International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 02 February 2024
Page No: 327 - 332
https://irjaeh.com

Digital Forensics and Windows Sandbox as Anti-forensics tool

*Mohammed Yousuf uddin[1], Mohammad Mazhar Afzal[2], Sultan Ahmad[3]

[1,2] Computer Science, Glocal University, Saharanpur, Uttar Pradesh, India.

[3]University Center for Research and Development (UCRD), Department of Computer Science and Engineering, Chandigarh University, Punjab, India.

Email id: mdyousufuddin@gmail.com[1], mazhar.afzal @gmail.com[2], sultan.14nov@gmail.com[3]

***Corresponding Author Orcid ID:** https://orcid.org/0000-0002-3220-9541

Abstract

Digital forensics is facing new challenges with rise in new anti-forensics techniques and tools including virtualization. Virtualization can be used as shield against different types of attacks, at the same time it can be leveraged by attackers as anti-forensics tool. Forensic investigators face enormous challenges while collecting the digital evidences in case where virtualization is used by an attacker. Virtualization comes in different forms, one of the difficulty form is light weight virtualization. Microsoft windows operating system offers sandbox light weight virtualization. Microsoft windows sandbox is an isolated testing environment to run programs or open files without affecting the application, system, or platform on which they run. After closing the sandbox nothing persists on the device, everything is discarded. This paper reveals the anti-forensics capabilities of sandbox and possible solutions to collect the forensics artefacts using windows registry. Registry analysis revealed that only use of sandbox on host operating system is discoverable and activities and data inside the sandbox are discarded permanently.

Keywords: *Windows sandbox, digital forensics, anti-forensics, virtualization, disposable virtual machines.*

1. Introduction

Digital forensics is the process of collecting, preserving, and analyzing digital evidence. Digital evidence can be [1] used to investigate a variety of crimes, including computer intrusions, malware infections, and intellectual property theft. The digital forensics process completes in four key phases; Collection, Examination, Analysis, and Reporting [2]. Figure 1 illustrates the digital forensic process proposed by NIST. The NIST definition of digital forensics is "Science of identifying, collecting, preserving, documenting, examining, and analyzing evidence from computer systems, the results of which may be relied upon in court" [3]. The data collection step involves obtaining data by copying it into an image, this phase aims to protect the data against unintentional modifications and guarantee the integrity of the acquired data through the utilization of cryptographic hashing. The examination phase combines forensic technologies, procedures, and manual processes to identify and extract pertinent evidence from the gathered data. The analysis phase involves the assessment of results in order to derive relevant details associated with the case. The final stage is generating reports that present the evidence derived from the findings of the analysis [4].

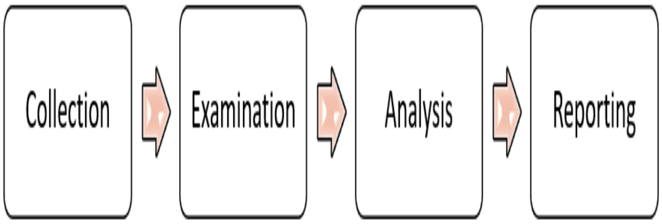


Figure 1 Digital Forensic phases

1.1 Virtualization

A virtual machine refers to a virtual representation, or emulation, of a physical computer. Virtual machines run on the host. On single host multiple virtual machines with their own operating system and application programs. Virtual machines runs on top of a software layer called hypervisor to coordinate with underlying physical hardware. Hypervisor is managing the resources between multiple virtual machines. Hypervisor implementation can be achieved in two ways basically, one hypervisor that directly placed on physical hardware it is referred as type-1 hypervisor and second is on top of host operating systems it is type-2 hypervisor. Type-1 hypervisors is also referred as bare metal hypervisors; examples include Citrix, Xen Server, ESXi from VMware, and Microsoft's Hyper-V. Layer architecture of type-1 hypervisor illustrated in Figure 2. Type-2 hypervisor runs as an application on top of the host operating system illustrated in Figure 3. Examples of type-2 hypervisors are VMware, Virtual Box, and Parallel Desktop for MAC OS. If compared type1 hypervisors offers security, performance and there is no overhead task for hypervisor to interact with host operating system as in type-2. Type-2 is convenient in emulating a different operating system other than their host OS such as Windows users can install and run Linux on virtual machine [5].

