A Digital Forensic Approach for Examination and Analysis of Frozen Hard Disk of Virtual Machine

M. George Christopher[1], Kumarshankar Raychaudhuri[2]

[1] State Forensic Science Laboratory, Madiwala, Bengaluru, India
[2] LNJN National Institute of Criminology and Forensic Science, Ministry of Home Affairs
Govt. of India

ABSTRACT

There are software tools in the open market which help in safeguarding the computer system from malware, viruses and other unintentional changes to the users Operating System. Faronics' Deep Freeze is one such type of software, which can be used to freeze any hard drive partition, so that any write operation to that partition is reset once the computer system is shutdown or rebooted. However, from the perspective of Digital Forensics, the same software application can also be used as a perfect anti-forensic tool to leave no traces of any activity, thus adding to the challenges of a forensic analyst. In this research work, our primary objective is to perform a forensic analysis of the Deep Freeze software using various tools and techniques, by collecting volatile and non-volatile data. This would be useful in further examination of the frozen partition of the hard disk in an attempt to recover the data, which might be lost after reboot or shutdown. Lastly, based on the results and conclusions of the experiments, some best practices necessary for handling of computer systems (with frozen virtual hard disks), will be suggested. Such best practices would be enlightening for the forensic practitioners in dealing with cyber-crime cases involving frozen virtual hard drives.

KEYWORDS

Deep Freeze, Virtual Machine, Frozen Virtual Hard Disk, Anti-Forensics, Background Process, Digital Forensics, Volatile Data, Data Recovery, Frozen Partition

1 INTRODUCTION

Computers now-a-days are an essential part of any educational institution, conventional library setups and corporate organizations, where it is mode of communication. They can be used for downloading harmful files from unknown websites or play around with the configurations of the system. In such circumstances, the need is to have a software application, which can keep the system safe from malwares and other unintentional changes. Faronics' Deep Freeze is an application software, which can be used to freeze the partitions of the hard drive, as a result of which any changes made (for e.g. addition or deletion of files, modification of files etc.) to the frozen partitions will revert and reset, once the computer system is rebooted or shutdown [3]. This will set the partition to its original state, as defined by the user. As the storage space increases, more and more data are being stored in digital exhibits such as hard disks or other USB storage devices [11,12]

The ability of Deep Freeze to reset the computer system back to its original state (defined by user) after every reboot or shutdown, makes it an excellent tool for performing anti-forensic activities. After committing an act of crime, this software can be used to remove all the traces of evidential data from the hard disk and set it to a state, which might not yield any footprints of the criminal. This makes forensic investigation a challenging task for the examiners. However, researches have been conducted by performing static forensic analysis on frozen hard disks of computer systems [2]. Different digital forensic tools have been used, resulting in the recovery of files from unallocated spaces of the frozen hard drive, even after the use of Deep Freeze software. No researches have been conducted by using the software inside virtual machine in a computer system. Therefore, in this research work, our primary objective is to perform a forensic analysis of a virtual machine installed with Deep Freeze software using various tools and techniques. Volatile data is collected to find artifacts of deep freeze software running as a background process in the computer. By establishing the presence of the software, it would in turn be useful in following a new data acquisition technique and further examination of the frozen partition of the virtual hard disk for recovery of data that might have been lost after reboot or shutdown. Lastly, based on the results and conclusions of the experiments some best practices necessary for handling of computer systems (with frozen virtual hard disk), will be suggested. It will also be helpful in uplifting the knowledge of forensic practitioners allowing them to deal more efficiently with different cyber-crime cases, involving frozen virtual hard disks.

The research paper has been organized as follows: Related Literature Survey has been presented in Section 2. This is followed by Experimental Design i.e. Section 3, which further consists of the tools used for the experiments and methodology adopted. Section 4 discusses the Results and Analysis based on the various tools and techniques used in carrying out the experiments. The Applicability of this research work is highlighted in Section 5, followed by Section 6, which consists of Conclusion and Future Scope.

2 RELATED LITERATURE SURVEY

Faronics Deep Freeze is a software, which helps in preserving the configurations of a computer system by reverting any unintentional or malicious changes on reboot [9]. All the write operations performed on a partition that has been frozen by Deep Freeze software, will be returned to their original state when the computer is shutdown or restarted [1,2]. This provides a high-end protection for the workstation or computer system by saving the desired configurations and settings each time. Thus, it ensures 100% recovery of workstation with every restart.

It is an efficient software to clear the computer system off all malicious programs including zero-day threats. This removes all the software applications, which might be installed without the authorization of the user. The software uses patented technology, which allows it to keep the original data intact by re-directing the newly written changes to an allocation table in the hard drive [2,9]. Once the computer system is restarted, the reference to the redirected information in the allocation table is lost, thereby restoring the system to its original configurable state, down to the last byte of data.

This type of technology is an excellent weapon in the hands of cyber-criminals. Since, a computer system having such software installed in it, loses all the last written data on the hard disk, it becomes easier for them to commit the crime and leave the system switched off. Thus, any trail of evidence or digital footprints will be lost even if the system is seized from the crime scene and forensic examination is done. Without any kind of digital evidence, conviction of the criminal would not be possible. Therefore, in other words, we can say that this is one of the most efficient anti-forensic tools for criminals and perpetrators, whereas on the other hand, it is a big challenge for forensic practitioners. Forensic analysis of frozen hard drives using static analysis methods have shown that it is possible to recover document files, image files and log files from frozen hard disks by using forensic tools such as Winhex, Foremost etc. [2]. Similar experiments performed on frozen Solid-State Drives (SSD) have concluded that not all files can be recovered due to damage of the file structure and data. Also, it is not possible to read all the artifacts by existing forensic tools. Only some artifacts can be acquired using the forensic tools [1].

Although, researches in the past have shown that data can be recovered even when deep freeze is working in a computer system, but no literature has been found suggesting on how evidences can be acquired from frozen hard disk in a virtual machine, with special focus on collection of volatile data. This is highly essential to be considered during digital investigations, since it is probable that computer systems with running virtual machines could be found at the crime scene. Taking the challenge as a foundation for our research, we make an attempt in tracking and detecting the presence of this software (in running condition) and recovering data from the frozen hard disk of a virtual machine, based on which some best practices can be suggested for handling cases involving frozen virtual hard drives.

3 EXPERIMENTAL DESIGN

This experiment has been conducted by installing Deep Freeze software in a virtual machine (VM). The host machine/base machine configuration are shown in Table 1.

Table 1: Configurations of host machine used for conducting experiment

Model	MacBook Air (Mid 2013)
Processor	1.3 GHz Intel Core i5
Memory	4GB 1600 MHz DDR3
Operating System	MacOS_Sierra
Graphics	Intel HD Graphics 5000 1536 MB
Storage	Apple SSD SD0128F: 128 GB

The guest machine installed in the virtual machine is Windows 10 Professional with configurations as shown in Table 2.

