Journal of Technical Science and Technologies, 1(2):41-46,2012 ISSN:2298-0032

Virtual Desktops Infrastructure in Terms of Digital Forensic

Medhat M. Mousa*

Abstract

Digital information forensics are a very important part of information Security, whereas via digital forensics a specialist could figure out and extract much information that could be represented in the court against an attacker. The Windows Registry is core of windows and its structure depends on the key and its sub keys building. However, the mechanism and structure of the Windows Registry could be different from one operating system to another, in this paper, we present some major aspects of the latest proposed virtual desktop infrastructure VDI techniques in terms of digital forensics as well as some recommendations.

Keywords: VDI, Digital Forensic, Information Security, Windows Registry.

Introduction

As a virtual infrastructure that includes a server and client side and many other components, VDI has become a very vital area in the current enterprise. Due to some facilities from the administrative standpoint, VDI by design has some different techniques, or it could be implemented by different mechanisms. One of them is that the created hosted desktop runs as a full operating system Pool-Dedicated" in the Data center" also is another form which implies the end user's persona in addition to some dedicated capacity, e.g. 2 GB of RAM for the daily business process such as word documents or even video content. Windows registry plays very important role in the enterprise in terms of security, the registry should be changed under certain circumstances and the changes should be done by the administrator's privilege. In case of any changes in the keys or sub keys, the behavior of the OS will be changed accordingly. The need to take control of the windows, meaning to take control of the registry that have a substantial impact on the rest of the enterprise, which means the attacker could possibly change some configuration settings in order to gain access or penetrate some resources over the network, or change some hardware parameters by specific values. Not only this but also the attacker could escalate his gained access by removing or modifying privileges of some users under specific groups. Therefore, it is desirable in this paper to introduce some important and significant clarifications about the mechanism of windows registry security and how it could be improved, also very importantly to create or extract any evidence against the attacker. The research has been conducted with some experimental environments such as Microsoft windows 7 32-bit Enterprise edition and some other Digital Forensic tools,

The paper is organized as follows: Section 2 explains the used methodology includes the materials. Section 3 discusses concept of Windows registry in addition its impact on the OS, Section 4 explains some aspects about VDI, Section 5 explains the structure of the Windows Registry, Sections 6 discusses analysis of the registry, Section 7 explains the experimental Scenario as well as the discussion, Section 8 discusses the conclusion, and at last the references in Section 9.

2. Method and Materials

The ultimate goal of our paper is to show how we can extract and Analyze data in order to get digital evidence from a Virtual Machine (VM) specifically from the "windows registry", according to journal article in (Mousa, M., 2012)., whereas the conducted experiment will be the backbone in our research. Meanwhile as we go along with the paper we shall discuss types of the VDI which means, VDI Linked-Clone will be explained as well as some other materials "forensic analysis Tools".

Materials

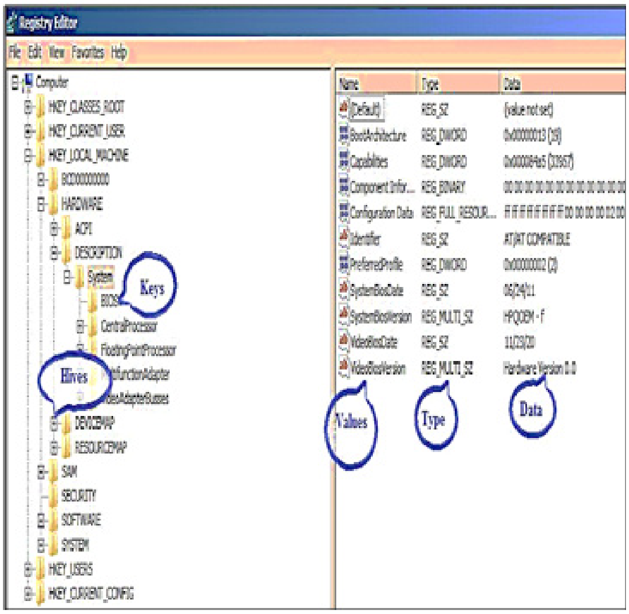
Firstly there should be some initial servers for the main services in the VDI infrastructure such as Domain Host Configuration Protocol (DHCP), Domain Name Services (DNS), and Domain Control (DC), View 4.1 components that includes a composer server, a connection server, and a Security Server.