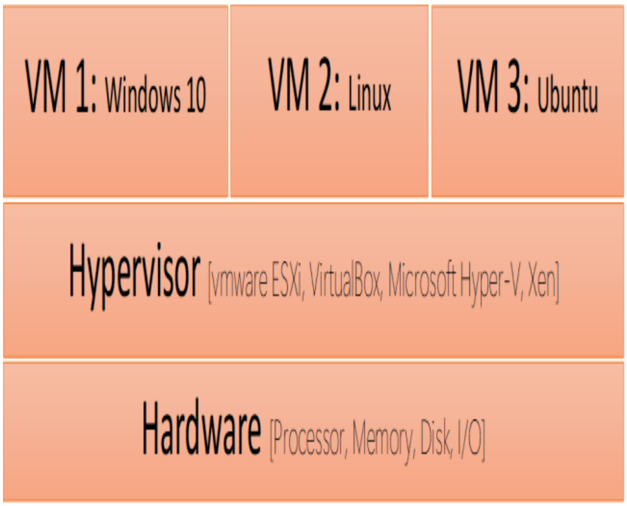

VM 1: Windows 10
VM 2: Linux
VM 3: Ubuntu
Hypervisor [vmware ESXi, VirtualBox, Microsoft Hyper-V, Xen]
Hardware [Processor, Memory, Disk, I/O]

Figure 2 Type-1 Hypervisor

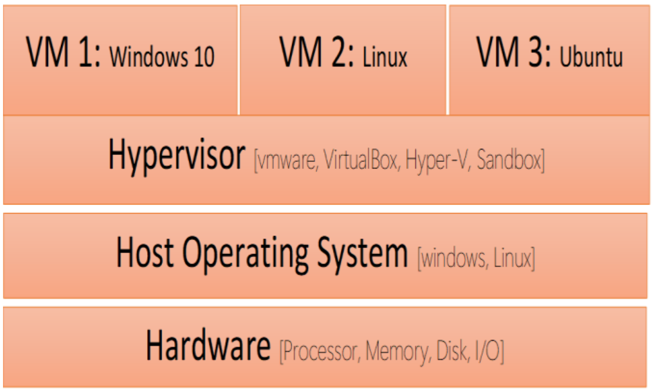

VM 1: Windows 10
VM 2: Linux
VM 3: Ubuntu
Hypervisor [vmware, VirtualBox, Hyper-V, Sandbox]
Host Operating System [windows, Linux]
Hardware [Processor, Memory, Disk, I/O]

Figure 3 Type-2 Hypervisor

1.2 Light weight virtualization

Lightweight virtual machine is instantaneously created, after use as soon as it is closed it will be disposed so it is referred as disposable virtual machines. Disposable VMs commonly used to host single application, such as web browser, viewer, editor and suspicious applications. This concept of single use virtual machines also adopted by various operating systems. This disposable virtual environment gives isolated environment to test suspicious applications, malwares, and ransomwares without any impact on host operating systems. In Table 1, the few popular disposable Virtual machine managers are listed [6].

Table 1 Disposable Virtual Machines

Disposable VM	Hypervisor	Type
Microsoft windows Sandbox	Microsoft Hypervisor	Type-2
Qubes disposable VM	KVM, Xen	Type-1
QEMU	Xen, KVM, Hax	Type-2
Virtual box Nested VM	Virtual Box	Type-2
Shade SandBox	Microsoft Hypervisor	Type-1

1.3 Windows Sandbox

A sandbox is a light weight VM it is isolated testing environment. Sandbox allows users to run application programs or open files without affecting the application, system, or platform on which they run. Windows Sandbox runs the same OS image as the host, if it is windows 10 sandbox will be windows 10. It is designed to use some physical memory pages as the host. Software developers use sandboxes to test new programming code. Cybersecurity professionals use sandboxes to test potentially malicious software. Malicious code in sandboxes executes safely without harming the host device, the network, or other connected devices. Using a sandbox to detect malware gives protection against security threats, such as stealthy attacks and exploits that use zero-day vulnerabilities. Sandbox is a type of disposable VM. Windows Sandbox has the following properties: Part of Windows: Everything required for this feature is included in Windows 10 and Windows 11 Pro and Enterprise. There's no need to download a VHD.

Pristine: Each instance of Windows Sandbox runs is clean as a brand-new installation of Windows.

Disposable: Everything is discarded when the user closes the sandbox; nothing persists on the host device.

Secure: Hardware-based virtualization provides kernel isolation. Microsoft hypervisor run a separate kernel that isolates Windows Sandbox from the host.

