VANJA KORAĆ,
Mathematical Institute,
Belgrade, Serbia
vanja@mi.sanu.ac.rs

UDC: 902/904:004; 572:004
Original research article
Received: October 12th 2013
Accepted: October 15th 2013

# DIGITAL ARCHAEOLOGY IN A VIRTUAL ENVIRONMENT

## ABSTRACT

*In this paper the most important elements are described which should gain special attention while doing digital forensic analysis in a virtual environment. The most important segments of virtual environments themselves are also explained, as well as ways in which they can be of importance for processes of digital forensic analyses. In the paper, two aspects of virtual environment are discussed. The first aspect regards virtual environment as a digital scene of crime. Services and networks of virtual environment are described within it, places in which potential evidence can be found, ways of securing digital scene of crime and preservation of digital proves discovered. The second aspect regards virtual environment as environment for a digital forensic data analysis.*

**Keywords:** digital archaeology, digital forensic, virtual environment, forensic analysis.

When it comes to digital data archaeology in a virtual environment, it is very important to know the virtual environment, its features and possibilities which the environment can offer in the sense of knowing the advantages and disadvantages which can occur during its usage. It should also be mentioned that there are certain differences in the research access of a digital forensic investigator when physical, i.e. virtual machines are concerned.[1] This paper shall not deal with detailed forensic methodology which regards digital virtual environment, but it aims to sterss only the most important elements which should be regarded while performing digital forensic analysis  in a virtual environment. The most important segments of a virtual environment itself shall be explained and a way in which they could be of importance for the process of digital forensic analysis.

The idea of virtualization was constructed aiming to make managing of a large number of virtual machines simplier, most of all in order to save space, time, money and energy. As a concept, it appeared already in 1960 with the appearance of mainframe computers and it was reborn with personal computers in 1990. In their paper "Formal requirements for virtualizable third generation architectures" (Popek and Goldberg 1974: 412-421), Popek and Goldberg wrote about requirements for architecture which

[1] Virtual machine represents a created environment made with a program package for visualization which posesses a simulated assemblage of hardwares (processor, hard disc, memory, network transmittors and other components) and personal system and application program.

can support a virtual machine describing it as a "effective, isolated duplicate of a real machine". The virtualization itself was described as an idea of virtual machine monitor (VMM).[2]

What is specific for virtual machines is that they use complete hardwares of physical servers. The VM application, the so-called guest, starts its own operation system on a real host machine. In simple words, the VM represents a virtual computer started within a physical computer. For example,a physical server can represent virtual environment with more than twenty virtual machines. Communication between physical server and virtual machines goes over a hypervisor (program supplying virtualization) or over a virtual machine manager via hyper-call. Hypervisor drives system processor, memory and other resources, putting them at disposal to other guest systems on demand (Barrett and Kipper 2010). Hypervisor can supply virtuelization directly on hardware (native VM or Bare-Metal Hypervisor) or on operating system (host VM or Hosted Hypervisor) (Ivaniš 2011). The representatives of virtualization being performed directly on hardware are: VMware ESX[3], Citrix XenServer[4] and Microsoft Hyper-V[5]. The representatives of virtualization being performed on operating systems are: Parallels Desktop[6], Microsoft Virtual Server[7], VMware Server[8] and VMware Workstation[9].

In other words, according to the mentioned concepts, a virtual machine can operate isolated or it can share resources with other virtual machines within the same or other server platform. Due to this specific design and optimized processor operations within realized virtual environment, there is no difference between operating virtual machines and physical machines. There are different types of virtual environment, the most famous ones being *Microsoft Hyper-V*[10], *VMWare Vsphere ESXi*[11], *QEMU*[12], *Citrix XenServer*[13]. This work is focused on two angles of digital forensic in a virtual environment on two angles of digital forensic in a virtual environment. The first one regards virtual environment as a digital crime scene, while the second one regards virtual environment as environment for a digital forensic analysis.

## VIRTUAL ENVIRONMENT AS A DIGITAL CRIME SCENE

As every environment, virtual environment can also be compromised in many ways, possibly resulting in compromising virtual machines themselves, as well as operating systems and files positioned within particular environments.

To a digital forensic investigator, to whom a digital crime scene is the actual virtual environment consisting of virtual machines, it is very important to be well-informed and to know how to work in a virtual environment. Access to investigation is based upon locating and accessing physical server which drives virtual machines. It is of great importance that digital forensics sceintist has "live" access to digital machine which is regarded as digital crime scene. In such a way, valuable data and information can be gathered as potential digital evidence during operation of a physical server (Milosavljević and Grubor 2010). A fact should be pointed out that suspect has great possibilities to manipulate with evidence in such a environment, thus making acquiring of digital evidence rather complicated.