Table 2: Configurations of guest machine used for conducting experiment

Operating System	Windows 10 Professional 64 bit
Base Memory	2048 MB
Storage	Windows 10.vdi (Normal, 50.00 GB)
Shared Folders	01

3.1 Tools Used

The following tools have been used in conducting the research:

a) Oracle VM VirtualBox 6.0
b) Faronics Deep Freeze Standard (Evaluation Version)
c) Win-UFO (Windows Ultimate Forensics Outflow)
d) Helix Incident Response v2.0
e) Windows SysInternals Suite
f) FTK Imager 3.2.0 (for Windows) [8].

3.2 Methodology

The procedure of performing the experiment are as follows:

i. Install Oracle VM VirtualBox 6.0 in the host machine.
ii. Create a new virtual machine with Windows 10 Professional as the guest operating system with configurations, as given in Table 2. The storage space allotted to virtual machine is not partitioned.
iii. Boot the virtual machine and clean install Windows 10 Pro.
iv. Download and install the software Faronics Deep Freeze. On successful installation, the hard disk partition is frozen by the software.
v. Different digital forensic tools (Windows SysInternals Suite, Helix 2.0 and Win-UFO) and Windows Task Manager are used to collect volatile evidences such as running background processes, processes accessing remotely, last activities of user etc. from the live system (virtual machine). These tools are used through USB thumb drive plugged-into the system.

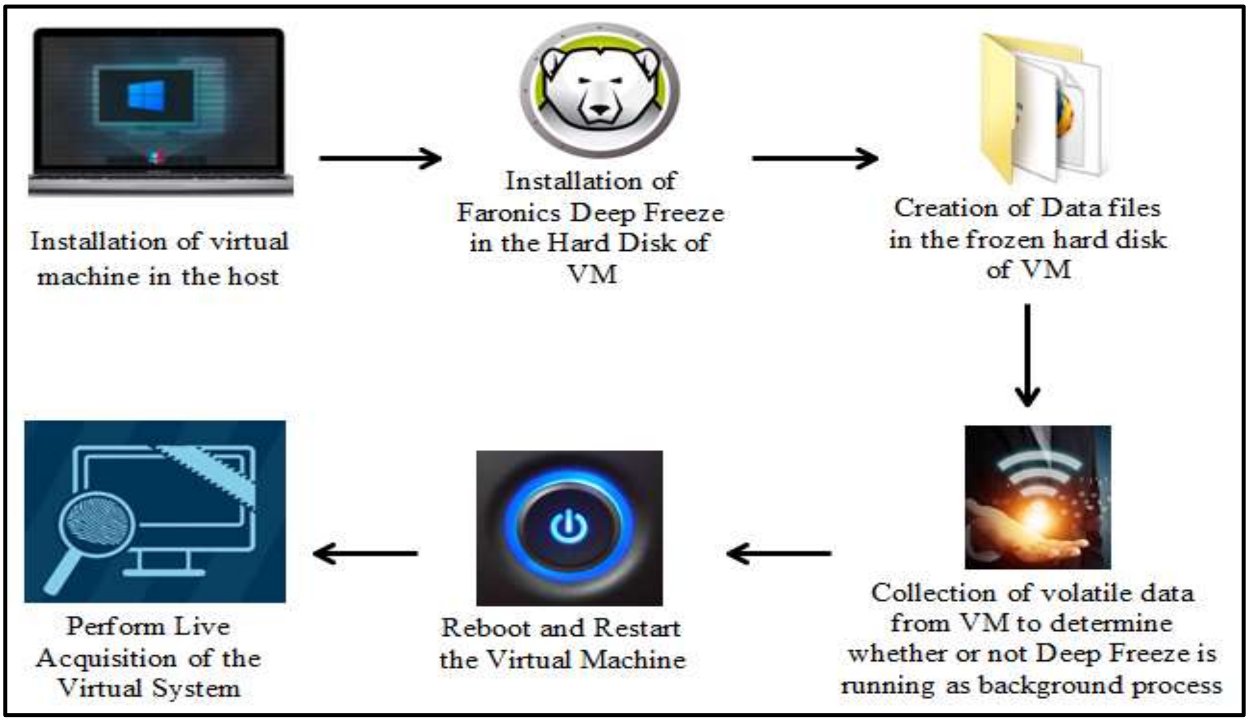

Installation of virtual machine in the host
Installation of Faronics Deep Freeze in the Hard Disk of VM
Creation of Data files in the frozen hard disk of VM
Collection of volatile data from VM to determine whether or not Deep Freeze is running as background process
Reboot and Restart the Virtual Machine
Perform Live Acquisition of the Virtual System

Figure 1: Illustration of Methodology of the Experiment

vi. Text files of sizes 4KB (4096 bytes), 8KB (8192 bytes), 12KB (12288 bytes), 16KB (16,384 bytes) and 4MB (4,194,304 bytes) are created in the location “C:\Users\Windows10\Desktop”.
vii. FTK Imager is used for imaging of the physical hard disk (in frozen state) of the virtual machine while in live running condition.
viii. The virtual machine is rebooted, following which step v and step vii are repeated.
ix. A comparative analysis of both, volatile evidences and forensic images before and after the reboot, are done in order to determine differences between them.
x. Based on the comparative analysis of volatile evidences and the forensic images, some best practices regarding handling of computer systems with frozen hard drives at the crime scene, are formulated.

4. RESULTS AND ANALYSIS

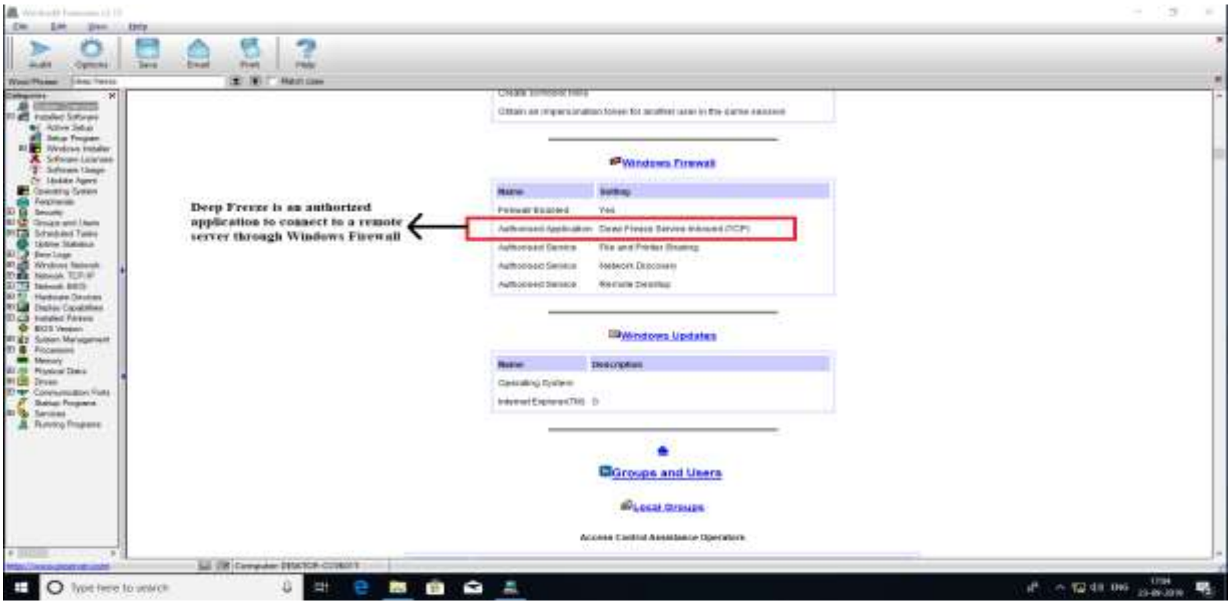
The volatile evidences from the running virtual machine is collected using different digital forensic tools such as Helix 2.0, Win-UFO, SysInternals and Windows Task Manager. The results obtained by the tools are analysed and discussed in this section.