Efficient: Integrated kernel scheduler, smart memory management, and virtual GPU provide efficient execution of sandbox. [7]

2. Experimental Setup

Objective of this experiment is to find the evidences after sandbox is used. In this study registry is compared before and after windows sandbox usage. Whole experiment is performed in seven steps as shown in Figure 4. First step is setting up windows sandbox on windows 11 operating system. Second step is to download and start registrychangesview tool from Nirsoft. Step 3 starts the Windows sandbox. Step 4 complete the activities show in Table 2. Step 5 copies the registry after closing the sandbox. Step 6 compares the two copies of the registry to find any changes before and after running the sandbox.

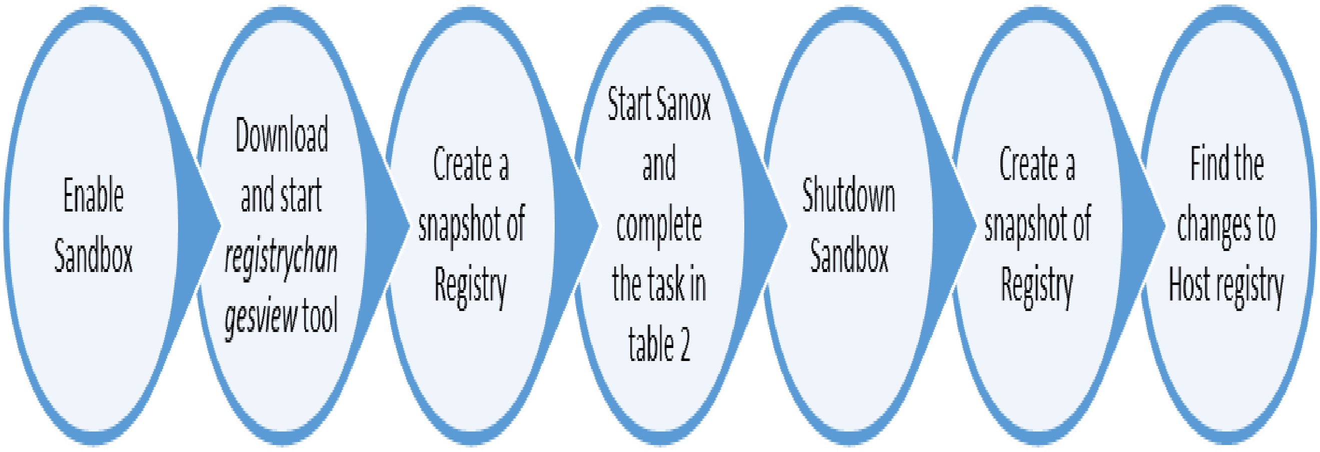

Enable Sandbox
Download and start registrychangesview tool
Create a snapshot of Registry
Start Sanox and complete the task in table 2
Shutdown Sandbox
Create a snapshot of Registry
Find the changes to Host registry

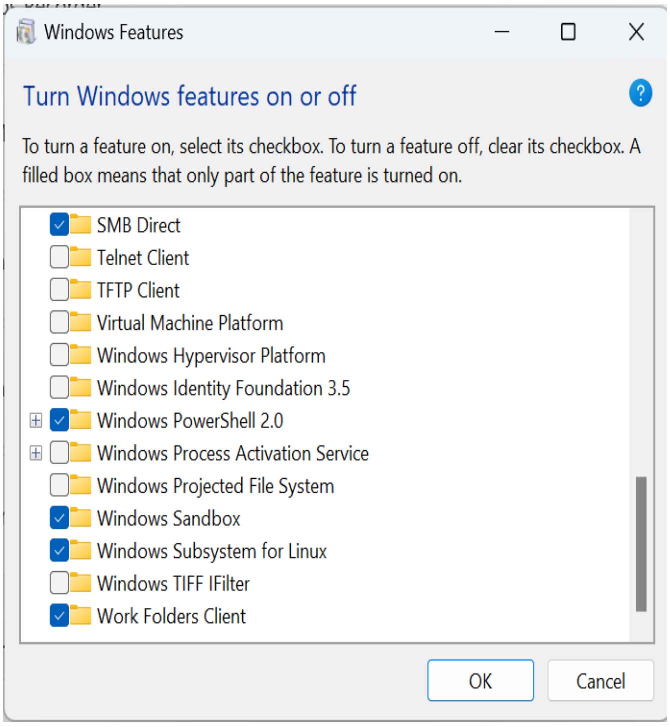
Figure 4 **Steps in Experiment**

2.1 Sandbox Setup

Windows sandbox first introduced in windows 10 Pro versions 1903. Windows 11 Pro, Enterprise and education edition includes Windows sandbox with added feature, where your data will persist after restart initiated from inside the virtualized environment after installing the application that require the OS to reboot [8]. After installing windows Operating System sandbox should be enabled by entering windows settings-system-optional features as shown in Figure 5.