[2] Virtual machine monitor represents a part of a program with three features. The first one is that VMM offers a environment for programs which is identical to environment on a physical machine. Second, programs being started within in such a virtual environment have a very small reduction of performances when it comes to speed compared to physical machine and thirdly, the VMM fully controls system resources.

[3] Available at http://www.vmware.com/products/esxi-and-esx/overview

[4] Available at http://www.citrix.com/products/xenserver/overview.html

[5] Available at http://www.microsoft.com/en-us/server-cloud/hyper-v-server/default.aspx

[6] Available at http://www.parallels.com/

[7]A vailable at http://www.microsoft.com/windowsserversystem/virtualserver/

[8] Available at http://www.vmware.com/products/vcenter-server/

[9] Available at http://www.vmware.com/products/workstation/

[10] Microsoft Hyper-V, http://www.microsoft.com/en-us/server-cloud/hyper-v-server/ , Accessed 09.02.2012.

[11] *VMWare Vsphere ESXi,* http://www.vmware.com/products/vsphere-hypervisor/overview.html , Acessed 09.02.2012.

[12] *QEMU*, http://wiki.qemu.org/Main_Page , Acessed 09.02.2012

[13] Citrix Xenserver http://www.citrix.com/English/ps2/products/product.asp?contentID=683148 , Acessed 09.02.2012.

Principles regarding digital computer forensics and which are applicable during acquiring, analyzing and presenting digital proves can also be applied at virtual machines in a virtual environment, but with certain differences, which shall be pointed out later on in this paper. It is important to stress that it is necesarry to use only tested and reliable forensic tools (ex. *Access data FTK*, *Encase, X-Way Forensic*) which support working in a virtual environment and possess compatibility with new operating systems.

If investigation dealing with illegal activities focuses on a virtual environment and if it is conducted according to adequate methodologies, using reliable forensic tools and aiming to find relevant digital proves, investigation shall be successfull. Contrary to that, it can end up unexpectedly. Digital investigation in a virtual environment can be public (official) and corporative, depending on the type of incident. Investigation begins with a physical access to a physical crime scene, where physical evidence is gathered. Further on, digital crime scene is accessed (virtual environment consisting of virtual machines) and it lasts until digital forensic investigator is not finished with investigating digital data ready to be included in a report, i.e. for presenting reconstructed crime or incident. All of the evidence found must be documented, secured, relevant, unchanged and acceptable in court, while the whole investigation (when dealing with official investigation) must be transparent for trial in court (Milosavljević and Grubor 2010).

It should be emphasized that virtual environment is a environment offering a row of positive possibilities through its very useful operations, but it is exactly them that can be abused. For example, operations which can be abused are migrations of virtual machines, manipulations with images of virtual machines, live migration (manipulations connected to „live“ migrations of virtual machines). Some of the abuses can result in controling or abusing virtual machines by a vicious person.

Malicious activities can be detected, since all of the activities are noted on server, i.e. host and it is very important that from the vey beginning, digital forensic investigator approaches investigation and acquiring evidence according to strictly defined procedures, since otherwise loss or dissapearance of important digital data can occur. Forensics in a virtual environment shows more gathered evidence compared to classical digital forensic, since digital forensic investigator must gather information about data packages and about communication between abuser and user upon whom the illegal action was performed. During investigation of virtual environment, everything happens within virtual spaces put on physical (server) machines, being connected to Internet, so actually virtualy they could be anywhere (one of such examples is Cloud computing[14]). In order to search digital places of crime, a digital forensic investigator has to enter digital virtual environment, which is complex and can represent a great problem to a forensic investigator if no preparations were performed. Such preparations include following and filming activities of suspect, as well as getting acquainted with operating systems themselves which are placed inside a virtual environment. Contrary to classical digital forensic, in which physical computer is accessed physically, when one is dealing with forensics in virtual environment, a forensic investigator would not have simple access to a physical machine on which virtual environment was designed. Exactly this is specific about digital forensics in virtual environment. One of the aims of a digital forensic investigator is locating a central spot with virtual computers (not just the location of a virtual machine). This place contains great quantity of useful information which can be used as potential digital proves whitnessing illegal activity. It is also very important that digital forensic investigator is well-acquainted to all of the concepts of virtualization.

[14] The way how Cloud computing is functioning as a type of virtual environment: user gains access to a computer placed in far north. This system enables its user safe and cosy work. Great advantage of such a system is that its user does not have to know where his/her computer is situated, while data are always at his/her disposal. The user also does have to worry about computer maintaining and depending on what he/she paid for, the user can have great quantity of space. Making connection with a virtual machine is quite simple. There are certain program clients who are in charge for making connections with servers connected to public networks. After successfull authentification, the user accesses his/her virtual machine.