4.1 Analysis using Helix Incident Response 2.0

Helix Incident Response is used to perform an audit of the entire operating system in the virtual machine [6]. On analysing the audit reports, it is observed that Deep Freeze is marked as an authorized application to connect through the Firewall (highlighted in red), as shown in Fig. 2.

4.2 Analysis of using Win-UFO (Windows Ultimate Forensics Outflow)

Windows Ultimate Forensics Outflow (Win-UFO) is a collection of several open-source digital forensics tools for acquisition, analysis and examination of digital evidences from computer systems, mobile phones, network connections etc. [4]. One of the tools “Last Activity View” has been used to collect volatile information from virtual machine to prepare a log of actions executed by the user and occurrence of events in the machine. The events include “Running of .exe files, Opening file/folder from explorer or other softwares, Installation of software.



Deep Freeze is an authorized application to connect to a remote server through Windows Firewall

Windows Firewall

Name	Setting
Firewall Enabled	Yes
Authorised Application	Deep Freeze Service Inbound (TCP)
Authorised Service	File and Printer Sharing
Authorised Service	Network Discovery
Authorised Service	Remote Desktop

Windows Updates

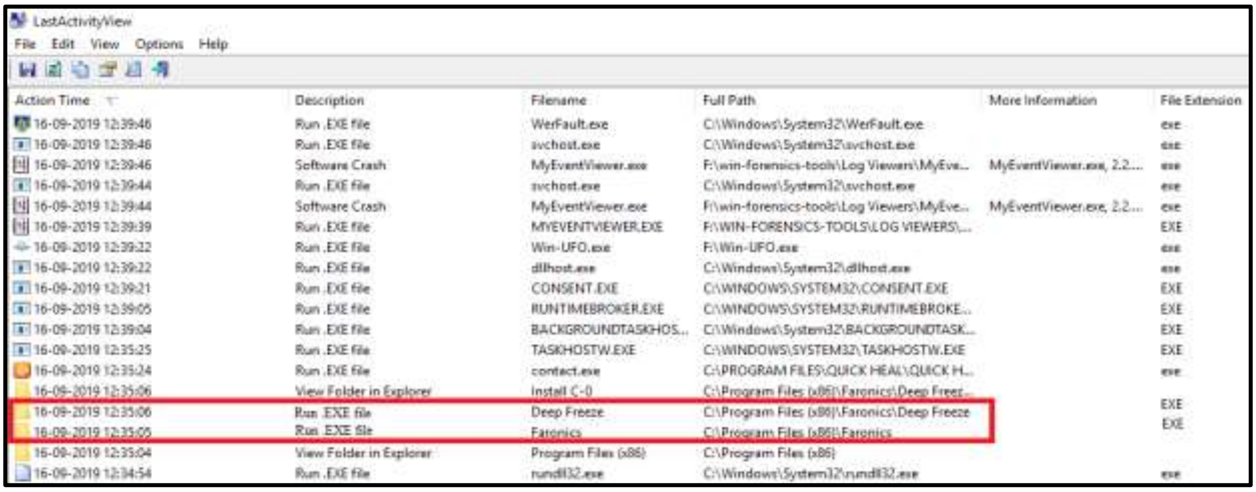
Name	Description
Operating System	
Internet Explorer(TM)	[illegible]

Groups and Users

Local Groups

Access Control Assistance Operators

Figure 2: A snapshot of Helix Incident Response tool used to perform Auditing of the virtual machine



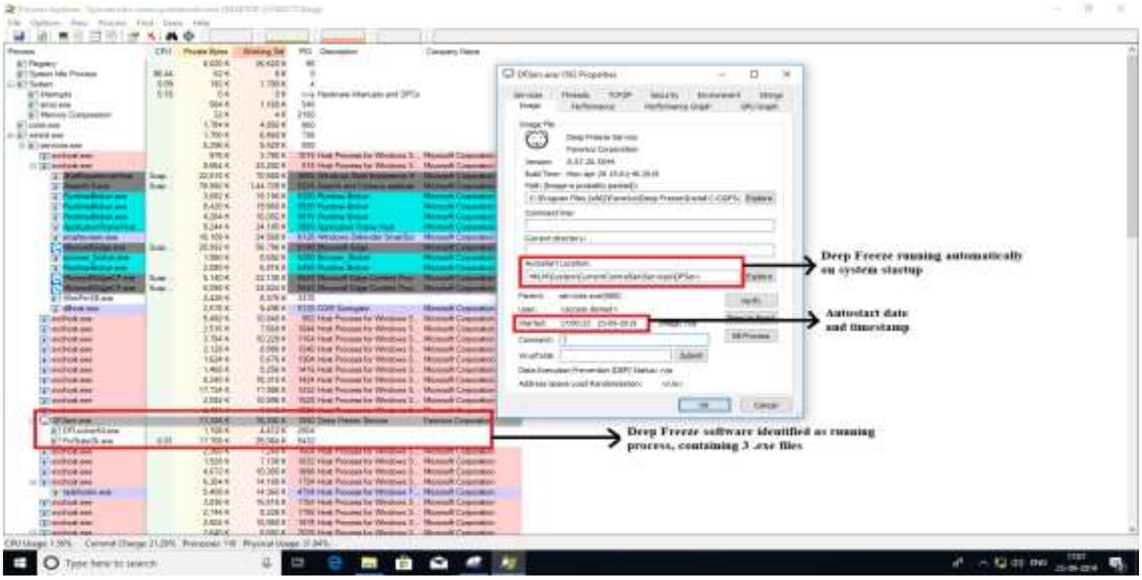
Action Time	Description	Filename	Full Path	More Information	File Extension
16-09-2019 12:39:46	Run .EXE file	WerFault.exe	C:\Windows\System32\WerFault.exe		exe
16-09-2019 12:39:46	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe		exe
16-09-2019 12:39:46	Software Crash	MyEventViewer.exe	F:\win-forensics-tools\Log Viewers\MyEve...	MyEventViewer.exe, 2.2...	exe
16-09-2019 12:39:44	Run .EXE file	svchost.exe	C:\Windows\System32\svchost.exe		exe
16-09-2019 12:39:44	Software Crash	MyEventViewer.exe	F:\win-forensics-tools\Log Viewers\MyEve...	MyEventViewer.exe, 2.2...	exe
16-09-2019 12:39:39	Run .EXE file	MYEVENTVIEWER.EXE	F:\WIN-FORENSICS-TOOLS\LOG VIEWERS\...		EXE
16-09-2019 12:39:22	Run .EXE file	Win-UFO.exe	F:\Win-UFO.exe		exe
16-09-2019 12:39:22	Run .EXE file	dllhost.exe	C:\Windows\System32\dllhost.exe		exe
16-09-2019 12:39:21	Run .EXE file	CONSENT.EXE	C:\WINDOWS\SYSTEM32\CONSENT.EXE		EXE
16-09-2019 12:39:05	Run .EXE file	RUNTIMEBROKER.EXE	C:\WINDOWS\SYSTEM32\RUNTIMEBROKE...		EXE
16-09-2019 12:39:04	Run .EXE file	BACKGROUNDTASKHOS...	C:\Windows\System32\BACKGROUNDTASK...		EXE
16-09-2019 12:35:25	Run .EXE file	TASKHOSTW.EXE	C:\WINDOWS\SYSTEM32\TASKHOSTW.EXE		EXE
16-09-2019 12:35:24	Run .EXE file	contact.exe	C:\PROGRAM FILES\QUICK HEAL\QUICK H...		exe
16-09-2019 12:35:06	View Folder in Explorer	Install C-0	C:\Program Files (x86)\Faronics\Deep Freez...		
16-09-2019 12:35:06	Run .EXE file	Deep Freeze	C:\Program Files (x86)\Faronics\Deep Freeze		EXE
16-09-2019 12:35:05	Run .EXE file	Faronics	C:\Program Files (x86)\Faronics		EXE
16-09-2019 12:35:04	View Folder in Explorer	Program Files (x86)	C:\Program Files (x86)		
16-09-2019 12:34:54	Run .EXE file	rundll32.exe	C:\Windows\System32\rundll32.exe		exe

