ports, 1 Ethernet port, 1 Memory Stick slot Pro/Duo, 1 SD/mini SD port, 1 Compact Flash port
Storage	20, 40, 60, 80, 120, 160 or 250 GB 2.5" SATA Hard Drive (swappable)

Forensic viability: The PS3 is similar to the Xbox 360 in terms of potential viability.

Large amounts of digital media can be stored on its hard drive, and the PlayStation Network (similar to Xbox LIVE) allows users to send messages much in the same way as with the Xbox 360. One key difference between the consoles is that 3rd party operating systems can be installed on the device without any sort of modification. One company has even gone so far as to sell pre-configured PS3 clusters for supercomputing applications (Fixstars, 2009), so special attention should be paid to any PS3 suspected of modification.

The PS3, like the PS2, has been released in both normal and slim versions.

### *III. Modified vs Unmodified*

As has been stated many times thus far, modified video game devices possess capabilities beyond the device's original design. In some cases, these modifications are used to circumvent copy protection measures, allowing the user to play pirated games. In others, modifications are made so that the device can execute code that allows the user to install 3rd party operating systems, or even play games from other systems via emulation. Once modified to this extent, a console may become indistinguishable from a normal desktop PC or server (at least from an operational perspective).

One important detail to note is that, at least from the outside, a modified console and an unmodified console can look exactly the same. While it is true that some members of the modding community opt to apply various case modifications to their consoles (ranging from simple paint jobs to clear plexiglas case transfers), many do not, and therefore the console could easily be mistaken for a standard, unmodified device. Due diligence is therefore necessary when examining video game devices in order to determine their status.

Modifications, aside from purely cosmetic changes, can be lumped into two categories: Softmods and hardmods. A softmod is a procedure where a programming flaw is used to circumvent the device's security restrictions to execute foreign code, without physically modifying the device. One common example of this technique is the Mech Assault Xbox softmod which, using a buffer overflow exploit present in the game 'Mech Assault', allowed code stored on an Xbox memory card to be executed. Using this method, users were able to install other operating systems on the original Xbox.

A hardmod, on the other hand, is when a user makes a physical modification to the device's circuitry, usually in the form of a device known as a modchip. Modchips used to allow the installation of alternative operating systems are typically soldered to the motherboard of a console and force a different boot sequence than intended by the manufacturer. This usually means utilizing a 3rd party BIOS, which allows the user to execute foreign code without the need of a software exploit. On the other hand, not all modchips are use for this purpose. Some are simply used to circumvent the device's copy or region protection, which would allow the user to play burned disks or games from other regions (NTSC, PAL, etc).

To determine if a device has been modified, assuming a forensic copy has been made, simply boot it up. An alternative technique would be to examine the contents of the hard drive, which may or may not be feasible depending on the tools available to the examiner. For example, a standard Xbox hard drive would be unreadable to most forensic toolkits, but a modified console running Linux would not present that problem. A physical investigation of the system hardware is also prudent, assuming it has been hardmodded. Most modchips are stamped with serial numbers or other identifying marks, which can provide investigators with valuable information regarding how to proceed.

In terms of investigative methods, very little has been written regarding video game device examination. While some traditional methods may be useful, such as the creation of bit stream copies of the storage media, a number of problems quickly become apparent; To begin with, not every video game device uses a storage medium that can easily be duplicated. The Nintendo Wii, for example, uses flash memory soldered directly to the motherboard, which is extremely difficult to remove without damaging. Assuming the chip could be removed and somehow read by another device, the Wii uses a proprietary file system about which little is

known, and a directory structure which is undocumented. Other consoles present similar problems: Little is known about where specific information is stored in the directory structure, and the file systems are either unreadable or can only be read by unverified tools. A comparison of a factory fresh console and a used console using KDIFF may prove helpful in determining where new data is stored, however this may not be viable for different versions of consoles.

Regarding tools that can be used for analysis, there is also very little available. Common toolkits will not read game device file systems, so the only available tools that function properly have come out of the modification and hacking community. These tools are often never developed past beta versions and may contain bugs or other flaws that could corrupt evidence or hamper the investigation. Also, due to their nature, they may not stand up to legal scrutiny.