## SERVICES AND ELEMENTS OF VIRTUAL ENVIRONMENT

Further on, a vivid description of important services making virtual environment shall be given. Getting acquainted with them can be of use to digital forensic investigators[15] (Tulloch 2010):

**-Virtual machine management service** (VMMS) – drives, i.e. determines which operations can be performed in some of the states of virtual machines. The VMMS drives the following states of virtual machines: starting, active state, inactive state, state of snapshot making, state of snapshot application, deleting state snapshots, disc connecting. According to these states, the VMMS drives operations on virtual machines, i.e. children. It does not drive operations like Pause, Recording, Switch-off. This is done with the Virtual machine worker proces (VMWP) process, which is being created when virtual machines are started;

**- Virtual machine worker process** – is created on a virtual machine and it appears as executive file vmwp.exe participating in a great number of interactions between opeartive system on host and virtual machines (children). These interactions include creating virtual machines and their configutrations, driving pauses and resuming virtual machines, saving and restoring virtual machines and snapshooting states of virtual machines. It also drives memory, in- and out ports on computer's motherboard and driving IRQs. Existence of such a file (vmwp.exe) represents a proof that there are virtual machines of host.

**-virtual devices** – represent program modules (driving programs) which enable configuration of devices and controlling partitions of virtul machines. They are steered through virtual motherboard ( VMB) which is given to each virtual machine;

**-driver VMBus** – supplies optimized communication between host and child, at the same time representing a part of Hyper-V service;

**- Virtual Infrastructure Driver** – represents kernel component responsible for regime of virtualization on host, making it possible to drive virtual processor and memory;

**- The Windows Hypervisor Interface Library** – represents kernel component as dynamic link library (DLL). It enables drives of operating systems to access the processor. As part of operating system, it is placed on host. DLL file makes drivers of operating systems possible to access the processor.

The services named above may not have direct influence on investigation, but it is important to know important processes and their possibilities in hardware communication between processor and hypervisor, actually host and child.

The presence of the files mentioned in shape of virtual devices and drives can indicate existence of virtual machines to a digital forensic investigator.

The Fairbanks Alaska University[16] performs research in the field of volatile data by using virtual introspection (VI). Virtual introspection as a new field of research and development in digital forensics, represents an observation process of state of virtual machine either through Virtual Machine monitor (VMM) or from some other virtual machine which is no subejct to forensic research. They developed a set of tools for Xen environment called VIX tools (Hay and Nance 2008), aiming to reduce the risk of changing evidence while they are examined. This tool also makes "live" analysis on Xen virutal machine possible.[17] Basic access of these tools is to pause suspected virtual machine, then gather necessary data by using the „read only" operation and afterwards end the pause. One of the useful things possible with this tool is memory mapping of the suspected machine and ascribing of the mapped segment to the virtual forensic machine.

## NETWORKS IN VIRTUAL ENVIRONMENT

When it comes to networks in virtual environment, there are three different kinds of virtual networks (Tulloch 2010) (Garrison 2010):

**Internal virtual networks** – this type of network does not rely on physical network adapter, but the physical network adapter is being used.

[15] Example is connected to making a Hyper V environment, on whse host Windows server 2008 R2 is installed.

[16] http://www.uaf.edu/, 03.01.2012.

[17] http://assert.uaf.edu/papers/forensicsVMI_SIGOPS08.pdf, 03.01.2012.

Internal virtual network is used as intranet and it is used for connecting virtual machines on intranet. There is also an option of their connection to host, potentially opening a possibility of children abuse if it comes to compromising the host computer. Malicious attack would aim at the program area with the goal to abuse virtual machines or stop them;

**External virtual networks** – this type of network relies on physical network adapter and on virtual network adapter, thus making communication of physical and virtual machines possible, in the Intranet as well as towards the Internet. A potential possibility of abuse of host is opened from the outside, but also from virtual machnes themselves, since communication between host and child is opened. Malicious attack would also aim the program area in order to abuse virtual machines or turn them off**;**

**Private virtual networks** – this type of network does not rely on physical network adapter (similar to Internal virtual network) and no communication with members outside private virtual network is allowed. Host also does not have direct communication with this network, making malicious attacks on this type of network impossible. There is a theoretical possibility of attack, but it is limited to the hardware host part.

Certain tools are used in order to find out host's name, data about network cards (physical and virtual) and their configurations (DHCP parameters, MAC addresses). All these pieces of information about network adapters of virtual machines directly on host are of great importance to a digital forensic investigator in order to get acquainted to the architecture of virtual environment.