Figure 3: Snapshot of user activity log showing execution of deep freeze, acquired using Win-UFO

In the result generated by this tool (as shown in Fig. 3), evidence associated to installation and execution of Faronics Deep Freeze software is acquired. The date and timestamp along with the type of action performed and location of the application can be acquired. The action “Run .EXE file” (as marked in red) indicates .EXE file of the specified software application, run either by the user or any other application in the background.

4.3 Analysis of running processes using Windows SysInternals Suite

Windows SysInternals Suite is a bundle of utilities, which can be used for managing, diagnosing and monitoring a Microsoft Windows Environment. It acts as one of the most useful digital forensic tools for examination of Windows operating system. In this suite, Process Explorer is used for conducting the experiments. This utility displays the currently active processes, their owning accounts, handles and DLLs that have been loaded by the operating system [7].



Deep Freeze running automatically on system startup

Autostart date and timestamp

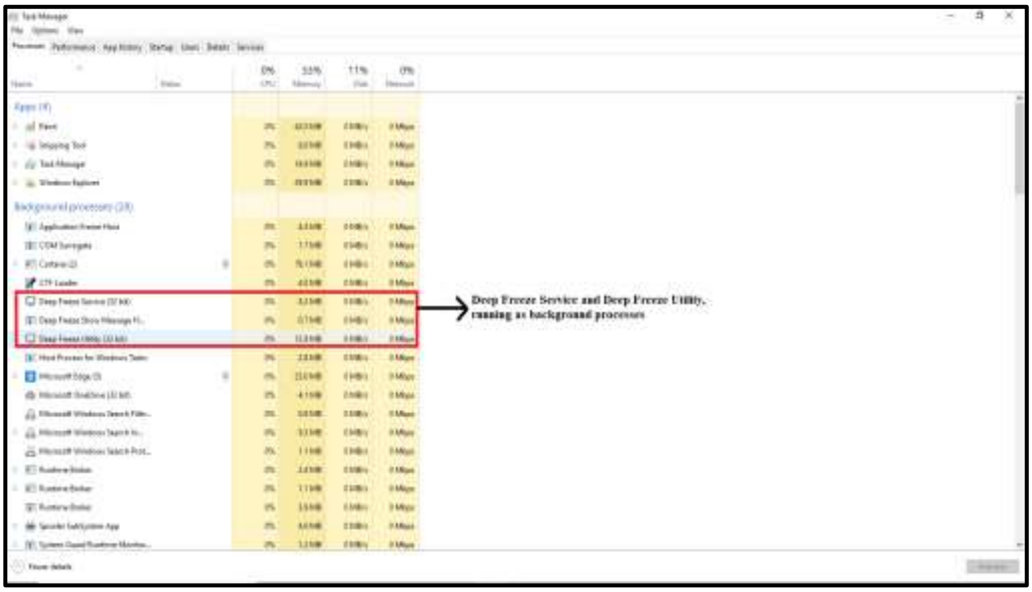
Deep Freeze software identified as running process, containing 3 .exe files

Figure 4: Snapshot of Process Explorer displaying Deep Freeze as an active process, acquired using Windows SysInternals Suite

The analysis of active processes in the VM (as shown in Fig. 4) provides a proof that the application Deep Freeze is a startup file, which indicates the fact that it is executed automatically and starts running on rebooting the VM. The autostart location is given as "HKLM\System\CurrentControlSet\Services\DFServ" along with date/timestamps of starting. The application Deep Freeze service consists of three running processes: "DFServ.exe", which is the parent process and 2 more processes "DFLocker64.exe" and "FrzState2k.exe", which are the child processes. The amount of memory allocated to Deep Freeze is seen to be 16,292K out of which the process is using 11,336K.

4.4 Analysis using Windows Task Manager

Windows Task Manager is a facility, which enables a user to view and monitor applications, processes and services currently running in the computer system [10]. On examination and analysis of the running processes, services and applications in the virtual machine, it is observed and noted that Deep Freeze Service (32-bit) and Deep Freeze Utility (32-bit) are the background processes running (highlighted in red), as shown in Fig. 5.



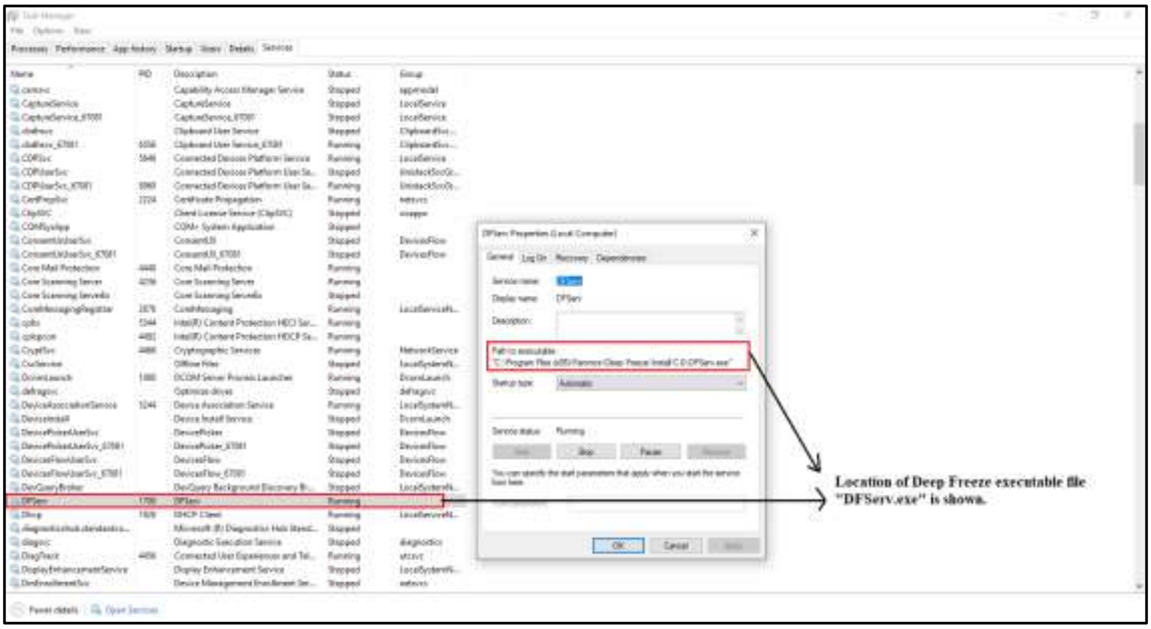
Deep Freeze Service and Deep Freeze Utility, running as background processes

Figure 5: Snapshot of Windows Task Manager showing Deep Freeze running as background process.

