When I'm Sixty Four (Bits)

10 Aug 2009

ManTech
International Corporation ®

Jesse D. Kornblum, ManTech International Corporation
jesse.kornblum@mantech.com

Forensic examiners are going to have to process computers running 64-bit operating systems in the near future. While this won't affect people doing document forensics, it will require significant changes for those who do code based forensics such as reverse engineering, malware analysis, etc.

Processors capable of running 64-bit code have been available for many years and they are installed on a sizable percentage of the existing computer population. But as of this moment the majority of users are still running 32-bit operating systems.

Until now most users have not had a compelling need for 64-bit computing. The primary advantage of a 64-bit operating system is that it allows individual programs to use more than 4GB of memory. The system as a whole can use more than 4GB thanks to technologies like Physical Address Extension (PAE)[1]. On Microsoft Windows an application can address more than 4GB or memory using Address Windowing Extensions (AWE)[2]. But these are not perfect solutions. PAE still limits each application to 4GB and the AWE requires developers to modify their programs for manual memory management. Those kinds of changes cost money to implement and software developers aren't about to spend it unless there's consumer demand.

Recently, however, some users have developed a need for applications that can use more than 4GB of memory. The files used by image and video editing programs, for example, are getting massive. Since programs run faster when they can keep their documents in RAM, some programs are getting to the point where they need more than 4GB of memory and thus a 64-bit operating system. In fact, Adobe has stated, for processing large files with Adobe Photoshop, "additional RAM usage requires a 64-bit version of Windows and a 64-bit capable computer."[3]

The marketplace, ever eager to meet consumer demand for 64-bit operating systems *and* sell new products, is responding in force. Major retailers are now selling 64-bit computers. These aren't just the souped up systems marketed to gamers and overclockers, but ordinary computers being sold to the mass market. For example, take a look at the Sunday newspaper circular for Office Depot[4]. (Right away, 'dead tree advertising' should give you a sense that we're not exactly on the technological bleeding edge.) The store is offering a number of personal computers and laptops, *all of which come with a 64-bit version of Windows Vista installed*. (As a bonus, if the thought of changing your methodologies for 64-bit systems doesn't worry you enough, remember that most of these machines come with a free upgrade to Windows 7 when it's released in October.)

---

[1] Microsoft Corporation, *Physical Address Extension – PAE Memory and Windows*, http://www.microsoft.com/whdc/system/platform/server/PAE/PAEdrv.mspx.
[2] Microsoft Corporation, *Address Windowing Extensions*, http://msdn.microsoft.com/en-us/library/aa366527%28VS.85%29.aspx.
[3] Adobe Corporation, *Compare Photoshop CS4 Versions,* http://www.adobe.com/products/photoshop/compare/, accessed 9 Aug 2009.
[4] Office Depot, Sunday advertisement in *The Washington Post*, 9 Aug 2009.

But moving to 64-bit operating systems doesn't mean everything will change. Many forensic examiners practice and will continue to practice document forensics. They are looking at the documents created by the user and stored on non-volatile media such as hard drives, USB sticks, CDROM, etc. The files created by the 64-bit version of Microsoft Word, for example, are indistinguishable from those created by the 32-bit version. In fact, when looking only at those files you may not be able to tell that they were created on a machine running a 64-bit operating system. The same will go for email, web browsing history, chat logs, NTFS artifacts, and many data we've come to depend on using during investigations. Document examiners might not even notice the switch to 64-bit computing.

On the other hand, examiners running cases that involve malicious software, reverse engineering, and other things that involve interaction with the operating system and the processor are going to see some changes. Memory forensics, which is highly dependent on the operating system and underlying architecture, will be significantly impacted. Examiners won't have to relearn everything though. The x64 instruction set is a superset of the x86 set. But there are some new wrinkles, namely instructions designed to process 64 bits of data at once. It's also possible there will be a rash of issues relating to the new 64-bit codebases. These codebases have not been used as much as their 32-bit counterparts and may contain bugs. One of the more common bugs could be parts of programs that expect to get 32-bit inputs but instead receive 64-bits.

In the words of Douglas Adams, DON'T PANIC. There are lots of free resources to help examiners learn about 64-bit architectures. There are two 64-bit architectures in use today that examiners should know. The first, x64, is a hybrid creation of the Intel Corporation and Advanced Micro Devices (AMD). Your first stop to learn more should be the Intel Architectures Software Developer's Manuals[5]. You can download free copies of these intensely detailed guides to how everything works on both x86 and x64 processors. Every instruction and its side effects are explained, along with paging, caching, and all of the other things those little silicon chips do. AMD offers something similar called AMD Architecture Tech Docs[6]. The other 64-bit architecture is the IA-64 platform, which runs on Intel Itanium chips. Intel, of course, also provides Itanium Architecture Software Developer's Manuals[7] free of charge.

Sixty four bit computing is coming, but it is nothing to be frightened about. The need to process large files in memory is driving users to purchase computers with 64-bit operating systems. While not impacting document forensics, they will change the way code based forensics is done.

---

[5] Intel Corporation, *Intel 64 and IA-32 Software Architectures Developer's Manuals*, http://www.intel.com/products/processor/manuals/index.htm.
[6] Advanced Micro Devices, *AMD64 Architecture Tech Docs*, http://www.amd.com/us-en/Processors/DevelopWithAMD/0,,30_2252_875_7044,00.html.
[7] Intel Corporation, *Intel Itanium Architecture Software Developer's Manuals*, http://www.intel.com/design/itanium/manuals/iiasdmanual.htm.