## PROOF OF THE EXISTENCE OF HARDWARE WHICH SUPPORTS VIRTUALIZATION

Modern concepts of virtualization (for example performing cloud computing) can be made only when specially adapted hardware compatible processors are being used, supported to work with hypervisor. The processors most commonly used for making virtual environments are Intel VT[18] and AMD-V[19]. Why is it important for digital forensic investigator to find out the location of physical server on which there is virtual machine being the subject of investigation? The reason is that that is exactly the way (physical access to host) to prove the existence of such processor types which support hardware virtualization, also proving a possibility of existence of machines which could have been (ab)used for illegal actions, which are on host itself or physical machine. For example, *Properties* of an operating system can offer basic and sufficient information about processor type. Digital forensic investigator can also find data about virtualization in BIOS (under options for adjusting virtualization), which indirectly can influence investigation and acquiring of evidence. The presence of application being driven by virtual machines (virtual machine manager) indicates the existence of virtual machines, but also a place from which virtual machines are being operated, being whitnessed also by log files of the regarded environment.

To a digital forensic investigator, console tools which can operate virtual machines can be of great use in cases when monitoring is needed and getting acquanited live to virtual machines. In such a way, important data can be exposed: names of virtual machines, condition of virtual machines (active or not), in which regime of work they are in, resource usage by virtual machines and data about time and time-zones. Such are for example „last logon" files or „configuration log" files, their operations depending on programs which make virtual environment possible. Profiles or roaming profile files which can be of interest to a digital forensic investigator include NTUSER.dat (specific system registry file) and other application data. In some cases, it can occur that TEMP directory is not copied together with profile and it is necessary to pay special attention to it during forensic investigation of gathered virtual hard disc.

## TIME PROOVING

Digital forensic investigator has to pay special attention to time and time zones of the examined virtual machine, of the host itself (if physi-

[18] Here the list of Intel processors which support virtualization: http://ark.intel.com/VTList.aspx, 10.02.2012

[19] AMD platform for virtualization: http://sites.amd.com/uk/business/it-solutions/virtualization/Pages/amd-v.aspx, 10.02.2012

cal access is possible) and of the environment in which forensic investigation is takin place. It must be ascertained if times match and whether there are differences.[20]

## SECURING DIGITAL CRIME SCENES IN VIRTUAL ENVIRONMENT

In order to save all potential digital evidence, in classical digital forensic as well as in forensics of a virtual environment, before live investigation takes place, it is very important to disable network communications of suspected host. It is done by pulling out the network cable from the physical host machine. If host is performing wireless communication to Intranet or Internet, wiresless machine to switch it is connected has to be switched off.

## ACESSING RAM

In order to perform a virtual environment with sixteen virtual machines working under Windows 7 operating system for example, at least 16 Gb RAM would be necessary. As minimum RAM memory, Windows 7 requires 1GB RAM. For an operating system on host, minimum 512gb to 4 GB Ram memory would be necessary, depending on the OS responsible for virtualization. Total RAM quantity in such a case is 20gb RAM (16 Gb RAM memory per child and 4 Gb for host). This information is important, since according to it, digital forensic investigator would get to know the total amount of RAM memory which is placed on a physical machine and how much has being by virtual machines.

Gaining information from RAM memory is possible from a part of RAM memory on host which is determined for virtual machine under investigation. It is performed by using live forensic (under the condition that computer was previously not switched off, because then the content of RAM would be deleted) and with application of forensic tools (su Encase[21], *FTK Imager*[22], *X-Way Forensic*[23]) for accessing digital data. When snapshot of a virtual machine is being performed (for example with VMware[24] environment), there is an option to choose whether the snapshot would also switch on the memory. If the investigated virtual machine had this option switchen on while snapshoting, the „vmem“ files would be present in snapshooting. A tool created by Chris Betz which can investigate these vmem files is named Memparser[25] (Beek 2010).

## VIRTUALNI HARD DISC

Every virtual machine writes its data on a virtual hard disc. For a digital forensic investigator, its location, extensions, size and configuration are of great importance, since virtual hard disc can contain potential digital evidence.

Every child on host must also have a place to write its data. Virtual hard discs can be placed on a SAN[26] (Storage Area Network) or NAS[27] (Network Attached Storage) devices or on local hard discs (Grubor, Njeguš i Ivaniš 2011). Information about size matters because of copying images of a virtual hard disc on its forensic medium, from which further investigation shall take place. This is important if one is dealing with virtual hard discs of great capacity, since they can pro-

[20] Documenting time form a virtual machine or from the host can be recorded with a camera, while time of the environment can be recorded on an official TV station or radio.

[21] https://www.encase.com/products/Pages/encase-forensic/overview.aspx

[22] http://www.accessdata.com/products/digital-forensics/ftk

[23] http://www.x-ways.net/forensics/

[24] http://www.vmware.com/

[25] Acessible at http://sourceforge.net/projects/memparser

[26] SAN represents a device for storing data and it functions at the level of data blocks, intended for enterprise solutions. Contrary to NAS devices, the SAN devices allow sharing of storage space into parts which can be ascribed to bigger number of servers with direct attached storage, making great speed of data transmissioning possible. Connection is made through fibre channel. It consists of a great number of high-speed SAS discs (15K rpm). Solid state discs (SSD) can also be used if performanse and saving enery are priorities. There are also vendors offering combined systems, so that data can also be accessible via block access through fibre channel or they can be accessed on the level of databases with expected speed increased up to 100GBps in the decade to come.

