B20 Challenges for Digital Forensic Acquisition on Virtualization and Cloud Computing Platforms

Christopher W. Day, BS, Terremark Worldwide, Incorporated, 2 South Biscayne Boulevard, Suite 2800, Miami, FL 33131*

After attending this presentation, attendees will understand the issues involved with acquiring digital evidence from virtualization systems such as VMware and Xen-based systems, as well as so-called “cloud computing” platforms that rely on these technologies to provide organizations and users with highly-scalable and distributed computing capabilities. Attendees will learn how virtualization systems work and the particular challenges they pose to the forensic investigator. In addition attendees will learn about the most common types of cloud computing platforms and how each introduces additional challenges for the investigator above and beyond those presented by virtualization technologies.

This presentation will impact the forensic science community by providing practitioners with a primer for these increasingly common but to many practitioners, still mysterious, technologies and platforms that they will likely be asked to perform forensics acquisitions and investigations on in the near future. This presentation will also present some practical techniques and procedures practitioners can utilize in their work with these systems.

Given the theme of this year’s conference, it seems fitting to examine the technology of virtualization and one of the primary emerging applications of this technology, cloud computing, and the challenges these will present to digital forensic investigators now and in the near future. Various estimates and projections point to an increasing use of cloud computing platforms now and in the near future, some indicating as much as 30% of corporate information processing will take place on some form of cloud platform by 2011. In any case, forensic investigators will need to have an understanding of the technologies involved, the different types of cloud platforms likely to be encountered and what acquisition and investigation challenges they are likely to encounter. Most importantly, investigators must have an established, tested, and accepted methodology for performing evidence acquisitions and investigations on these platforms. One methodology the author is working on in conjunction with the FBI will be presented as an example. **Digital Forensics, Virtualization, Cloud Computing**