3. Concept of Windows Registry

The registry has been the centralized configuration database for Windows and supported applications since Windows 95s' introduction. From the Windows registry, a

* *A PHD. C. and Lecturer in the International Black Sea University at the faculty of Computer Technologies and Engineering, Tbilisi, Georgia,*
E-mail: mmousa@ibsu.edu.ge

forensics examiner can discover hardware and software configuration, user preferences, and even logon and password information (Nolan R., 2005) however, The Registry is a binary, hierarchal database (support.microsoft.com, 2012) In addition, the Registry maintains historical information about user activity. In order to provide the user with a "better" personalized experience, the Registry maintains details about applications installed and opened, as well as window positions and sizes. This information is maintained within the Registry in terms of (tree, sub tree, key, sub key, or value) in a similar manner to a log; meanwhile this log could be helpful in case of digital crime investigations. The end user or the system administrator should take into account the size of these logs "registry configuration size" which means the more programs the operating System has, the more complicated and bigger the registry hierarchy.



Name	Type	Data
(Default)	REG_SZ	(value not set)
BootArchitecture	REG_DWORD	0x00000013 (19)
Capabilities	REG_DWORD	0x000084e5 (33967)
Component Infor...	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 00 00
Configuration Data	REG_FULL_RESOUR...	ff ff ff ff ff ff ff ff 00 00 00 00 02 00
Identifier	REG_SZ	AT/AT COMPATIBLE
PreferredProfile	REG_DWORD	0x00000002 (2)
SystemBiosDate	REG_SZ	06/24/11
SystemBiosVersion	REG_MULTI_SZ	HPQOEM - f
VideoBiosDate	REG_SZ	11/23/20
VideoBiosVersion	REG_MULTI_SZ	Hardware Version 0.0

Figure 1: *Registry Editor in Windows 7*

In addition, there is an important role of time-stamped information maintained in the Registry, including, but not limited to file (Carvey, H., 2011).

When a user opened an application or accessed a Control Panel applet

The last time the system connected to a particular wireless access point

When a graphic image viewing application was used to access a particular file

3.1. Impact of the Registry Changes on the Operating System

As mentioned before the size of the registry keys depends on the installed Applications and Software, which means the end user may install a program that modifies the registry or may "Open" a back door for the attacker. The created backdoors if used by the attacker will give high possibility to exploit the system that has this built-in vulnerability "the created Backdoors" thereafter the behavior of the OS will be changed accordingly or any sensitive data will be exposed by the attacker.

A Digital Forensic investigator is a specialist person in collecting and analyzing the digital evidences from different sources, in many cases, the best source of information or evidence is available in the computer memory (network connections, contents of the IM client window, memory used by the IM client process, encryption keys and passwords, etc.) (Carvey, H.,2009)

4. VDI as a New Paradigm,

In fact, VDI is a new and young aspect in IT Infrastructure and it has been constructed by some manufactures such as VMware, Microsoft, and CITRIX,

4.1 Definition of VDI

According to VMware View, IT departments can run virtual desktops in the datacenter and deliver desktops to their end users as a managed service. The End users gain a familiar and personalized environment that they can access from any (Remote/Local) device, throughout the enterprise or from home. Administrators gain centralized control, efficiency, and security by having their desktops in addition to their data in the datacenter.