[27] NAS represents a device for data storage functioning on database level. It connects with computers via local network, mostly via TCP/IP over internet. It consists of a great number of discs adjusted to operate using SAS SCSI or SATA discs. NAS is most commonly used as a file server supporting file systems and protocoles, for windows networking CIFS, HTTP, linux networking SAMBA, NFS.

longue investigation. For a digital forensic investigator it is important to find out as much information as possible about the number of partitions and to make a snapshot only for those partitions suspected to contain digital prooves. This information can be found in configuration files of the virtual machine itself. Certain extension[28] can indicate the state of virtual machine itself, if it is complete, is it a snapshot or change of state. Such changes can testify installing certain programs and their usage. Regarding classical research of a digital crime scene which deals with physical digital environment exclusively, information regarding condition of a virtual machine can only be placed in a virtual environment. There are also files which bear configuration information of a virtual machine under investigation. It is important to tell discs of defined size from dynamic virtual discs (dynamc capacity enlargement depending on needs). It is also important to stress that some programs for virtualization can drive virtaul hard discs in different ways. This is of importance for digital forensic investigator, since after certain operations on virtual hard discs, their structure can be very much changed. There are operations which can reduce virtual machine size by removing the unused space (on host such a space would be marked with zeros). Further on, there are operations which can convert dynamic virtual discs into the fixed ones and vice versa or to enlarge fixed virtual discs. They can also merge virtual hard discs and merge physical hard disc into a new virtual hard disc.

Since the field of virtualization grows bigger, Microsoft began to integrate virtualization techniques into its operating systems, such as Microsoft Windows 7. In the Configuration menu which regards disk management, it is possible to mount virtual hard disc (VHD) into read-only mode. Another useful operation is bootin the computer from a virtual hard disc (it regards only Windows vhd files). What was called Complete PC backup in Windows Vista, in Windows 7 it is called System image backup and it is saved in vhd formate (Beek 2010). From the perspective of a digital forensic investigator it is very useful, since such an image (which can contain great amount of useful information) can be connected to a forensic computer in read-only mode.

## SNAPSHOTS OF VIRTUAL MACHINES

Snapshots of virtual machines have a wide field of usage. They can be used for finding changes on operating system, returning virtual machine into the previous working menu in case installing of a program (applicative or system) influenced change of work of an operating system. For a digital forensic investigator they are of great importance, since by getting to know the moment of illegal action, over snapshooting (reversed) on a forensic machine and with applying forensic tools, a simple overview of a virtual machine for a forensic relevant moment would be performed. according to that, it is possible to gain data from RAM memory or virtual hard disc about action of an illegal virtual machine. Snaphot comparation of the investigated virtual machine aiming to note changes, change of files or identification of hidden files can also be of great interest. The tool which enables tracing of changes on Vmware virtual machines is written by Zairon[29] and it is called Compare Vmware snapshots (Beek 2010).

## FORENSIC COPIES OF VIRTUAL MACHINES

When digital forensic is concerned, physical machines made two copies of physical hard disc by using appropriate forensic tools. The first copy, which is numerated, is used to calculate the hash value of MD5 or SHA algorythm, aiming to proove that it was not changed, i.e. integrity of hard disc. This copy represents a proof and it is kept until it is necessary in court to indicate that there were no changes in bits. The second copy is used for performing forensic anaylses on a forensic computer. Recently, when virtual machines came to use, the need arose to make a third hard disc copy for suspected machines, representing a special feature. On such copies there are virtual hard discs and their snapshots, together with all folders and files which describe a virtual machine

[28] Extensions of these files are different depending on programs which perform virtual environment.

[29] Accessed at http://zairon.wordpress.com/2007/09/19/tool-compare-vmware-snapshots/

under investigation. The third copy is used for investigation on a forensic virtual machine in a similar environment, referred to further on in the paper. Making snapshots of an operating system is an extremely complex process, since integrity of hard disc must remain undamaged. Bootable disc is usually used in such cases, containing all the necessary tools, but external forensic device can be used as well for storing hard disc snaphots of a suspected machine. File analysis from hard disc snapshots should be performed on a forensic computer. Just like with every forensic analysis, documentation has to be kept about gathered prooves. There are even program tools for such a purpose.