On performing further analysis, the full path or location of the executable file of Deep Freeze “DFServ.exe” inside the virtual machine could be found as well (highlighted in red), as shown in Fig. 6.

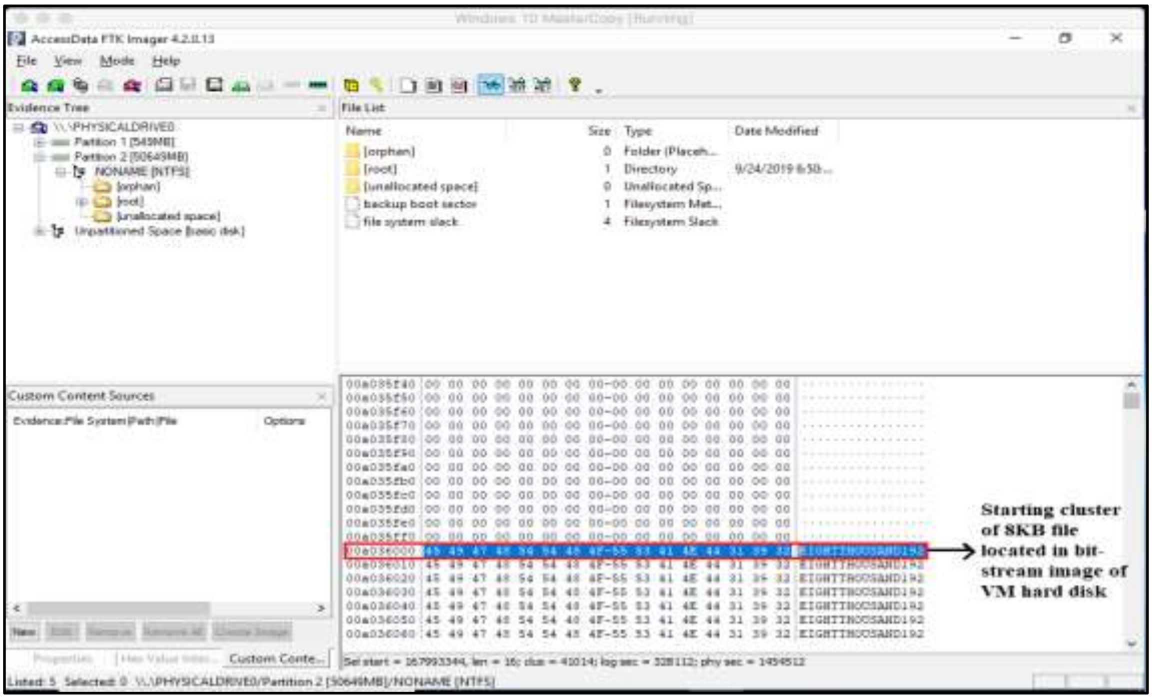
4.5 Imaging and Analysis of non-volatile data using FTK Imager

Different text files of sizes 4KB, 8KB, 12KB and 16KB respectively, are created and stored in the location “C:\Users\Windows10\Desktop” and the bit-stream image of the entire physical hard disk of the running virtual machine is captured and analysed using FTK Imager. On analysis of the image, it is found that the starting and ending clusters of the text file could be located (highlighted in red), along with recovery of the entire content of the file [5], as shown in Fig. 7 and Fig. 8. This is observed to be true for all the text files.



Location of Deep Freeze executable file "DFServ.exe" is shown.

Figure 6: Snapshot of Task Manager showing the location of Deep Freeze executable file "DFServ.exe"



AccessData FTK Imager 4.2.0.13

Evidence Tree
- \\.\PHYSICALDRIVE0
  - Partition 1 [549MB]
  - Partition 2 [50649MB]
    - NONAME [NTFS]
      - [orphan]
      - [root]
      - [unallocated space]
  - Unpartitioned Space [basic disk]

File List

Name	Size	Type	Date Modified
[orphan]	0	Folder (Placeh...	
[root]	1	Directory	9/24/2019 6:50...
[unallocated space]	0	Unallocated Sp...	
backup boot sector	1	Filesystem Met...	
file system slack	4	Filesystem Slack	

```
00a035f40  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00a035f50  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00a035f60  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00a035f70  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00a035f80  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00a035f90  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00a035fa0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00a035fb0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00a035fc0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00a035fd0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00a035fe0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00a035ff0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  ................
00a036000  45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32  EIGHTTHOUSAND192
00a036010  45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32  EIGHTTHOUSAND192
00a036020  45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32  EIGHTTHOUSAND192
00a036030  45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32  EIGHTTHOUSAND192
00a036040  45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32  EIGHTTHOUSAND192
00a036050  45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32  EIGHTTHOUSAND192
00a036060  45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32  EIGHTTHOUSAND192
```

Sel start = 167993344, len = 16; clus = 41014; log sec = 328112; phy sec = 1454512

Listed: 5 Selected: 0 \\.\PHYSICALDRIVE0/Partition 2 [50649MB]/NONAME [NTFS]