2.2 Registry Snapshots

To compare the registry before and after windows sandbox registrychangesview tool is downloaded from Nrisoft website [9]. Step 2 and step 3 is completed by taking the snapshots of the registry before and after windows sandbox activities listed in Table 2. Registry snapshot is illustrated in Figure 7. Windows registry is the database to store information required to configure users, application and hardware devices. Registry is used continuously during operations on [11] user profile, contains information related to applications installed and types of documents that each application can create, folders and application icons settings, what hardware exists on the system, and the ports that are being used. Windows registry is organized in to hives and each hive consists of group of keys, sub keys and values [10].



Windows Features

Turn Windows features on or off

To turn a feature on, select its checkbox. To turn a feature off, clear its checkbox. A filled box means that only part of the feature is turned on.

☑ SMB Direct
□ Telnet Client
□ TFTP Client
□ Virtual Machine Platform
□ Windows Hypervisor Platform
□ Windows Identity Foundation 3.5
⊞ ☑ Windows PowerShell 2.0
⊞ □ Windows Process Activation Service
□ Windows Projected File System
☑ Windows Sandbox
☑ Windows Subsystem for Linux
□ Windows TIFF IFilter
☑ Work Folders Client

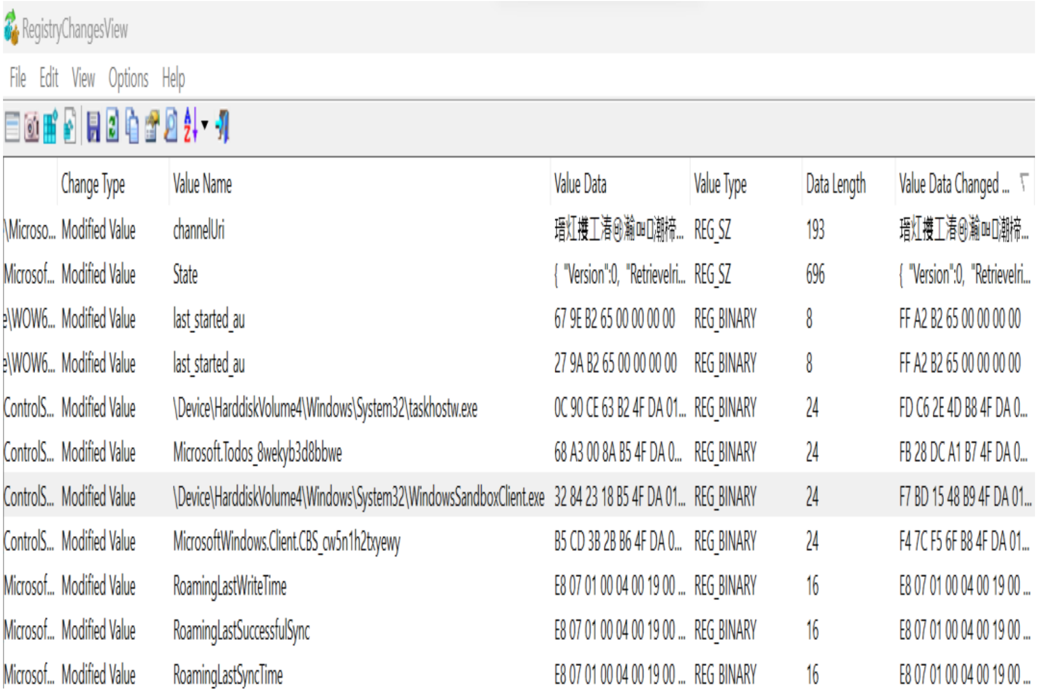
Figure 5 **Enable Windows Sandbox**

Table 2 **Activities to Complete in Sandbox**

Activity in Sandbox	**Outcome**
Install Application	Acrobat Reader Installed
Create File	A notepad file created
Start command Line console	Executed networking command 'ipconfig'
Copy a file from host to Sandbox	A pdf file copied from host to sandbox
Browse internet	Edge browser start for browsing news channels

