Virtual Machines (VMs) have become extremely popular in recent years, mainly due to the rise of cloud computing solutions. Since most of the organizational servers are virtualized, VMs are now primary targets for malwares and hackers. Rapid development and application of Linux OS, has put it in risk due to its unique vulnerabilities. As a result, the malware landscape has been changed, and the number of threats towards Linux has been increased significantly.

In order to detect compromised VMs, we use the hypervisor to take snapshots, in a trusted manner, of the running VM. We then extract the volatile memory dump from the snapshot and apply Machine Learning methods in order to analyze and detect the presence of malware on the machine's volatile memory. The VM is not aware of the inspection process; thus, our methodology is trusted.

Linux malware are classified into various kinds of families: Botnets, Ransomware, Rootkits, Trojans, Viruses, Worms and even crypto miners. Linux malware can attack a diverse set of targets, such as Internet routers, printers, surveillance cameras, smart TVs, medical devices, web servers and more. During our research, we have found that most distributed and popular Linux malware are binary executables that appear in ELF format (Executable and Linkable Format). ELF files are compatible with various architectures (ARM, MIPS, Advanced Micro Devices X86-64, Intel 80386) and can be run simultaneously by different CPUs, despite the fact they have a field that indicates which architecture they can be executed on.

In this research, we used the Min-Hash method in order to sign the whole volatile memory dump, taken in a trusted manner, from a suspected VM. We then train a KNN classifier on signatures of benign and compromised VMs, and then use the classifier to classify new unknown VMs.

In order to collect the data, we have developed an automatic snapshotter based on Microsoft's Hyper-V and PowerShell.