4.2 Linked Clone Concept

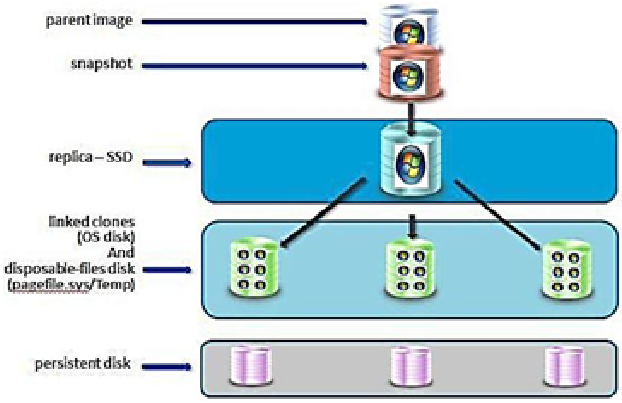


Figure 2: *Linked clone and parent Image*

The Linked-clone desktop pools and its replica have been created "Generated" after creating the parent image "Golden Image" and its snapshot, which means that there is a single image for building the hosted desktops as Figure (2) shows, whereas it should be done under certain circumstances and special security parameters, namely after installing the required applications and software e.g. MS

Office 2010. There is a snapshot should be taken thereafter the replica image will be the second source for the virtual desktop machines. Also the end user will be able to use his/her profile efficiently, meanwhile a user might log in to a floating-assignment, linked-clone desktop pool and change the desktop background and Microsoft Word settings. When the user starts the next session, the received virtual machine will be different, but the user sees the same settings. A user profile comprises a variety of user-generated information (Corp, V., 2012)

a) User-specific data and desktop settings

b) Application data and settings

c) Windows registry entries configured by user applications

In addition, there are some aspects about linked-clones Approach like:

a) The end user has no possibility to change in behavior of the OS or even modify configuration of its parameters,

b) In such a way with every restart the end user will receive the same desktop/ profile by the same settings, which means that any changes will be removed by the next log on, and then the default configuration will be restored.

c) The actual registry (tree, sub tree, key, sub key, or value) has been extracted from the original source "Golden image", it is taken off by the administrator.

The conclusion from the previous section is that, the in case of the traditional desktop when the end user tries to install some software which includes "malicious code" the changes remain in the core of the OS "Backdoors" even after restart. Therefore, the Digital Forensic Investigator can initiate his research methodology to collect and get evidence, unlike in the Linked-Clone Desktop approach.

5. Structure of the Registry

Windows registry is a centralized hierarchical Database (support.microsoft.com, 2012) that maintains configuration settings for applications, hardware devices, and users. When the administrator opens regedit.exe, there will be a treelike structure with five root folders, or "hives," in the navigation area of the GUI, as Figure (3) illustrates. This folder like structure allows the administrator to navigate easily through the Registry, much like a file system (Carvey, H., 2009)

As figure (3) shows, "Five Root Hives" the System Administrator is able to edit the content of the registry easily via Graphical User interface GUI by typing "regedit", but now it is desirable to know and understand structure of the registry. Meanwhile the Analyst should be able to get an abstraction layer by looking at the structure of the Hives and its nodes,

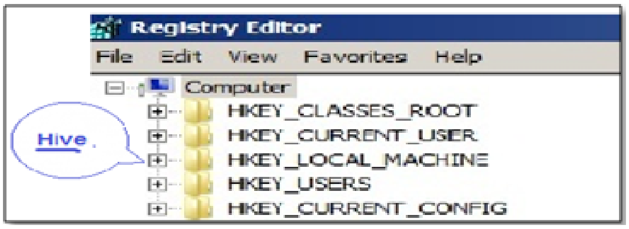


Figure 3: *Regedit.exe View Showing Five Root Hives*

5.1. Hierarchies of Five Root Hives

In order to explain structure of the registry we need firstly to understand the main function of the "Five Root Hives", each of these hives plays an important role in the function of the system. The HKEY_USERS hive contains all the actively loaded user profiles for that system. HKEY_CURRENT_ USER is the active, loaded user profile for the currently logged-on user. The HKEY_LOCAL_MACHINE hive contains a vast array of configuration information for the system, including hardware settings and software settings. The HKEY_CURRENT_CONFIG hive contains the hardware profile the system uses at startup. Finally, the HKEY_CLASSES_ROOT hive contains configuration information relating to which application is used to open various files on the system. This hive is sub classed to both HKEY_CURRENT_USER\Software\Classes (user-specific-settings), and HKEY_LOCAL_MACHINE\Software\Classes (system wide settings). All of this is fine and good, but it helps to know where the hives come from and where they exist on the hard drive within the file system (Carvey, H., 2011) The five root keys and their subkeys are described below.