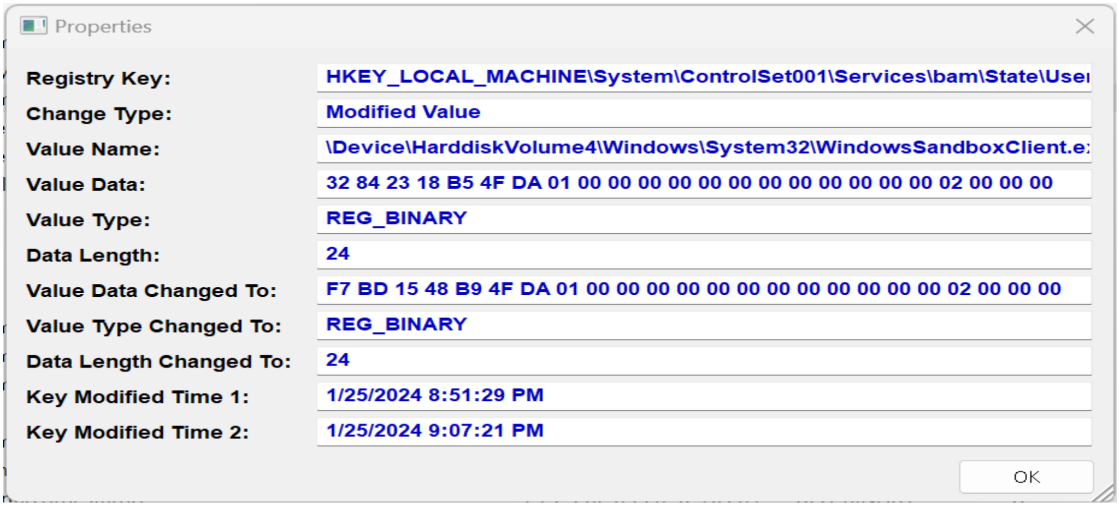
2.3 Forensics Analysis of Windows Sandbox

Windows sandbox is the basic copy of your host Windows operating system without any applications except Microsoft [14] Edge, Explorer and Windows defender firewall is enabled. Third-party anti malware programs can be installed. Files can be copied to and from the guest and host using copy and paste but drag [12] and drop does not work. Mouse cursor and keyboard commands work smoothly on guest image and the host seamlessly. The sandbox access the Internet through virtual Ethernet interface installed on [13] both the guest and the host. Applications which required user account control cannot be installed. In this experiment windows sandbox is started on windows 11 pro after performing the activities show in table 2 it is closed. [15] Forensics analysis of registry is performed by comparing the registry snapshots of before and after windows sandbox usage, Figure 6 shows the Sandbox entry in registry and Figure 7 shows the registry key values of sandbox. It is found after comparing the registry files that evidence of Windows sandbox [16] execution is available but activates performed inside the sandbox are untraced through registry.



	Change Type	Value Name	Value Data	Value Type	Data Length	Value Data Changed ...
\Microso...	Modified Value	channelUri	瑨灯摟工渹⑩瀚ㅁ潮梯...	REG_SZ	193	瑨灯摟工渹⑩瀚ㅁ潮梯...
Microsof...	Modified Value	State	{ "Version":0, "Retrievelri...	REG_SZ	696	{ "Version":0, "Retrievelri...
e\WOW6...	Modified Value	last_started_au	67 9E B2 65 00 00 00 00	REG_BINARY	8	FF A2 B2 65 00 00 00 00
e\WOW6...	Modified Value	last_started_au	27 9A B2 65 00 00 00 00	REG_BINARY	8	FF A2 B2 65 00 00 00 00
ControlS...	Modified Value	\Device\HarddiskVolume4\Windows\System32\taskhostw.exe	0C 90 CE 63 B2 4F DA 01...	REG_BINARY	24	FD C6 2E 4D B8 4F DA 0...
ControlS...	Modified Value	Microsoft.Todos_8wekyb3d8bbwe	68 A3 00 8A B5 4F DA 0...	REG_BINARY	24	FB 28 DC A1 B7 4F DA 0...
ControlS...	Modified Value	\Device\HarddiskVolume4\Windows\System32\WindowsSandboxClient.exe	32 84 23 18 B5 4F DA 01...	REG_BINARY	24	F7 BD 15 48 B9 4F DA 01...
ControlS...	Modified Value	MicrosoftWindows.Client.CBS_cw5n1h2txyewy	B5 CD 3B 2B B6 4F DA 0...	REG_BINARY	24	F4 7C F5 6F B8 4F DA 01...
Microsof...	Modified Value	RoamingLastWriteTime	E8 07 01 00 04 00 19 00 ...	REG_BINARY	16	E8 07 01 00 04 00 19 00 ...
Microsof...	Modified Value	RoamingLastSuccessfulSync	E8 07 01 00 04 00 19 00 ...	REG_BINARY	16	E8 07 01 00 04 00 19 00 ...
Microsof...	Modified Value	RoamingLastSyncTime	E8 07 01 00 04 00 19 00 ...	REG_BINARY	16	E8 07 01 00 04 00 19 00 ...

