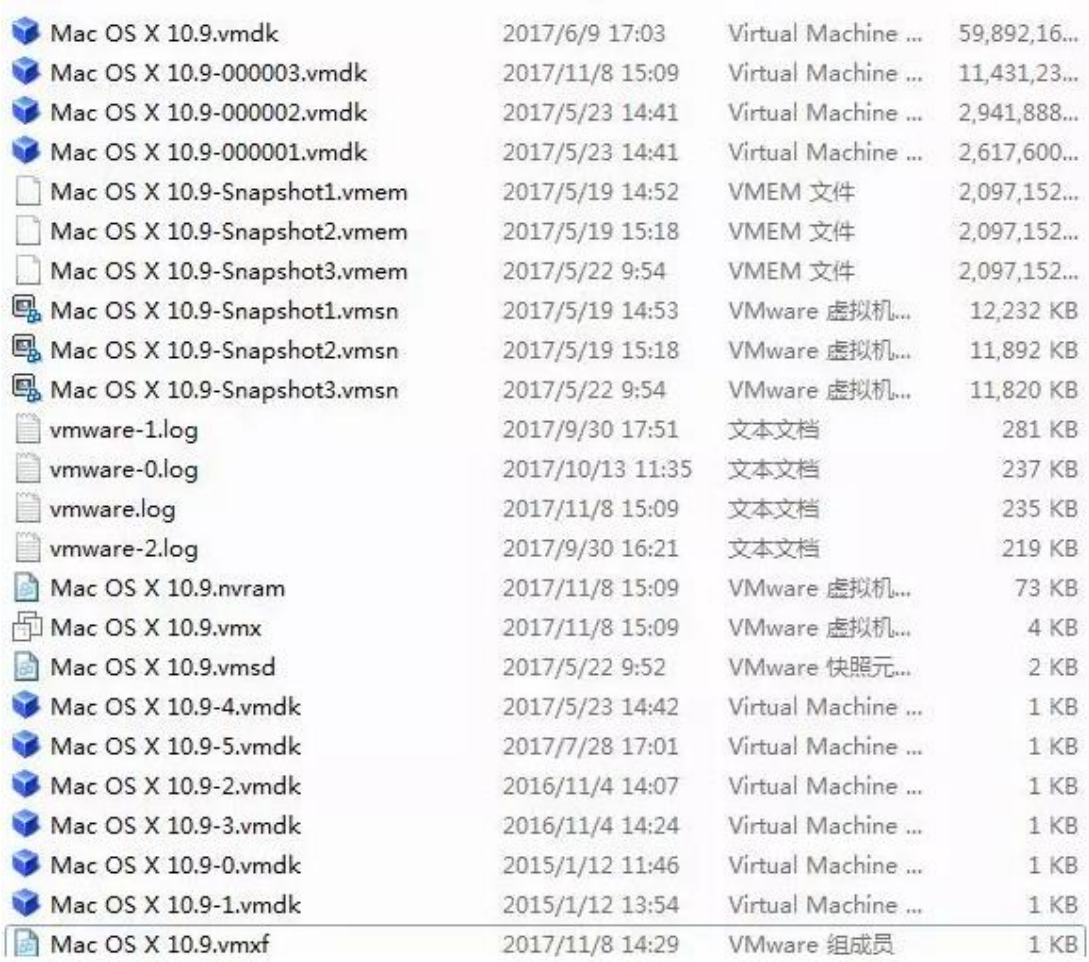
[Case Study] How To Forensically Extract Evidence Data From A Virtual Machine

Editor's notes:

Virtual machine (VM) is a quite popular technology in recent years. Every single VM simulates the performance of all crucial components and runs like a real computer system. All VM data is stored as files in a real hard drive. VMware Workstation is one of the most popular VM tool today. Now let's see how SalvationDATA forensic experts extract evidentiary data from virtual machines based on VMware Workstation.

About Virtual Machines

As explained, all VM data is stored as files in a real hard drive. Therefore, a VM forensic process is actually to extract evidentiary digital data from VM files. So let's first talk about these different types of VM files.