## MIGRATION OF A VIRTUAL MACHINE

One important feature of a virtual environment (as its component in most cases) is an operation of transferring i.e. migration of virtual machines. It was already mentioned that such an operation is of great advantage for administrator of virtual environment (migrating a virtual machine from one place to the other inside the same physical server or to some other physical server). On the other hand, it can make it possible for a supect to hide evidence of illegal action.

It should be pointed out that when a virtual machine migrates, only information containing data about configuration used for multiplying virtual machines is being transferred. Still, if it comes to export of a virtual machine, all of the data shall be transferred, including snapshots (if there were any). These operations can influence digital forensic investigator to make wrong conclusions if no preparations were performed, i.e. the following of virtual environment.

The goal of a digital forensic investigator for virtual environment is to create the sequence of illegal actions, gathered with digital and physical evidence. The investigator needs to collect data of network adapters, network configuration of the virtual environment itself, domain, data regarding virtual hard discs, data from system snapshoting, data about periphere virtual devices, data from RAM memory etc.

Forensics shall develop towards virtual environment, since some of the classical tools for digital forensic cannon be fully used in a virtual environment either because of their compatibility with later operating systems or because the use of tools is inadequate (dynamic and capacity of hardware are in such a state that complete investigation would become very slow). This is another feature of virtual environment, so it is recommended to perform live forensic investigation of virtual environment whenever possible, making snapshots of partitions or disc parts which might contain potential evidences. It should be pointed out that when investigation is aiming to a virtual environment in which one machine is being suspected for an illegal action, it is also necessary to investigate other virtual machines on forensic working station. All of this indicates certain special features in collecting data and contrary to a classical digital forensic of physical machines.

## VIRTUAL ENVIRONMENT AS ENVIRONMENT FOR DIGITAL FORENSIC ANALYSIS

The concept of virtualization and the specifics of digital forensic of a virtual environment were explained at the beginning of this paper, while this part of the paper shall be dedicated to virtual environment representing environment for performing digital archaeology while investigating digital crime scene. General concept of virtual environment and its limitations in applying digital forensic analysis shall be analyzed. The idea of this approach is to apply the process of digital forensic analysis at the same time under conventional and virtual environment independently, which can benefit in reducing duration of digital forensic analysis. The focus of this chapter is a phase of digital investigation, actually digital forensic analysis. The process of digital forensic analysis can include three key phases, as shown by Kruse and Heiser in their model: acquiring evidence, establishing authenticity and analysis (Kruse and Heiser 2010).

Christopher Brown, founder of one of the leading companies dealing with digital forensic (CTO of Technology Pathways LLC[30]) stresses that in the acquiring phase, digital forensic investigator should record and note as many vol-

[30] http://www.techpathways.com/Desktop Default.aspx, 31.02.2012

atile data as possible from live system, further switch off the computer and finally create bit stream copy[31] of all of the data storage devices, actually hard discs. Most of the authors claim that making forensic copies i.e. images of a suspected hard disc is relized with programs based on "dd tools"[32] and that the gained forensic copy is kept in dd format or some format based on dd (Nelson, Phillips, Enfinger, and Steuart, 2006)(Rude 2003)(Bunting and Wei 2006). The gained forensic copy i.e. image represents an identical copy of the original disc. It should be mentioned the old rule, according to which image needs to be identical with the original disc, is not applied lately. There is a great number of apropriate image formates of the original hard disc used most commonly, but which are not identical to the original hard disc, since they can contain additional metadata. like investigators' names, notes or hash values. An example for such forensic adequate format is the popular Advanced forensic format - AFF (Garfinkel 2005) (Garfinkel, Malan, Dubec, Stevens and Pham 2006) developed by Dr. Simson Garfinkel and the Basis Technology company.[33] Since this format also includes segmentation of the original snapshot with adding chapetrs, digital forensic investigator bases its finding on investigating the image which is in some way altered, actually not identical with the original.

On the other hand, the dd tools creates a snapshot identical to the original and can be created at the same or at a hard disc of greater capacity and can be driven on another computer system. A problem could occur here regarding re-establishing original environment because of different hardware components' computer combinations. For example, if a snapshot of a researched computer is driven on a computer with different hardware components from the first one, operating system shall try to recognize the differences and add driver programs for the missing hardware components in order to run the operating system successfully. Still in some cases, system would not be able to run successfully or there would be systems and programs which would not be able to run. The mentioned problem also relates to application in a virtual environment, since virtual machines can only simulate basic hardware components and they are not intended to support a great number of hardware devices. That also means that a forensic snapshhot obtained with a „dd tool" cannot be run without adding files with certain parametres needed to run the snapshot in a new environment. There are differnt tools that can solve this roblem. Comercial tools include Encase's Physical Disk Emulator[34] and Technology Pathways'es Prodiscover.[35] Among free tools there are Live View[36] and some free tools by Technology Pathways.