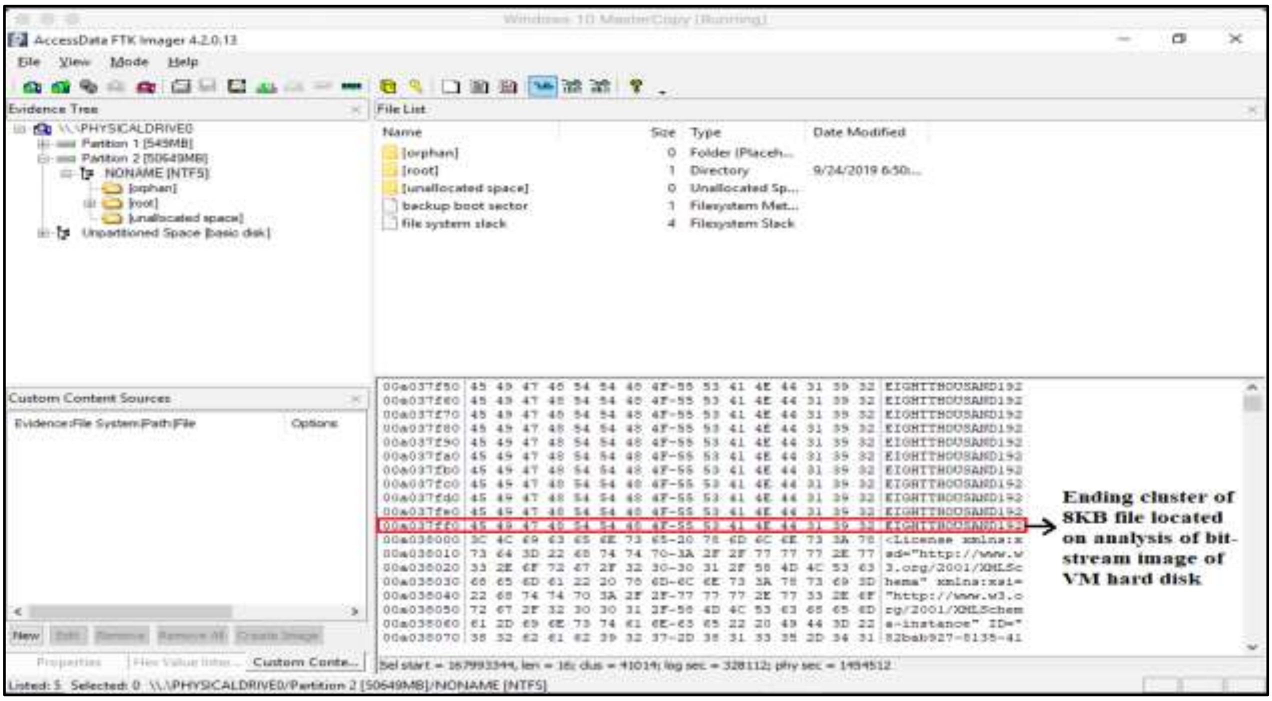
Starting cluster of 8KB file located in bit-stream image of VM hard disk

Figure 7: Starting cluster and sector of 8KB text file located on analysis of forensic image of the virtual machine hard disk, using FTK Imager

Similarly, larger files of size 4MB (4,194,304 bytes), which are created and stored in the same location ("C:\Users\Windows10\Desktop"), are also recovered from the bit-stream image of the virtual hard disk.

4.6 Analysis of Volatile and Non-volatile Evidences after Rebooting the Virtual Machine

On rebooting the virtual machine, the same set of forensic tools are used for collection of volatile evidences such as running processes, executables and DLLs. The result obtained shows that Deep Freeze is running in the background, thus having no deviation from previous results, as shown in Sections 4.1, 4.2, 4.3 and 4.4.



Name	Size	Type	Date Modified
[orphan]	0	Folder (Placeh...	
[root]	1	Directory	9/24/2019 6:50...
[unallocated space]	0	Unallocated Sp...	
backup boot sector	1	Filesystem Met...	
file system slack	4	Filesystem Slack	

Evidence:File System|Path|File Options

```
00a037f50 45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32 EIGHTTHOUSAND192
00a037f60 45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32 EIGHTTHOUSAND192
00a037f70 45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32 EIGHTTHOUSAND192
00a037f80 45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32 EIGHTTHOUSAND192
00a037f90 45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32 EIGHTTHOUSAND192
00a037fa0 45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32 EIGHTTHOUSAND192
00a037fb0 45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32 EIGHTTHOUSAND192
00a037fc0 45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32 EIGHTTHOUSAND192
00a037fd0 45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32 EIGHTTHOUSAND192
00a037fe0 45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32 EIGHTTHOUSAND192
00a037ff0 45 49 47 48 54 54 48 4F-55 53 41 4E 44 31 39 32 EIGHTTHOUSAND192
00a038000 3C 4C 69 63 65 6E 73 65-20 78 6D 6C 6E 73 3A 78 <License xmlns:x
00a038010 73 64 3D 22 68 74 74 70-3A 2F 2F 77 77 77 2E 77 sd="http://www.w
00a038020 33 2E 6F 72 67 2F 32 30-30 31 2F 58 4D 4C 53 63 3.org/2001/XMLSc
00a038030 68 65 6D 61 22 20 78 6D-6C 6E 73 3A 78 73 69 3D hema" xmlns:xsi=
00a038040 22 68 74 74 70 3A 2F 2F-77 77 77 2E 77 33 2E 6F "http://www.w3.o
00a038050 72 67 2F 32 30 30 31 2F-58 4D 4C 53 63 68 65 6D rg/2001/XMLSchem
00a038060 61 2D 69 6E 73 74 61 6E-63 65 22 20 49 44 3D 22 a-instance" ID="
00a038070 38 32 62 61 62 39 32 37-2D 38 31 33 35 2D 34 31 82bab927-8135-41
```

Sel start = 167993344, len = 16; clus = 41014; log sec = 328112; phy sec = 1454512

Listed: 5 Selected: 0 \\.\PHYSICALDRIVE0/Partition 2 [50649MB]/NONAME [NTFS]

Ending cluster of 8KB file located on analysis of bit-stream image of VM hard disk

Figure 8: Ending cluster and sector of 8KB text file, along with recovery of entire contents, located on the analysis of forensic image of the virtual machine hard disk, using FTK Imager

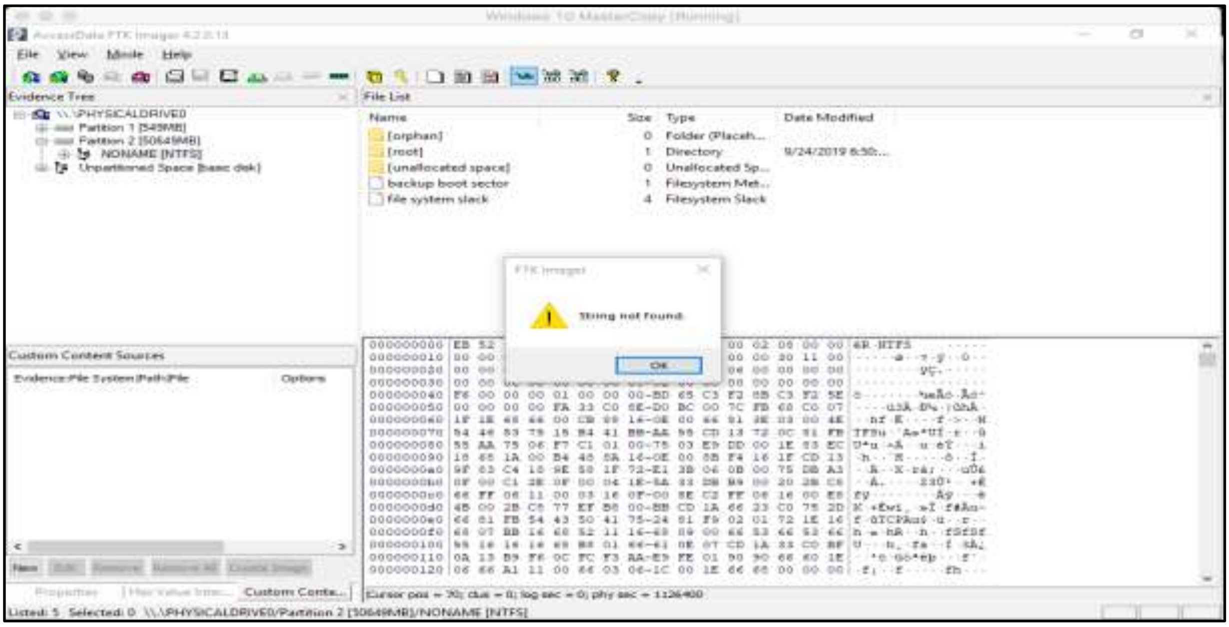
On rebooting the virtual machine, the different text files that were created and stored in the Desktop of the operating system, are not present at the same location anymore. Using FTK Imager, the virtual hard disk is again imaged and analysed, to search traces of the files, which were created and stored in the location "C:\Users\Windows10\Desktop". Following are the results achieved while trying to search and recover different types of text files:

a) In an attempt to recover the contents of smaller text files (size 4KB, 8KB or 12KB), no trace or artifacts related to the file is found during image analysis, using FTK Imager, as shown in Fig. 8.

