OSAC RESEARCH NEEDS ASSESSMENT FORM

Title of research need: Digital Forensic Tools to Support Virtual Machines and Virtual File Systems

Keyword(s): vm, virtual machines, hypervisor, virtualization

Submitting subcommittee(s): Digital Evidence **Date Approved:** 12/12/2018

(If SAC review identifies additional subcommittees, add them to the box above.)

Background Information:

1. Description of research need:

In recent years, virtual machines (VM), virtual private servers (VPS), and enterprise virtualization solutions have caused a proliferation of virtualized computers to arrive in our diverse technology environment. A virtual machine could be described as a full computer instance running as a file or series of files on another computer. Virtual machines run as intact computer even emulating the hardware with a software solution.

As technology shifts, the needs for digital forensics tools to support investigate request against new technology shifts as well. Industry support of digital forensics tools for virtual machines and virtual machine file systems is immature with some specific challenges presenting that need assistance.

Virtualization options exists from a variety of manufacturers and large online cloud companies today. Gaps in the available tools and guidance surrounding virtual machines and virtual file systems include:

1. Ingestion and processing of a variety of virtual machine containers. Early research supported consumer and professional level tools but significant gaps exist from enterprise and cloud vendor container solutions.
2. Support for the native READ ONLY mounting of virtual machine file systems from operation systems or digital forensics tools. Limited tools exist to act as an intermediate step between a virtual machine file system and other tools. Little is known about the forensic impact of the intermediate step between evidence source and digital forensic tool.
3. Support for low level reconstruction and file recovery of deleted data from virtual machine file system files systems.

Support for these gaps areas affecting containers, virtual file systems and low level recovery tools will enhance the ability of digital forensic practitioners to address investigative tasks as they are presented.

2. Key bibliographic references relating to this research need:

1. Digital Forensics in a Virtualized Environment, https://fedtechmagazine.com/article/2011/02/digital-forensics-virtualized-environment
2. A research on the investigation method of digital forensics for a VMware Workstation's virtual machine, https://www.sciencedirect.com/science/article/pii/S0895717711001014
3. Forensics Acquisition and Analysis of VMware Virtual Hard Disks, http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1300&context=other
4. Digital Forensic Investigation for Virtual Machines, http://www.academia.edu/3021092/Digital_Forensic_Investigation_for_Virtual_Machines
5. Virtual Forensics: A Discussion of Virtual Machines Related to Forensic Analysis, https://www.forensicfocus.com/downloads/virtual-machines-forensics-analysis.pdf

3a. In what ways would the research results improve current laboratory capabilities?

Existing digital forensics laboratories are receiving data artifacts and complete virtualized computers as evidence in a wide range of investigations. Validated industry tools capable of addressing virtual machine, virtual machine containers and virtual machine file systems will enhance the ability of laboratories to address the new technology platform.

3b. In what ways would the research results improve understanding of the scientific basis for the subcommittee(s)?

A deeper understanding of the technology mechanisms that exist in virtual machines can be enabled through robust tools allowing for the interrogation of these technologies.

3c. In what ways would the research results improve services to the criminal justice system?

Capable validated tools will allow for more robust analysis of virtualized environments. Research and tool support in this technology space will enable faster processing of evidence rather than working each individual data artifact from virtualized environments as a one-off support case needing additional support and attention.

4. Status assessment (I, II, III, or IV): I

	Major gap in current knowledge	Minor gap in current knowledge
No or limited current research is being conducted	I	III
Existing current research is being conducted	II	IV

This research need has been identified by one or more subcommittees of OSAC and is being provided as an informational resource to the community.

Approvals:

Subcommittee

Approval date: 12/12/2018

(Approval is by majority vote of subcommittee. Once approved, forward to SAC.)

SAC

1. Does the SAC agree with the research need? Yes ☒ No □
2. Does the SAC agree with the status assessment? Yes ☒ No □

If no, what is the status assessment of the SAC: □

Approval date: 12/12/2018

(Approval is by majority vote of SAC. Once approved, forward to NIST for posting.)