B5 A Virtual Architecture for Digital Forensic Tool Validation

K. Philip Craiger, PhD, Chris Marberry, BS, Greg Dorn, BS, and Scott Conrad, BS, National Center for Forensic Science, University of Central Florida, PO Box 162367, Orlando, FL 32816-2367*

After attending this presentation, attendees will have an overview of virtual systems, tool validation, and how the two can be combined to create a powerful testing architecture.

This presentation will impact the forensic community by demonstrating how crucial it is that examiners validate their tools. This talk will provide examiners with the necessary information for them to create a comprehensive architecture for tool validation.

The evolving nature of computer software is fast paced and constantly changing. However, no software is perfect and anomalies can present themselves; bugs can be introduced with new features, or as an unintended consequence of a bug fix. This is, unfortunately, the reality of computer software and as a result of this it is vital for computer forensic examiners to validate the forensic tools they use and to ensure that the tool’s results are accurate. A simple way to validate a tool is to compare a tool’s calculated value against a previously known value, such as a one-way cryptographic hash value of a drive, volume, or even a file. Another is to ”triangulate” results by testing the same function of several different programs against the same medium to see if they produce the same results.

While evaluating digital forensic proficiency tests it was noted several examiner’s test results differed from our “validated answers.” (The validated answers were obtained by triangulating results from several different forensic suites and different versions of these suites). Of interest was determining whether these discrepancies were due to user error, forensic suite error, or some other unanticipated anomaly (e.g., bad hardware).

In order to test these hypotheses a virtual architecture was developed that allows the separation of the influences of different forensic suites, different versions of the suites, and operating systems in order to identify the possible source of these errors. A typical validation methodology would involve dedicating several computers to running different forensic suites (separate computers would be used so as not to contaminate the results by installing and/or running two forensic suites on the same computer). This methodology results in significant duplicated time and effort for every single instance of forensic suite that requires validation. Disk imaging has simplified this process to a degree, by allowing a “baseline” image to be created and kept, but it is still undesirable in terms of required storage space and the amount of time required. Virtualization technologies, however, allow a significant portion of this process to be streamlined, in terms of both required disk space and time spent. One important feature that virtualization allows are snapshots: a complete save of the current state of a running computer, such as any installed programs or an active running program. The ability to freely and quickly move between snapshots is immensely beneficial as this allows a user to move between different versions of software in only a few minutes instead of waiting for whole disk images to be applied back to the hard drive or having to re-install everything from scratch.

The use of virtualization has greatly improved the process of the internal result validation for the competency test. Not only has using this functionality saved time, but this is all derived from a single feature of virtualization technologies. Decreasing the time spent performing the necessary yet time consuming tasks is something that can benefit any laboratory or practitioner. Virtualization also has many other features that are desirable to the forensic community, such as creating self- contained (air-gapped) investigative virtual machines, and completely standardized hardware that does not change even if you move the virtual machine to different physical computers. These and many other features of virtualization should be sufficient reason to investigate the use of these technologies in any digital forensic environment.

Virtual System, Tool Testing, Tool Validation

** Presenting Author*