b) In an attempt to recover larger file of size 4MB, while analysing the image of the virtual hard disk, it is found that traces of the file content could be recovered from few clusters i.e. 512 bytes of data found in cluster 10002293, 512 bytes of data found in cluster 10002294, 8704 bytes of data recovered from cluster 10002295 to 10002297, while 4608 bytes of data recovered from clusters 10002861 to 10002862. Hence, in total, around 14336 bytes of data could be recovered out of the entire file contents, which is 4MB (4,194,304 bytes) in size. On detailed calculation, it is observed that only 0.34% of the file contents is recoverable from the frozen virtual hard disk. Thus, less than 1%

of the entire file data is recovered, as shown in Fig. 9.

Forensic analysis of frozen hard disks using different digital forensic tools have shown that only few tools (for e.g. Winhex, Foremost etc.) are able to recover data, while other tools are not able to acquire any piece of data from the hard disk in which Deep Freeze has been installed [2]. The results of our experiment are somewhat similar to that performed by other researchers in the past, in that smaller sized files could be recovered through the use of forensic tools, whereas larger files could not be recovered once the virtual machine is rebooted. However, volatile evidence on deep freeze running in the background could be collected even after reboot. Therefore, our research on both volatile and non-volatile data in a virtual environment makes the overall results different from existing literature.



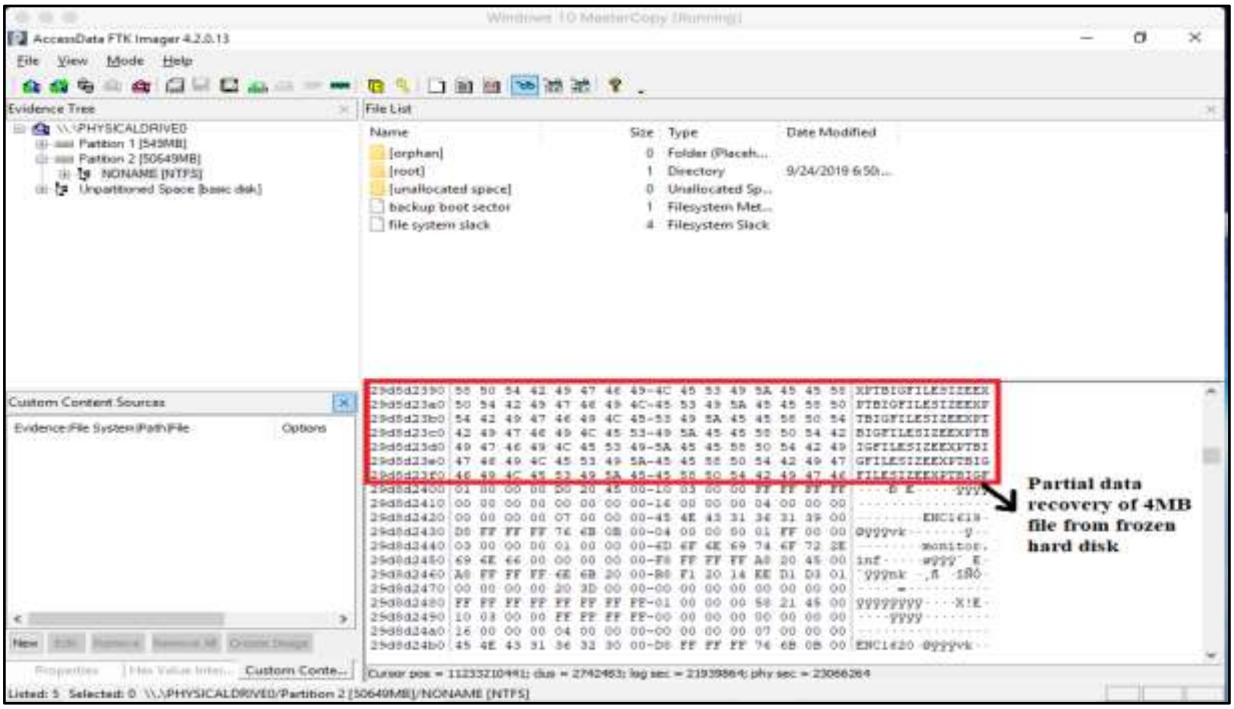
Name	Size	Type	Date Modified
[orphan]	0	Folder (Placeh...	
[root]	1	Directory	9/24/2019 6:50:...
[unallocated space]	0	Unallocated Sp...	
backup boot sector	1	Filesystem Met...	
file system slack	4	Filesystem Slack	

String not found

Cursor pos = 30; clus = 0; log sec = 0; phy sec = 1126400

Listed: 5 Selected: 0 \\.\PHYSICALDRIVE0/Partition 2 [50649MB]/NONAME [NTFS]

Figure 9: Text files not found on analysis of forensic image of virtual hard disk, using FTK Imager



Name	Size	Type	Date Modified
[orphan]	0	Folder (Placeh...	
[root]	1	Directory	9/24/2019 6:50:...
[unallocated space]	0	Unallocated Sp...	
backup boot sector	1	Filesystem Met...	
file system slack	4	Filesystem Slack	

```
29d8d2390 58 50 54 42 49 47 46 49-4C 45 53 49 5A 45 45 58  XPTBIGFILESIZEEX
29d8d23a0 50 54 42 49 47 46 49 4C-45 53 49 5A 45 45 58 50  PTBIGFILESIZEEXP
29d8d23b0 54 42 49 47 46 49 4C 45-53 49 5A 45 45 58 50 54  TBIGFILESIZEEXPT
29d8d23c0 42 49 47 46 49 4C 45 53-49 5A 45 45 58 50 54 42  BIGFILESIZEEXPTB
29d8d23d0 49 47 46 49 4C 45 53 49-5A 45 45 58 50 54 42 49  IGFILESIZEEXPTBI
29d8d23e0 47 46 49 4C 45 53 49 5A-45 45 58 50 54 42 49 47  GFILESIZEEXPTBIG
29d8d23f0 46 49 4C 45 53 49 5A 45-45 58 50 54 42 49 47 46  FILESIZEEXPTBIGF
29d8d2400 01 00 00 00 D0 20 45 00-10 03 00 00 FF FF FF FF  ····Ð E·····ÿÿÿÿ
29d8d2410 00 00 00 00 00 00 00 00-14 00 00 00 04 00 00 00  ················
29d8d2420 00 00 00 00 07 00 00 00-45 4E 43 31 36 31 39 00  ········ENC1619·
29d8d2430 D8 FF FF FF 76 6B 0B 00-04 00 00 00 01 FF 00 00  Øÿÿÿvk·······ÿ··
29d8d2440 03 00 00 00 01 00 00 00-6D 6F 6E 69 74 6F 72 2E  ········monitor.
29d8d2450 69 6E 66 00 00 00 00 00-F8 FF FF FF A8 20 45 00  inf·····øÿÿÿ¨ E·
29d8d2460 A8 FF FF FF 6E 6B 20 00-B8 F1 20 14 EE D1 D3 01  ¨ÿÿÿnk ·¸ñ ·îÑÓ·
29d8d2470 00 00 00 00 20 3D 00 00-00 00 00 00 00 00 00 00  ···· =··········
29d8d2480 FF FF FF FF FF FF FF FF-01 00 00 00 58 21 45 00  ÿÿÿÿÿÿÿÿ····X!E·
29d8d2490 10 03 00 00 FF FF FF FF-00 00 00 00 00 00 00 00  ····ÿÿÿÿ········
29d8d24a0 16 00 00 00 04 00 00 00-00 00 00 00 07 00 00 00  ················
29d8d24b0 45 4E 43 31 36 32 30 00-D8 FF FF FF 76 6B 0B 00  ENC1620·Øÿÿÿvk··
```