Mac OS X 10.9.vmdk	2017/6/9 17:03	Virtual Machine ...	59,892,16...
Mac OS X 10.9-000003.vmdk	2017/11/8 15:09	Virtual Machine ...	11,431,23...
Mac OS X 10.9-000002.vmdk	2017/5/23 14:41	Virtual Machine ...	2,941,888...
Mac OS X 10.9-000001.vmdk	2017/5/23 14:41	Virtual Machine ...	2,617,600...
Mac OS X 10.9-Snapshot1.vmem	2017/5/19 14:52	VMEM 文件	2,097,152...
Mac OS X 10.9-Snapshot2.vmem	2017/5/19 15:18	VMEM 文件	2,097,152...
Mac OS X 10.9-Snapshot3.vmem	2017/5/22 9:54	VMEM 文件	2,097,152...
Mac OS X 10.9-Snapshot1.vmsn	2017/5/19 14:53	VMware 虚拟机...	12,232 KB
Mac OS X 10.9-Snapshot2.vmsn	2017/5/19 15:18	VMware 虚拟机...	11,892 KB
Mac OS X 10.9-Snapshot3.vmsn	2017/5/22 9:54	VMware 虚拟机...	11,820 KB
vmware-1.log	2017/9/30 17:51	文本文档	281 KB
vmware-0.log	2017/10/13 11:35	文本文档	237 KB
vmware.log	2017/11/8 15:09	文本文档	235 KB
vmware-2.log	2017/9/30 16:21	文本文档	219 KB
Mac OS X 10.9.nvram	2017/11/8 15:09	VMware 虚拟机...	73 KB
Mac OS X 10.9.vmx	2017/11/8 15:09	VMware 虚拟机...	4 KB
Mac OS X 10.9.vmsd	2017/5/22 9:52	VMware 快照元...	2 KB
Mac OS X 10.9-4.vmdk	2017/5/23 14:42	Virtual Machine ...	1 KB
Mac OS X 10.9-5.vmdk	2017/7/28 17:01	Virtual Machine ...	1 KB
Mac OS X 10.9-2.vmdk	2016/11/4 14:07	Virtual Machine ...	1 KB
Mac OS X 10.9-3.vmdk	2016/11/4 14:24	Virtual Machine ...	1 KB
Mac OS X 10.9-0.vmdk	2015/1/12 11:46	Virtual Machine ...	1 KB
Mac OS X 10.9-1.vmdk	2015/1/12 13:54	Virtual Machine ...	1 KB
Mac OS X 10.9.vmxf	2017/11/8 14:29	VMware 组成员	1 KB

*.vmx – Virtual machine configuration file.

*.vmem – Virtual machine memory file
*.vmdk – Virtual machine storage disk file
*.vmss – Virtual machine information file
*.log – Virtual machine log file
*.nvram – Keeps VM's BIOS information
*.vmsn – Virtual machine snapshot file
*.vmxf – Additional configuration file.

***.vmdk** is the most important type of files from the forensic point of view. It simulates the hard disk of a virtual machine, and stores all digital data of this VM. It is the major data source in VM forensics.
***.vmem** is like the RAM of a real computer. It stores all in-process digital data, it could sometimes contain information like user account, password, chat history, web browsing history etc.
***.log** is the log file of a virtual machine, it keeps records of the user's operations like creating files, plugging USB drives. It also records the VM's basic info and status history.

So apparently, almost all the valuable information for a digital forensic investigation is included in these three types of files. The remaining problem is, how to extract valuable digital data from such VM files? Let's continue our topic.

Forensic Acquisition From VMDK Files

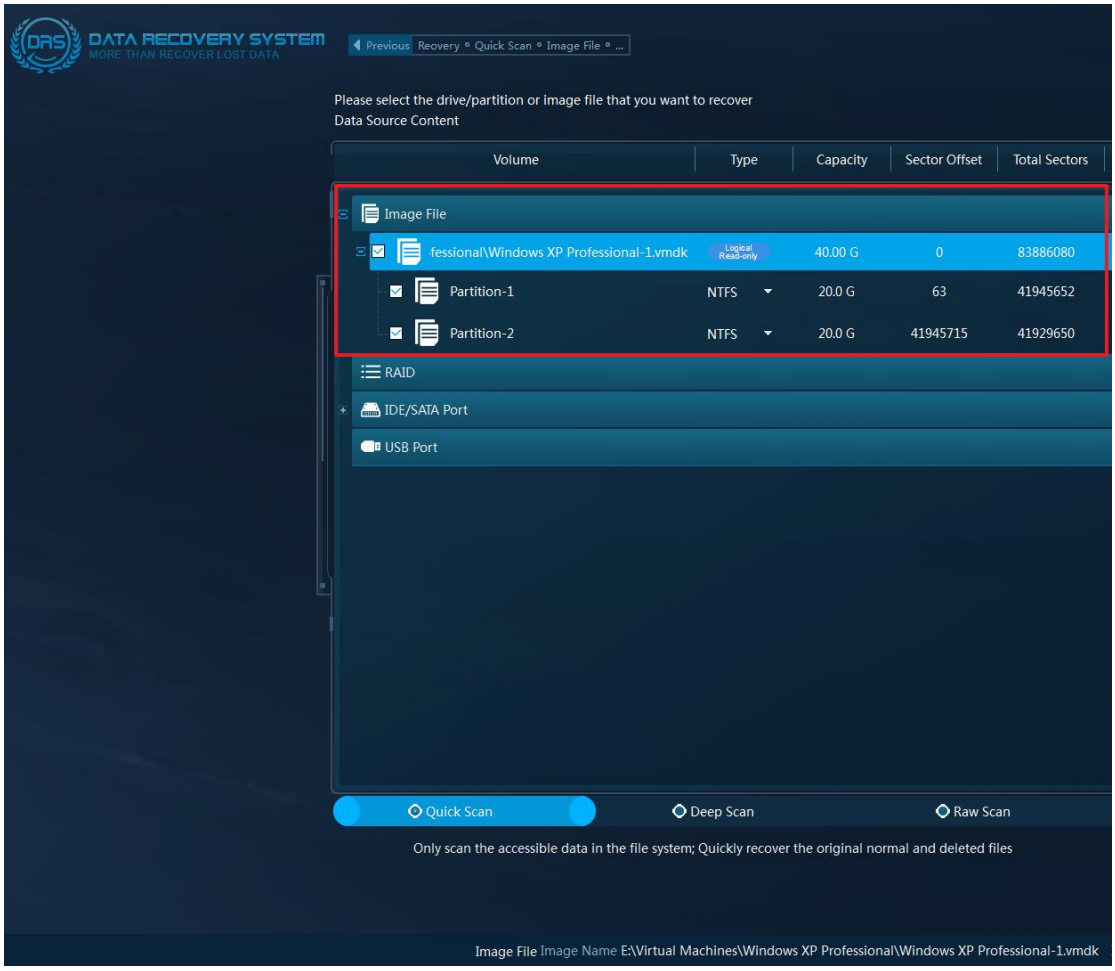
VMDK file is the virtual hard disk file of a virtual machine. It is possible to contain case relevant files, user's trace, application data etc.
There are basically two forensic extraction methods from VMDK files, online and offline.