Moving forward, there are four key areas that require research in order to properly investigate these devices. First, tools must be developed that can read all of the devices' various file systems, with special emphasis on adhering to legal standards. Second, an understanding of each system's proprietary file formats will be key in discovering potential evidence. Third, an understanding of the device's file system structure will allow investigators to more quickly locate and analyze any relevant information. Finally, with this information, it will be possible to create software tools to assist in discovering and processing data from these devices.

Clearly, the lack of information and research about video game devices represents a problem for any law enforcement agency tasked with examining these systems. With a better understanding of these devices, it is possible that new avenues of evidence retrieval could be pursued, and further useful evidence obtained. Until adequate investigation techniques are proposed and documented, more research into this field will be required.

## Works Cited

(2009, August 11). Retrieved October 19, 2009, from XBox-Linux: [http://www.xbox-linux.org/wiki/Main\\_Page](http://www.xbox-linux.org/wiki/Main_Page)

(2009, June 04). Retrieved October 19, 2009, from PlayStation 2 Linux Community: <http://playstation2-linux.com/>

Burke, P., & Craiger, P. (2006). Xbox Forensics. *Journal of Digital Forensic Practice* , 275-282.

*Fixstars*. (2009). Retrieved December 2, 2009, from <http://www.fixstars.com/en/index.html>

Harrill, D., & Mislán, R. (2007). A Small Scale Digital Device Forensics ontology. *SMALL SCALE DIGITAL DEVICE FORENSICS JOURNAL* .

*History of video game consoles (seventh generation)*. (2009, October 19). Retrieved October 19, 2009, from Wikipedia:  
[http://en.wikipedia.org/wiki/History\\_of\\_video\\_game\\_consoles\\_%28seventh\\_generation%29#Comparison](http://en.wikipedia.org/wiki/History_of_video_game_consoles_%28seventh_generation%29#Comparison)

*History of video game consoles (seventh generation)*. (2009, October 18). Retrieved October 19, 2009, from Wikipedia:  
[http://en.wikipedia.org/wiki/History\\_of\\_video\\_game\\_consoles\\_%28seventh\\_generation%29#Handheld\\_systems](http://en.wikipedia.org/wiki/History_of_video_game_consoles_%28seventh_generation%29#Handheld_systems)

Mathieu, D. (2009, March 20). *Warning: Child predators can use Nintendo DS to chat with your kids*. Retrieved October 19, 2009, from WOAI.com:  
<http://www.woai.com/content/troubleshooters/story/Warning-Child-predators-can-use-Nintendo-DS-to/7cvwzePdUECLrNlkndDT6w.csp>

Mo, J. (2008, February 3). *Linux on PSP*. Retrieved October 19, 2009, from <http://jacksonm80.googlepages.com/linuxonpsp.htm>

*PlayStation 2*. (2009, October 18). Retrieved October 19, 2009, from Wikipedia:  
[http://en.wikipedia.org/wiki/PlayStation\\_2#Technical\\_specifications](http://en.wikipedia.org/wiki/PlayStation_2#Technical_specifications)

Turnbull, B. (2008). Forensic Investigation of the Nintendo Wii: A First. *Small Scale Digital Device Forensics Journal* .

*Wii FileSystem Dumper v1*. (2008, April 13). Retrieved December 2, 2009, from WiiNewz:  
<http://wiinewz.com/forums/nintendo-news/67726-wii-file-system-dumper-v1.html>

*Wii Linux*. (2009, October 19). Retrieved October 19, 2009, from Wii Brew:  
[http://wiibrew.org/wiki/Wii\\_Linux](http://wiibrew.org/wiki/Wii_Linux)

*Wiki/Main Page*. (2009, September 22). Retrieved October 19, 2009, from Free60:  
[http://www.free60.org/Wiki/Main\\_Page](http://www.free60.org/Wiki/Main_Page)

Wolf, M. J. (2008). *The video game explosion: a history from PONG to Playstation and beyond*. Greenwood Publishing Group.

Xbox. (2009, October 18). Retrieved October 19, 2009, from Wikipedia:  
[http://en.wikipedia.org/wiki/Xbox#Technical\\_specifications](http://en.wikipedia.org/wiki/Xbox#Technical_specifications)