XBox forensics

30 April 2009

A forensics toolkit for the Xbox gaming console is described by US researchers in the latest issue of the *International Journal of Electronic Security and Digital Forensics*. The toolkit could allow law enforcement agencies to scour the inbuilt hard disk of such devices and find illicit hidden materials easily.

Computer scientist David Collins has probably spent more time messing around with the Microsoft XBox, other gaming consoles, and PDAs in the name of forensic science than anyone else. He is a digital forensics expert at Sam Houston State University, and is working hard to replicate "mods" - both hardware and software for the Xbox and other devices.

Criminals often hide illicit data on the XBox in the hope that a gaming console will not be seen as a likely evidence target especially when conventional personal computers are present in the same premises, for instance. The toolkit developed by Collins will allow police and other investigators the chance to lay bare the contents of XBox hard disks.

Cell phones, smart phones, PDAs, game consoles and other devices provide a convenient means to store data of all kinds, including images, video, audio and text files. But they also provide a simple way for criminals to possess and hide illegal material too.

Collins' XFT utility can mount an image of the FATX file system used by the XBox, allowing the user to explore in detail the directory structure. Collins points out that unlike the standard FAT32, NTFS, and similar systems used by the hard disks in personal computers, there is little documentation on the proprietary FATX system. However, it is possible nevertheless to acquire an image of a FATX hard disk and to mount it on another device.

"Once the Xbox file system is mounted, the analyst can use shell commands to browse the directory tree, open files, view files in hex editor mode, list the contents of the current directory in short or long mode and expand the current directory to list all associated subdirectories and files," explains Collins.

Importantly, from the legal perspective, XFT can also record such investigative sessions for playback in a court of law, which protects the defendant from falsified as well as providing more solid evidence for the prosecution.

Collins explains how future work on XFT will involve making the toolkit into a fully functional forensic operating system (OS). This OS will be packaged as both a bootable operating system from a hard disk and a "live" bootable compact disk. "This implementation will be open source, verbosely commented and designed from the ground up as a forensic OS," says Collins, "This will remove any and all proprietary operating system dependencies, making the forensic process as transparent as possible."

Source: Inderscience Publishers (news : web)

APA citation: XBox forensics (2009, April 30) retrieved 20 October 2019 from https://phys.org/news/2009-04-xbox-forensics.html