(1) HKEY LOCAL MACHINE (HKLM). HKLM is the first master key. It contains all of the configuration settings of a computer. When a computer starts up, the local machine settings will boot before the individual user settings. If we double-click this entry in Windows Registry Editor, five sub keys will be listed: HARDWARE, SAM, SECURITY, SOFTWARE, and SYSTEM. The information contained by these sub keys are listed below (Xie1 H., 2012)

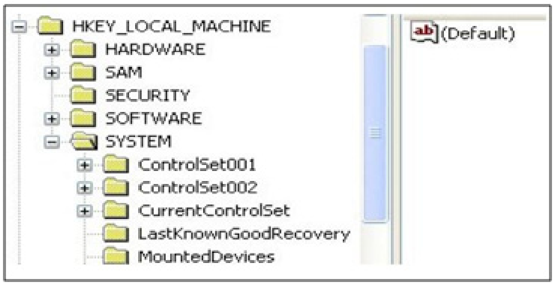


Figure 4: *HKEY_LOCAL_MACHINE Root Key and Its Sub keys*

a) HARDWARE is used to store the information of hardware devices that a computer detects when the computer starts up. Therefore, the sub keys in HARDWARE are also created during the booting process.

b) SAM is the abbreviation of Security Account Manager which is a local security database. Sub keys in SAM contain the setting data of users and work groups.

c) SECURITY includes a local security database in SAM and a strict ACL is used to manage the users who could access the database.

SOFTWARE includes all of the configuration settings of programs. Information on the programs is stored in a standard format: HKLM\Software\Vendor\Program\Version.

SYSTEM contains the configuration settings of hardware drivers and services. The key path is HKEY_LOCAL_MACHINE\SYSTEM\ControlSetXXX, where XXX is a three digital number from 000, as shown in Figure (4)

(2) HKEY USERS (HKU): HKU is another master key. It contains all of the per-user settings such as current console user and other users who logged on this computer before. Double-click this entry; we can see at least three kinds of sub keys listed: KEFAUTL, SID, and SID_CLASS. SID is security identifier, which refers to the current console. SID-CLASSES contains per user class registration and file association. Usually, we could see S-1-5-18, S-1-5-19, and S-1-5-20, which represents Local System Account, Local Service Account, and Network Service Account respectively. Unlike the above two keys, HKEY CLASSES ROOT (HKCR), HKEY CURRENT USER (HKCU), and HKEY CURRENT CONFIG (HKCC) are derived keys and they only link to the two master keys and their sub keys.

(3) HKEY CLASSES ROOT (HKCR): HKCR contains two keys: HKLM\SOFTWARE\Classes and HKCU\Software\Classes. The first one refers to the default registration classes, and the second one refers to per user registration classes and file associations.

(4) HKEY CURRENT USER (HKCU): HKCU links to a sub key of HKU, HKU\SID. This key allows all of the Windows programs and applications to create, access, modify, and store the information of the current console user without determining which user is logging in. Under the root key HKCU, there are also five sub keys: Environment, Identities, Network, Software, and Volatile Environment.

Environment is about the environmental configurations.

Identities are related to Outlook Express.

Network contains settings to connect the mapped network drive.

Software refers to the user application settings.

Volatile Environment is used to define the environmental variables according to different users who logon a computer.