In literature it is still discussed whether data obtained from a virtual environment can be relevant. The reasons are exactly the changes which have to be applied upon the snapshot of the original hard disc (original environment) in order to make running of the virtual environment possible. If it is known that snapshot was much changed, it can imediately be sustained in court, although an IT expert could claim that changes have no influence on presented evidence. Some authors consider that virtual environment in the role of a digital forensic tool has no perspective regarding its application in forensic analysis (Fogie 2004). Still, if virtual environment in the role of digital forensic tool is applied in a combination with classical digital forensic approach, data analysis can be radically reduced and better results can be obtained. One of the models suggesting this approach is the Ben and Huebner model (Bem and Huebner 2007 : 1-13). This model type includes two levels of digital forensic staff. The first one includes digital forensic investigators - professionals (DFIP), fully trained and with great experience, strictly acting according to methods of rules and proceduresof digital forensic investigation. The second level includes digital forensic investigators – computer technicians (DFIRT) with less forensic knowledge

[31] These bit-stream copies can be made as bit-for-bit copies or bit-for-bit plus copies. Both ways are widely accepted, while the difference is that bit copy plus implements certain metadata data which aim to tag proof-files in order to preserve the responsibility chain (Nelson, Phillips, Enfinger, and Steuart, 2006) (Bunting and Wei 2006) (Scott 2004).

[32]http://en.wikipedia.org/wiki/Dd_%28Unix%29, accessed 31.02.2012

[33] http://www.basistech.com/e-discovery/ , 13.02.2012

[34] http://www.pc-ware.com/medialibrary/central_files/de/hersteller/software/guidance_software/files/guidance_07_06_19_encase_forensic_prosuite.pdf, 16.02.2012

[35] http://www.techpathways.com/prodiscoverdft.htm, 16.02.2012

[36] http://liveview.sourceforge.net/, 16.02.2012

and experience and do not strictly need to stick to the rules and procedures, since they have no direct influence on the investigatin process. Their role is to search the copies of digital evidence in order to find as many data possible of interest for the investigation and to report everything they find to digital investigators – professionals who, by using relevant forensic techniques approve the finds or search the data further if needed.

The methodology used a show-case would go as follows: computer technicians run a copy of gathered snapshots in a virtual environment (as a virtual machine), treating it as a normal system and search „live" all of the details relevant for the investigation. Although methodology used by computer technicians influences the integrity of gathered snapshots of the original system, it does not influence the investigation. The reason is that computer technician works only with one of the copies of digital snapshots of the suspected hard disc. That means that computer technicians possess good technical, but less forensic knowledge can apply computer forensic techniques also in phases without endangering digital evidence.

It is logical that to one copy, the hashing function aiming to keep the integrity is being applied  and it should be kept safe, while the other copy remains with digital investigators – professionals intact and forensically valid.

According to the data obtained by computer technicians, the DFIP can confirm all of the results using adequate forensic tools, strictly sticking to adequate forensic methodology, techniques and procedures.

## CLOSING CONSIDERATIONS

Virtual environment, just like any other environment, can be compromited in different ways, which can result in compromizing virtual machines, as well as operating systems and files placed within such a environment. This is why digital archaeology becomes necessary when compromizing computer systems. In this paper, two aspects of virtual environments of were considered. The first aspect regards virtual environment as a digital crime scene. Services and nets of digital environment were described in it, places in which potential evidences can be found, ways of securing digital crime scenes and preserving the discovered digital prooves. The importance of digital forensic investigator's live access to a digital machine regarded as digital crime scene was pointed out. In such a way, it is possible to gather valuable data and information which can represent potential digital evidence. Manipulation possibility in such a environment by a suspect is huge, making the process of collecting digital evidence rather complex. All of the principles regarding digital forensic of a computer which can be applied during collecting, documenting, analysing, preserving integrity and presentation of evidence are applicable also for virtual machines in a digital environment, with certain differences which were pointed out in this paper.

The second aspect regards virtual environment as a environment for digital forensic data analysis. A general concept of virtual environment with described limitations in applying digital forensic analysis was shown. Such a concept shows that process of digital forensic analysis is performed simultaneously in a conventional and virtual environment independently, which can benefit in reducing the duration of digital forensic analysis. This actually means that with such a forensic access, combination of classical and virtual concept, which is being performed as a co-operation of teams on different expertise levels and with applying different tools, can lead to reducing time of a digital forensic analysis. Time is saved and also pressure upon digital investigators – professionals, which is very important since there is a lack of forensic professionals.

## BIBLIOGRAPHY

**Popek, G. J. and Goldberg, R. P., 1974**
*Formal requirements for virtualizable third generation architectures*, Communications of the ACM 17 (7): 412–421.

**Barrett, D. and Kipper, G., 2010**
*Virtualization and Forensics – A digital forensic Investigator's guide to Virtual Environments*, Elsevier Inc., USA.

