

**METHOD AND SYSTEM FOR DYNAMICALLY DETECTING, ANALYZING, MONITORING,
INVESTIGATING AND/OR EXECUTING A LIVE TARGET PROGRAM**

ABSTRACT

5

Dynamic accesses to a running process's virtual address space is critical to many security applications, such as malware analysis and live forensics. The present invention provides a virtualization-based system called Onsite AnalySis InfraStructure (OASIS) for dynamic address space analysis. OASIS empowers a full-fledged analysis application to securely run within the live address space of an

10 untrusted process. With the support of OASIS, the analysis application can conduct intensive on-demand accesses to the target program's virtual memory at native speed with ensured mapping consistency. OASIS is transparent to the target program and does not require modification on the analysis tool. OASIS may be easily used for different applications, such as analyzing a target program's live address space; terminating a malware detected, monitoring events of a target program in real time;

15 conducting live forensics and conducting virtual machine (VM) introspection etc.

Figure 3