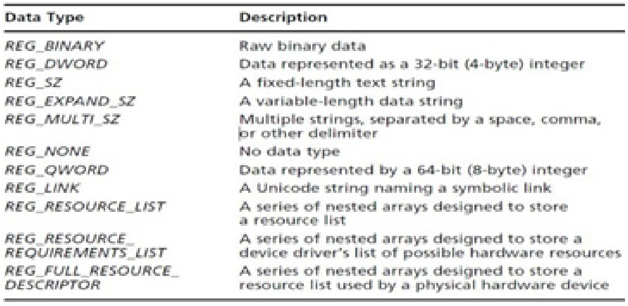
(5) HKEY CURRENT CONFIG (HKCC): HKCC is an image of the hardware configuration profiles.

HKLM\SYSTEM\Current\ControlSet\Hardware\Current, Is also a link to HKLM\SYSTEM\ControlSet\Hardware Profiles\XXXX, where XXXX is a four digital number from 0000.

5.2. Types of the Data in the Registry

In addition to the different sections or hives, the Registry supports several different data types for the various values that it contains. Table (1) lists the various data types and their descriptions (Carvey, H., 2009)

Table 1: *Registry Data Types and Descriptions*



Data Type	Description
REG_BINARY	Raw binary data
REG_DWORD	Data represented as a 32-bit (4-byte) integer
REG_SZ	A fixed-length text string
REG_EXPAND_SZ	A variable-length data string
REG_MULTI_SZ	Multiple strings, separated by a space, comma, or other delimiter
REG_NONE	No data type
REG_QWORD	Data represented by a 64-bit (8-byte) integer
REG_LINK	A Unicode string naming a symbolic link
REG_RESOURCE_LIST	A series of nested arrays designed to store a resource list
REG_RESOURCE_REQUIREMENTS_LIST	A series of nested arrays designed to store a device driver's list of possible hardware resources
REG_FULL_RESOURCE_DESCRIPTOR	A series of nested arrays designed to store a resource list used by a physical hardware device

5.3. Registry Structure within a Hive File

Each type of cell has a specific structure and contains specific types of information, Figure (5). The various types of cells are:

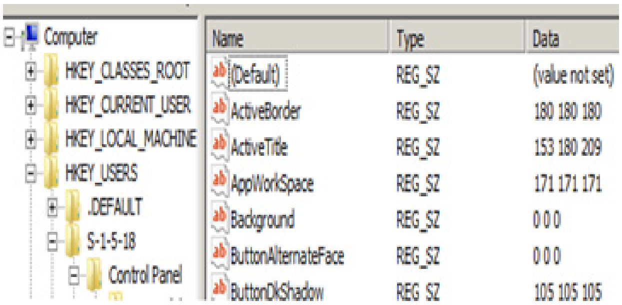
Key cell, this cell contains Registry key information and includes offsets to other cells as well as the Last Write time for the key (signature: kn).

Value cell, this cell holds a value and its data (signature: kv).

Sub key list cell, this is a cell made up of a series of indexes (or offsets) pointing to key cells; these are all sub keys to the parent key cell.

Value list cell, this is a cell made up of a series of indexes (or offsets) pointing to value cells; these are all of the values of a common key cell.

Security descriptor cell, this is a cell that contains security descriptor information for a key cell (signature: ks).



Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
.DEFAULT
S-1-5-18
Control Panel

Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveBorder	REG_SZ	180 180 180
ActiveTitle	REG_SZ	153 180 209
AppWorkSpace	REG_SZ	171 171 171
Background	REG_SZ	0 0 0
ButtonAlternateFace	REG_SZ	0 0 0
ButtonDkShadow	REG_SZ	105 105 105

Figure 5: *Registry Showing Keys, Values, and Data*

5.4. Windows Registry Analysis

In short, “Registry analysis” can run across a spectrum of activities, from extracting specific key and/or value information to searching within the Registry and correlating data retrieved from different areas of the Registry. All of these activities can constitute the scope of “analysis” although both analysis and the examination itself may often benefit from something more.

