B16 Taking a Deeper Look Inside Microsoft's XBox® 360: The Acquisition and Investigation

Veronica Y. Serrano, 3904 Regatta Rd, Yukon, OK 73099; and Mark R. McCoy, EdD, Forensic Science Institute, 100 N University, Edmond, OK 73034*

The goals of this presentation are to discuss: (1) data preservation and forensic collection from an XBox® 360 system; (2) forensic investigation of an XBox® 360 system; and, (3) differences between the XBox® 360 FATX file system and other computing systems, such as Windows™ and Macintosh-based file system structures and file formats.

This presentation will impact the forensic science community by providing basic tools and techniques used to forensically acquire information of evidentiary value on XBox® 360 gaming devices.

The Microsoft XBox® 360 with Kinect is the latest online gaming device on the market. The addition of the Kinect gives the XBox® 360 the ability to control games without using a controller, to record voices, and to snap digital images of the users. The XBox® 360 is recognized as a popular entertainment and educational device, as well as a platform that can be used by online predators to victimize children or store evidence of criminal activity. Because the XBox® 360 can be used in criminal activity, it is vital that digital forensics examiners be able to recover items of evidentiary value. While some research has been conducted on forensic examination of the XBox® 360, no known studies have addressed the evidence left on the XBox® 360 with Kinect. This study examines the evidentiary artifacts left by users on the XBox® 360 with Kinect and the implications for digital forensics examiners.

The first step is being able to capture the image of the drive used by the XBox® 360 system. However, despite it being able to be imaged as any other hard drive would, the file system is unsupported by Windows and can only be read by a special program. This program, known as Xplorer 360, is the only known program on the market today that has been able to read, write, and retrieve information from a hard drive used by an XBox® 360 system. Using this program, examiners will be able to retrieve information from a user's game history, saved games, achievement lists, gamer information; even photos and video bites captured from the game.

Once the basics of acquisition have been covered, a basic overview of the XBox® FATX file system will be provided so participants will be able to familiarize themselves with the system and the differences between Windows or Mac OSX file systems as well as be able to find information kept in the memory of the system taken from the XBox® 360 Kinect that is or may be of evidentiary value. A basic overview of how to use the program Xplorer 360 to retrieve such information taken by the XBox® 360 Kinect will also be provided.

Due to increasing XBox® 360 with Kinect system sales, working with these gaming devices, being able to study how they are being used in criminal activity, and understanding the system so one can retrieve any information that may be of evidentiary value is essential as the future of this technology grows. Such knowledge would prove useful in any forensic investigator's toolbox in that, should the crime related to it ever arise; such information would be greatly beneficial to getting one step closer to solving the puzzle.

Digital Forensics, Xbox® 360, Investigation

 ** Presenting Author*