1. Offline Forensic Extraction

Offline forensic extraction is to directly analyze VMDK files, identify partition information from the VMDK files then extract valuable user data from the virtual hard disk.

It requires professional skills and tools to analyze and identify the file system structure within the VMDK files and extract valid data from it in the end. And it's highly unlikely for digital forensic investigators to possess such skills or tools for the job.

We have perfect solutions for this kind of problem! Our DRS (Data Recovery System) is integrated with virtual machine forensic capabilities. Equipped with professional technology, DRS can help users easily deal with virtual machine forensic cases. Users simply need to load the VMDK files in DRS, and our system will automatically analyze the file system structure, and identify disk partitions. And then users will have free access to the files and user data stored in the virtual machine.



According to our forensic experts' experience, some skilled criminals may also modify the extensions of VM files to hide important data. So it is crucial for investigators to know how to identify VM files even after their extensions are modified. Here we listed all the popular virtualization software and their virtual hard disk file format, and the hexadecimal signature below for your reference.

Item	Software	File Extention	Hexadecimal Signature
1	Hpyer-V	vhd/vhdx	0x636F6E6563746978
2	Windows Virtual PC	vhd	0x636F6E6563746978
3	VMware	vmdk	0x4B444D56
4	Oracle VM VirtualBox	vdi	0x3C3C3C204F7261636C6520564D205669727475616C426F78204469736B20496D6167652 03E3E3E
5	QEMU	qcow/qcow2	0x514649FB
6	Parallels	hdd	0x576974686F7574467265655370616365
7	Docker	vdi	0x3C3C3C204F7261636C6520564D205669727475616C426F78204469736B20496D6167652 03E3E3E

Our DRS supports all the VM formats above.

2. Online Forensic Extraction

Online forensic extraction is to simulate a running virtual machine, use a simulation tool to boot up the operating system stored in the virtual hard disk file. And directly access the files, check for system logs, social chat history and any other valuable data stored in the virtual machine. By simulating a VM, some easy-to-lose information are also possible to be acquired like process data, network data, MAC address etc.

VM simulation forensic solution is also integrated in our new product DF (Digital Forensic System), which is about to be officially released! Please keep an eye on our updates!

Forensic Acquisition From VMEM Files

VMEM file is an accessory file that the VMware Workstation virtual machine generates by default when running. The size of a VMEM file is determined by the virtual physical memory size set in the VM configuration file (.vmx). VMEM contains the memory data managed by the virtual machine operating system.

Through a simple experiment, it was found that when the VMware Workstation virtual machine is started, a VMEM temporary file will be generated. When the “pause” function of the virtual machine is enabled, a normal file with the same name as the virtual machine and the suffix “.vmem” is generated under the path saved by the virtual machine. The memory-related data of all virtual machine operating system that needs to be saved when the virtual machine is suspended are saved in the file. The data is stored and organized in a structure and manner that can be understood by the virtual machine. This feature of VMEM is enabled by default in the virtual machine.

The valuable digital information that can be extracted from a VM memory file includes: the kernel data structure of the operating system, processes, threads, stack data, and other sensitive user information, such as user password, chat history, web browsing information etc.

VM memory file forensic solution is also integrated in our new product DF.

Forensic Acquisition From LOG Files

Many operations of the user in the virtual machine are recorded in the LOG file, such as file creation, USB access, VM running status, basic operating system information, user behavior, etc.

LOG files are recorded in plain text, so they are easy to analyze. Investigators can semantically analyze log files and classify the operations involved in the log file, and the user's behavior can be analyzed and collected according to the timeline.