B24 A Forensic Analysis of a Vista 64 Hard Drive

Marc Rogers, PhD, 401 North Grant Street, West Lafayette, IN 47907; Katie Strzempka, BS, 3708 Sweet Valley Lane, Apartment A1, Lafayette, IN 47909; and Eric Katz, BS*, 2099 Malibu Drive, West Lafayette, IN 47906*

After attending this presentation, attendees will have the tools and knowledge necessary to view evidence and other data stored in Microsoft Vista's Shadow Volumes.

This presentation will impact the forensic science community by communicating one potential way of analyzing Vista Shadow copies and viewing a Vista 64-bit hard drive using a virtual machine.

Sixty-four bit processing may be revolutionary for computing, but can create a hassle for computer investigators. This is especially true in departments without the funding to afford a new 64 bit PC. Criminals rarely face the same limitations. Vista tries to help its users by offering a function called Shadow Copy that creates restore points to recover files as they were. Shadow Copy is a wonderful tool, but in some Vista versions, such as Home Premium, the user has no access to the Shadow Copy. For investigators this means that the Shadow Copy is there and files may be present in it, but there is no easy way to access or restore from it. What happens when an investigator must look at a Vista 64 bit machine and restore the Shadow Copy volume and all that is available are 32 bit computers?

The case discussed in this paper addresses these exact issues. Illegal images were known to be on the suspect's hard drive, but were inaccessible. Several methods were utilized to access the files within the shadow volume and the combination of some of these methods proved to be successful and forensically sound.

Vista, Shadow Copy, 64 Bit

** Presenting Author*