**Ivaniš, N., 2011**
*Digitalna forenzička istraga u virtuelnom okruženju*, master rad, Univerzitet Singidunum

**Tulloch, M., 2010**
*Understanding Microsoft Virtualization Solutions from desktop to the datacentar, second edition,* Microsoft Press A Division of Microsoft Corporation One Microsoft Way Redmond.

**Hay, B. and Nance, K., 2008**
*Forensics Examination of Volatile System Data Using Virtual Introspection***,** SIGOPS Operating Systems Review, ACM Special Interest Group on Operating Systems, Volume 42 Issue 3, ACM.

**Beek, C., 2010**
*Virtual Forensics*, TenICT proffesionals, http://securitybananas.com/wp-content/uploads/2010/04/Virtual-Forensics_BlackHatEurope2010_CB.pdf.

**Kruse, G. W. and Heiser, G. J., 2010**
*Computer Forensics Incident response essentials,* 14th printing, New York: Addison Wesley, March.

**Nelson, B., Phillips, A., Enfinger, F., and Steuart, C., 2006**
*Guide to Computer Forensics and Investigations, Second Edition*, Thomson Course Technology, Boston.

**Rude, T., 2003**
*DD and Computer Forensics*, Retrieved October 23.

**Bunting, S., and Wei, W., 2006**
*En Case Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide,* Indianapolis, in: Wiley Publishing.

**Scott, M., 2004**
*Independent Review of Common Forensics Imaging Tools*, Memphis Technology Group, SANS GIAC Paper Submission.

**Garfinkel, S., 2005**
*The Advanced Forensic Format 1.0*. 2005, http://stuff.mit.edu/afs/sipb/user/simsong/afflib/affdoc.doc.

**Garfinkel, S., Malan, D., Dubec, K., Stevens, C. and Pham, C., 2006**
*Disk imaging with the advanced forensics format, library and tools*, The second Annual IFIP WG 11.9 International Conference on Digital Forensics, National Center for Forensic Science , Orlando, Florida, USA, January 20-February 1.

**Fogie, S., 2004**
*VOOM vs The Virus (CIH)*, http://voomtech.com/downloads/Shadow%20Eval%20-%20Fogie.pdf.

**Bem, D. and Huebner, E., 2007**
*Computer Forensic Analysis in a Virtual Environment*, International Journal of Digital Evidence Fall 2007, Volume 6, Issue 2: 1-13.

**Garrison, C., 2010**
*Digital Forensics for Network, Internet, and Cloud Computing a forensic evidence guide for moving target and data*, Elsevier Inc., Burlington, MA 01803, USA.

**Milosavljević, M., Grubor, G., 2010**
*Istraga kompjuterskog kriminala – metodološko tehnološke osnove*, Univerzitet Singidunum, Beograd.

**Grubor, G., Njeguš, A. i Ivaniš, N., 2011**
Glavni faktori uticaja virtuelizacije tipa I na forenzičku istragu”, Naučni skup sa međunarodnim učešćem Sinergija.

## REZIME

## DIGITALNA ARHEOLOGIJA U VIRTUELNOM OKRUŽENJU

**Ključne reči**: digitalna arheologija, digitalna forenzika, virtuelno okruženje, forenzička analiza.

U ovom radu su opisani najznačajniji elementi kojima treba posvetiti posebnu pažnju prilikom digitalno forenzičke analize u virtuelnom okruženju. Takođe su objašnjeni i najvažniji segmeti samog virtuelnog okruženja i na koji način oni mogu biti značajni za postupak digitalne forenzičke analize. U radu su razmatrane dva aspekta virtuelnog okruženja. Sa prvog aspekta posmatra se virtuelno okruženje kao digitalno mesto krivičnog dela. U njemu su opisani servisi i mreže virtuelnog okruženja, mesta na kome se mogu pronaći potencijalni dokazi, načini

ni obezbeđenja digitalnog mesta krivičnog dela i očuvanja pronađenih digitalnih dokaza. Drugi aspekt posmatra virtuelno okruženje kao okruženje za digitalno forenzičku analizu podataka. Analiziran je jedan opšti koncept virtuelnog okruženja sa prikazanim ograničenjima u primeni digitalno forenzičke analize. Koncept podrazumeva da se proces digitalno forenzičke analize sprovodi istovremeno pod konvencionalnim i virtuelnim okruženjem nezavisno jedno od drugog, što kao benefit može da ima skraćenje trajanja digitalno forenzičke analize. To zapravo znači da se sa ovakvim forenzičkim pristupom, kombinacijom klasičnog i virtuelnog pristupa, koji se realizuje kroz saradnju timova različitih nivoa stručnosti uz primenu različitih tipova alata rezultati u fazi digitalno forenzičke analize mogu brže dobiti.