Cursor pos = 11233210441; clus = 2742483; log sec = 21939864; phy sec = 23086264

Listed: 5 Selected: 0 \\.\PHYSICALDRIVE0/Partition 2 [50649MB]/NONAME [NTFS]

Figure 10: Partial Data recovery (from few clusters) of large text files from forensic image of frozen hard disk, using FTK Imager

5 APPLICABILITY OF RESEARCH WORK

The results achieved from performing different experiments are applied in formulation of best practices for handling of computer systems (at the scene of crime) involving frozen virtual hard disks. The suggested best practices are given as follows:

a) The volatile data should be acquired from the virtual machine as per the order of volatility.

b) Digital forensic tools such as Process Explorer (SysInternals Suite), Win Audit (Helix Incident Response) or Task Manager can be used to capture the running processes to ascertain whether Deep Freeze software is running in the background.

c) A bit-stream imaging of the physical hard disk of the virtual machine should be done using tools like FTK Imager so as to recover non-volatile data, which would otherwise be lost as soon as the machine is shutdown or rebooted.

d) As the traditional techniques of disk forensics will not yield any evidentiary data, a videography (along with generation of hash values of the video file) and documentation of all the activities performed by the forensic examiner on the suspect machine, should be a part of the search and seizure procedure.

In addition to the suggested best practices, an examination and analysis of both the live captured bit-stream image of the virtual machine hard disk and the bit-stream image of the physical hard disk of the host computer system should also be performed, as a part of traditional forensic examination procedure.

6. CONCLUSION AND FUTURE SCOPE

This research work has been conducted with the aim of performing a forensic analysis of virtual machine hard disk, which is frozen using Faronics Deep Freeze software. Based on the results best practices for handling computer systems with frozen virtual hard disks, have been suggested. Deep Freeze software is installed successfully in Windows operating system in a virtual machine. Following this, digital forensic tools are used for collection of volatile evidences such as running and background processes, last user activities etc. in order to determine whether or not deep freeze is running in the background. Different types of files (small-sized and large-sized) are created and stored in the frozen partition and imaging of virtual hard disk is done and analysed, both before and after rebooting the virtual machine.

Based on the results of the experiments, several important conclusions, related to frozen virtual hard disks, can be drawn. Faronics Deep Freeze software can be considered as a startup process, which initiates execution on reboot and runs in the background as long as computer system is working, thus keeping the hard disk in frozen state and preventing any inadvertent changes to it. Apart from volatile artifacts, non-volatile data stored in the VM hard disk can also become volatile in nature unless acquired while the virtual machine is in live running condition. An attempt to acquire the same using traditional techniques of disk forensics (imaging and analysis), results in recovery of less than 1% of the file data for 4MB files and no data can be recovered for smaller files with size ranging from 4KB to 16KB.

Therefore, from anti-forensics point-of-view, Deep Freeze is very effective, resulting in restoration of operating system in user-configured state on every reboot and thus making data recovery from frozen virtual hard disks a difficult task. It is indeed a big challenge for forensic experts and practitioners to delve with incidents of cyber-crime involving frozen virtual hard disks, as evidence acquisition phase might not yield expected results. However, following the suggested best practices would be useful in unearthing of evidentiary data from both the virtual machine (having frozen hard disk) as well as the host computer system.

The research can be extended in future by using more files and documents of different sizes in order to achieve a more generalized result on data recovery. Using larger number of files of different file sizes would be useful in finding out whether or not data can be recovered from frozen hard disks of virtual machine. If data recovery is possible, then it would be essential to determine the amount of data that can be recovered and whether or not the data is recovered from the same location of a virtual hard disk as that in a physical hard disk. The working of Deep Freeze in reverting the operating system to user-configured state could also be a primary objective of future research. This would allow for the formulation of more appropriate and effective best practices useful for forensic examiners in handling cases involving both physical and virtual frozen hard disks.

7. REFERENCES

1. Riadi I., Umar R., Nasrulloh I.M., “Experimental Investigation of Frozen Solid-State Drive on Digital Evidence with Static Forensic Methods”, Lontar Komputer, Vol. 9, No. 3, pp. 169-181, (2018). DOI: 10.24843/LKJITI.2018.v09.i03.p06
2. Albana F., Riadi I., “Forensic Analysis of Frozen Hard Drive using Static Forensic Method”, International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No.1, pp. 173-178, (2017).
3. Scarboro T., “Forensics Steady State”, DigitalCommons@URI, University of Rhode Island, (2014).
4. White S., Mullis E., “Windows Ultimate Forensics Outflow concept and design: Introduction and User Manual”, (2012-2013).
5. Nabity P., Landry B.J., “Recovering Deleted and Wiped Files: A Digital Forensic Comparison of FAT32 and NTFS File Systems using Evidence Eliminator”, SWDSI, (2013).
6. “e-fense: Helix Incident Response”, Available at www.efense.com
7. “Microsoft SysInternals Suite”, Available at https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite
8. “FTK Imager version 3.2.0”, Available at www.accessdata.com
9. “Deep Freeze Enterprise- Faronics”, Available at www.faronics.com
10. Russinovich M., Solomon D., Ionescu A., “Windows Internals-Part 1 6th Edition”, Microsoft Press, Redmond-Washington, (2012).
11. Beer R., Stander A., Belle JP.: Anti-Forensics: A Practitioner Perspective. In: International Journal of Cyber-Security and Digital Forensics, vol. 4, issue 2, pp 390-403, SDIWC (2015).
12. Raychaudhuri K.: A Comparative Study of the Analysis and Extraction of Digital Forensic Evidences from exhibits using Disk Forensic Tools. In: International Journal of Cyber-Security and Digital Forensics, vol. 8, issue 3, pp 194-205, SDIWC (2019).