5.5. Analysis Concepts

Before we talk about Registry analysis specifically, there are a few analysis concepts that we need to discuss that are pertinent to examinations as a whole. Keeping these concepts in mind can be extremely beneficial when performing digital analysis in general (Carvey, H., 2011)

• Everything Leaves a Trace
Almost any interaction with a Windows system, particularly through the Windows Explorer graphical interface, will leave a trace. These indications are not always in the Registry, and they may not persist for very long, but there will be something, somewhere. It’s simply a matter of knowing what to look for and where, and having the right tools to gain access to, and understanding of how to correctly interpret the information.

• Least Frequency of Occurrence
The point of Least Frequency of Occurrence (LFO) is that during the lifetime of a system, malware infections and intrusions are often what occur least frequently on that system. Operating system and application updates are extremely noisy,” generating a great deal of file system (file creations, modifications, and deletions) and Registry (keys being created, values updated, and so on) activity, and occurring fairly frequently. Windows XP, by default, will create a System Restore Point every24 hours (as well as under other conditions) and will also launch its Disk Defragmenter utility every three calendar days to perform a limited defrag.

• Goals
Before starting any analysis, every analyst should carefully consider and document their goals. And take into account that after the investigation there should be answers for some questions that were mysteries before the digital forensic analysis.

• Documentation
Perhaps the most important aspect of any analysis, after the goals, is documentation. Forensic analysts and incident responders should document all aspects of what they do, however, sometimes the investigator may need to learn from previous and similar cases that have been documented by him, or even the others but if there is no documentation for the previous cases it would be difficult for the investigator to initiate the investigation from scratch in every case.

• Assessment Mechanisms
Since we have mentioned in the previous sections Regedit “Registry Editor” Tool as an easy tool and handy because of its GUI, the administrator can add delete or modify any key under any Hive. Whereas we found the used tool has some limitations such as Last Time access that is very important for the investigator to perform a detailed research and data acquisition “after the image creating”. There are some different tools that could be used to create an image then extract and acquire some certain data, some of these tools (RegRipper, MiTeC, and FTK Imager Lite X.x, and EnCase).

6. Experimentation

In our experiment we have used ProDiscover 7.2 in addition VMware View 4.1, and “Windows 7 32-bit Enterprise Edition”, also it is important in our research that the main concept of collecting the digital evidences in a documented manner for the court of law. ProDiscover is a powerful tool for windows registry analysis and it has some other capabilities. The following steps were taken during the experiment:

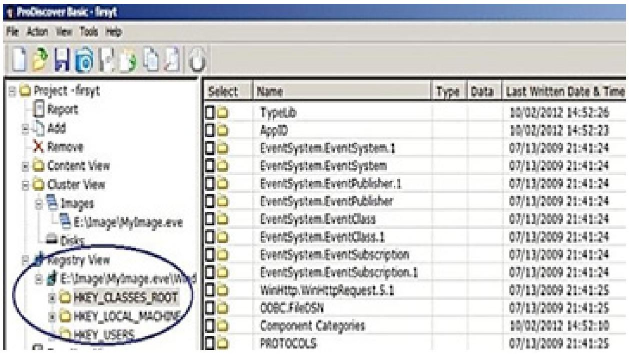
1. After creating a project and specifying location “Directory” of the image, therefore the captured image should be loaded in the current project/ profile.

2. The analyst should explore the image content till approach the “Windows” Directory, then by adding the selected directory to Registry Viewer,

3. ProDiscover will locate “system32\config” which has the Hives directory,

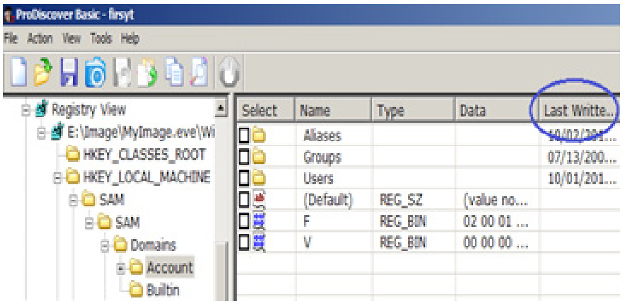
6.1. Discussion

Since ProDiscover populated the Hives that are located under “system32\config”, the analyst will be able to get into any proper information under any hive as figure (6) shows. for instance, in case of Trojan horse, and the analyst would like to analyze behavior of the attacker by verifying last write time, as figure (7) shows, then the analyst can decide whether the attacker could escalate his/her privileges or not,



