PlayStation helps paint user's digital footprint

May 6 2015, by Carys Garland

Dr Read says discovering a lot of the significant information on a PlayStation cannot be accessed if the internet is disabled, which is standard practice for digital forensics. Credit: Farley Santos

Digital investigators are now able to extract information stored on a

PlayStation 4 console thanks to a forensically sound method developed by local researchers.

New web browsing and communication features of gaming consoles could prove valuable to law enforcement investigators, with the idea prompting research into ways of obtaining information.

Edith Cowan University Security Research Institute adjunct professor Iain Sutherland says the PlayStation 4 posed some challenges for data recovery, including its non-standard file system, something that tells the operating system how files are arranged.

Prof Sutherland says the team wanted to avoid simply turning on the console and looking at what was on the screen because of the potential to alter evidence as they explore menus.

"If there are things like a time stamp of when it was last accessed, then because you're accessing it, you're changing the time stamp," Prof Sutherland says.

Instead, researchers tried using a file carving tool; a method that works to find the beginnings and ends of files which are characterised by particular sequences and numbers.

However, this method was unsuccessful in retrieving data, likely due to the console being encrypted.

University of South Wales senior computing lecturer Huw Read says the team used the graphical user interface—the console menu that appears when the PlayStation is turned on—to navigate their way around the system.

A PlayStation 4 with the forensics kit in use. Credit: Carys Garland

"By carefully navigating between the different menus, the logs, the settings, etcetera, we were able to manually extract information useful to forensic examiners," Dr Read says.

A shadow drive was used to ensure any inadvertent changes made to the PlayStation could be restored to the original state.

Prof Sutherland says they used appropriate write-blocking technology to prevent changes to data.

"What we would do was carry out specific activities on the system, then take the drive out, plug the drive into a shadow drive and then analyse what data was present on the disk," he says.

"We were able to check the drive was not altered in any way by this method."

Dr Read says discovering a lot of the significant information on a PlayStation cannot be accessed if the internet is disabled, which is standard practice for digital forensics.

"A lot of the information we recovered was stored on Sony's Cloud, indicating a continuing trend for forensic investigators, in that the evidence is less about the gadget in your hand, but what the gadget lets you access and store online," he says.

  More information: "Forensic analysis of a Sony PlayStation 4: A first look," *Digital Investigation*, Volume 12, Supplement 1, March 2015, Pages S81-S89, ISSN 1742-2876, dx.doi.org/10.1016/j.diin.2015.01.013

Provided by Science Network WA