Figure 6 **Registry Entry of Sandbox**



Registry Key:	HKEY_LOCAL_MACHINE\System\ControlSet001\Services\bam\State\Usei
Change Type:	Modified Value
Value Name:	\Device\HarddiskVolume4\Windows\System32\WindowsSandboxClient.e:
Value Data:	32 84 23 18 B5 4F DA 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
Value Type:	REG_BINARY
Data Length:	24
Value Data Changed To:	F7 BD 15 48 B9 4F DA 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
Value Type Changed To:	REG_BINARY
Data Length Changed To:	24
Key Modified Time 1:	1/25/2024 8:51:29 PM
Key Modified Time 2:	1/25/2024 9:07:21 PM

Figure 7 **Registry Key for Windows Sandbox**

Conclusion

This study has evaluated the role of registry in collecting the evidence for sandbox. Windows sandbox on windows 11 is used and registrychangeview software to take the snapshots of the registry to compare the changes in the registry after using the sandbox. Evidence retrieval from registry is proven to be useful to detect the use of sandbox, but further details of activities performed inside the sandbox were not available. Potential artefacts can be retrieved through means are possible; network forensics could be one option to further collect the evidences.

References

[1] https://www.nist.gov/digital-evidence

[2] Dimitriadis, Athanasios, Nenad Ivezic, Boonserm Kulvatunyou, and Ioannis Mavridis. "D4I-Digital forensics framework for

reviewing and investigating cyber-attacks." Array 5 (2020): 100015.

[3] Kent, Karen, Suzanne Chevalier, and Tim Grance. "Guide to integrating forensic techniques into incident." Tech. Rep. 800-86 (2006).

[4] https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf

[5] Tobin, Patrick, and Tahar Kechadi. "Virtual machine forensics by means of introspection and kernel code injection." In Proceedings of the 9th International Conference on Cyber Warfare & Security: ICCWS, p. 294. 2014.

[6] Bhimani, Janki, Zhengyu Yang, Miriam Leeser, and Ningfang Mi. "Accelerating big data applications using lightweight virtualization framework on enterprise cloud." In 2017 IEEE High Performance Extreme Computing Conference (HPEC), pp. 1-7. IEEE, 2017.

[7] https://learn.microsoft.com/en-us/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-overview

[8] Bashir, Reem, Helge Janicke, and Wen Zeng. "Evaluating the impact of sandbox applications on live digital forensics investigation." (2021).

[9] Ahmad, Ijaz, Haider Abbas, Asad Raza, Kim-Kwang Raymond Choo, Anam Sajid, Maruf Pasha, and Farrukh Aslam Khan. "Electronic crime investigations in a virtualised environment: a forensic process and prototype for evidence collection and analysis." Australian Journal of Forensic Sciences 50, no. 2 (2018): 183-208.

[10] Singh, Avinash, Hein S. Venter, and Adeyemi R. Ikuesan. "Windows registry harnesser for incident response and digital forensic analysis." Australian Journal of Forensic Sciences 52, no. 3 (2020): 337-353.

[11] Binjuraid, Hasan, and Mazura Mat Din. "Case Based Interpretation of Windows 10 Registry Forensics." International Journal of Innovative Computing 8, no. 1 (2018).

[12] Ali, Muhammad, Stavros Shiaeles, Nathan Clarke, and Dimitrios Kontogeorgis. "A proactive malicious software identification approach for digital forensic examiners." Journal of Information Security and Applications 47 (2019): 139-155.

[13] Tobin, Patrick, Nhien-A Le-Khac, and Tahar Kechadi. "Forensic analysis of virtual hard drives." Journal of Digital Forensics, Security and Law 12, no. 1 (2017): 10.

[14] https://learn.microsoft.com/en-us/windows/security/application-security/application-isolation/windows-sandbox/windows-sandbox-overview

[15] https://learn.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users.

[16] https://www.nirsoft.net/utils/registry_changes_view.html.