Select	Name	Type	Data	Last Written Date & Time
□	TypeLib			10/02/2012 14:52:26
□	AppID			10/02/2012 14:52:23
□	EventSystem.EventSystem.1			07/13/2009 21:41:24
□	EventSystem.EventSystem			07/13/2009 21:41:24
□	EventSystem.EventPublisher.1			07/13/2009 21:41:24
□	EventSystem.EventPublisher			07/13/2009 21:41:24
□	EventSystem.EventClass			07/13/2009 21:41:24
□	EventSystem.EventClass.1			07/13/2009 21:41:24
□	EventSystem.EventSubscription			07/13/2009 21:41:24
□	EventSystem.EventSubscription.1			07/13/2009 21:41:24
□	WinHttp.WinHttpRequest.5.1			07/13/2009 21:41:25
□	ODBC.FileDSN			07/13/2009 21:41:25
□	Component Categories			10/02/2012 14:52:10
□	PROTOCOLS			07/13/2009 21:41:25

Figure 6: *Registry Viewer and its Hives structure*



Select	Name	Type	Data	Last Writte...
□	Aliases			10/02/201...
□	Groups			07/13/200...
□	Users			10/01/201...
□	(Default)	REG_SZ	(value no...	
□	F	REG_BIN	02 00 01 ...	
□	V	REG_BIN	00 00 00 ...	

Figure 7: *Excerpt of a hive and last write time access*

Conclusion

In this paper we have clarified and discussed some important aspects about “VDI” from digital forensic standpoint, as mentioned previously that VDI could be deployed in some different manners with the corresponding to the end user level “Standard or Power user” e.g. Pool-Floating or Poll-Dedicated. However, when we look at Linked-Clone based VM/desktop pool, and Standard user, we found that the end user receive a new fresh Desktop at every log on. In another words, “no impact of violation of security policy”, on the contrary, when we give a full VM/desktop to the end user i.e. Power user Pool-dedicated, and in case of violation of security policy there will be a great negative impact on the infrastructure because the VM has been hosted in the data center itself. Therefore, the malicious code will be able to exploit the infrastructure entirely.

Some Recommendations

As we explained previously the View administrator should take in to account some aspect in terms of security violation:

1. The pools should be assigned to whom can deal and act professionally with the organization’s policy,
2. The entire infrastructure should be supplied by multiple high security protection levels; includes Security Server of View 4.1 suite.
3. The infrastructure should face a penetration-test periodically to evaluate the present and exposed backdoors.

References

MOUSA, M. (2012). Virtualization Technology| Revolution of Virtual Desktop Infrastructure. p. 8.

Richard Nolan, C. O. (2005). First Responders Guide to Computer Forensics.

Microsoft. (n.d.). Windows registry information for advanced users. [Online]. Available. Retrieved Septemper 20, 2012, from http://support.microsoft.com/kb/256986

Carvey, H. (2011). Windows Registry Forensics P 20.

Harlan Carvey, E. C. (2009). Windows Forensic Analysis DVD Toolkit 2E. P 27.

Corp, V. (2012). VMware View Administration Guide, P 209. VMware.

Microsoft Corp. (n.d.). Retrieved Septemper 28, 2012, from Microsoft: [online]. Available http://support.microsoft.com/kb/256986

Harlan Carvey, E. C. (2009). Windows Forensic Analysis DVD Toolkit, P184.

Carvey, H. (2011). Windows Forensic Analysis DVD Tool kit, P 185.

Haoyang Xie1, K. J. (2012). Forensic Analysis of Windows Registry. International Journal of Network Security & Its Applications (IJNSA), 3.

Harlan Carvey, E. C. (2009). Windows forensic analysis Toolkit P. 162.

Harlan Carvey, D. H. (2011). Windows Registry Forensics P. 24.