



13166 Morning Spring Lane, Fairfax, VA 22033
703.786.8529 (Phone)
703.563.9387 (Fax)
info@conceras.com (E-mail)

www.conceras.com

Key Highlights

Computer Forensics



CHALLENGE

Methodologies and tool sets for computer forensics and incident response are in high demand. The computer crime scene may consist of a number of computer systems, services, configurations, and connecting networks.

SOLUTION

Virtualization has been historically resource-intensive to consider for forensics use. Today, however, this has changed. By utilizing technology from major virtualization vendors (e.g., Red Hat, Citrix, and VMWare) Conceras is able to cut down the cost, complexity, and time to perform Forensics Computer Investigations.

BENEFITS

Using virtualization as a forensics tool provides many benefits:

- **Flexibility:** The ability for the examiner to use a myriad of different tools that runs on separate operating systems from his desktop.
- **Availability, Efficiency, and Usability:** Reducing resource demands, allowing proprietary software to run on the suspect system, and providing case organization. Allows for rapid system deployment and automated provisioning, reducing case time readiness from hours to minutes.

Conceras has provided the training and mentoring of virtualization as a forensics tool, providing the most up-to-date technologies and tools for forensics casework and incident response.

Forensics within a virtual environment provides a means of evaluating and doing the casework in the suspects' environment. For example, for network intrusion cases, the examiner is able to rapidly expedite and replicate a network. This plays a vital role when more than one machine is involved, cutting the costs of the hardware. In the case of out-of-date proprietary software, you are able to run it in its native environment.

With virtualization, you are ready for *court testimony*. The examiner can leave hardware behind and only take the needed software. The examiner is now able to convey the findings accurately (with integrity) from a laptop. In addition, the technology allows for the case examiner to experience greater availability, improved productivity, and reduced administrative burden.

Using a Virtualized Laboratory environment, Conceras has valuable, important multi-OS benefits, including: enhanced security and third party application provisioning from Red Hat as well as tool sets from both Windows and Linux. Virtualization has allowed Conceras to fully secure and compartment certified and accredited 'golden' VM libraries and tools sets that can be quickly provisioned for new environments.

What's more, virtualization in a forensics environment has enabled Conceras to rapidly test and simulate third party applications, reverse engineer and contain/isolate Trojan Horses and Viruses, testing methods, and attack techniques (e.g., reconnaissance and covert channels) on multiple OS platforms.

Examiner application and tool set installations have been seamless, providing a secure and known environment that can be repeated with integrity. The virtual machine stability and uptime have been spectacular, allowing for consistent key word searches and large file set analysis, using each resource to its fullest capacity.

With Conceras leadership, training and migrating casework environments to virtualization improves cost, allowing for the most flexible and current tool set environments, and allowing for a complete systems suite and eases the case management and methodologies presented to an examiner.