A Review of Forensic Insight into Windows 10 - Windows Subsystem Linux (WSL)

Diwakar Yash Dilipkumar[1], Dr. Ravi K Sheth[2]
[1]M.Tech Cyber Security
[2]Assistant Professor, Dept of IT
[1, 2] Raksha Shakti University

Abstract- *The field of Digital Forensics is usually dynamic together with developments in hardware and operational systems. Windows Subsystem Linux, one of the new features introduced by Microsoft in Windows 10 operating system, is a new feature provided by Microsoft to integrate Linux kernel within the system. There's no need to install VMware or any other virtualization technology to use Linux in Windows environment. Being the platform comparatively new, the forensic examination of Windows Subsystem has been largely unexplored in the literature. This paper seeks to work out the data and information remnants of Windows Subsystem Linux in a Windows 10. The analysis contributes in-depth understanding of the location of evidentiary artifacts on the disk and the type of information recorded in these artifacts as a result of user activities on Windows Subsystem Linux-Ubuntu. Therefore, in this paper, we can demonstrate the Architecture provided by Microsoft and artifacts generated by Windows Subsystem Linux in the forensic context.*

Keywords- Windows Subsystem Linux, Digital Forensic, Windows Forensic, Cyber Forensic, Linux Forensic

I. INTRODUCTION

Microsoft recently released Bashof Ubuntu on Windows that allows native Linux ELF64 binaries to run on Windows via the Windows Subsystems for Linux (WSL). This approach is totally different from a conventional virtual machine. It is the outcome of the project of running POSIX Apps in minimal Picoprocess. [1]

Windows Subsystem Linux is not installing any emulator or Virtual Machine. Instead, it provides a layer to translate system calls in system. WSL is a collection of components that enables native Linux ELF64 binaries to run on Windows. It contains both user mode and kernel mode components. It primarily contains User mode session manager service, Pico provider drivers (lxss.sys, lxcore.sys), Pico processes, System Calls. VolFs and DriveFs are two types of file system which are responsible to provide file permissions, directories listing and interoperability Windows. [2]

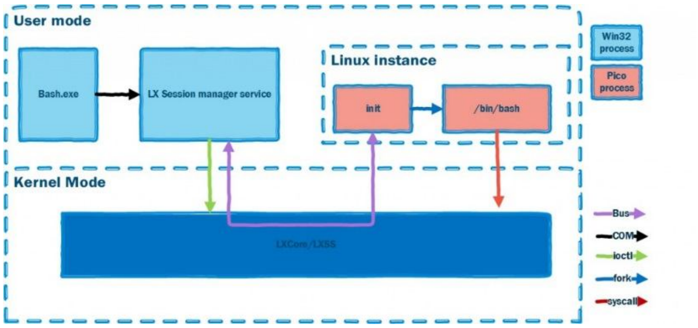
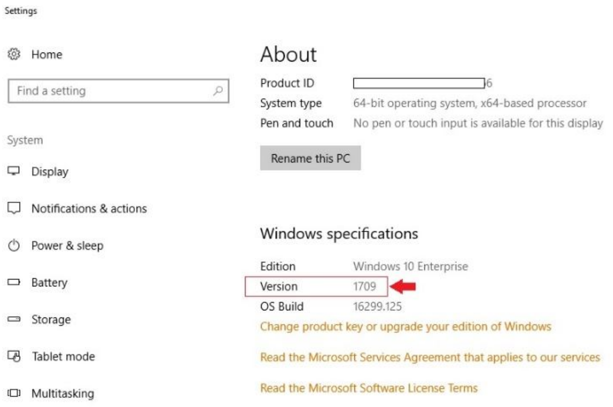


Fig.1 WSL Components

II. DOWNLOAD AND INSTALLATION

Windows Subsystem for Linux is an optional feature provided by Microsoft in Windows 10 Anniversary Updates. For this feature, you required 64-bit Windows 10. And check you have latest windows 10 version 1709 by going to Setting -> System -> About.



About

Product ID [redacted]6
System type 64-bit operating system, x64-based processor
Pen and touch No pen or touch input is available for this display

Windows specifications

Edition Windows 10 Enterprise
Version 1709
OS Build 16299.125

Change product key or upgrade your edition of Windows

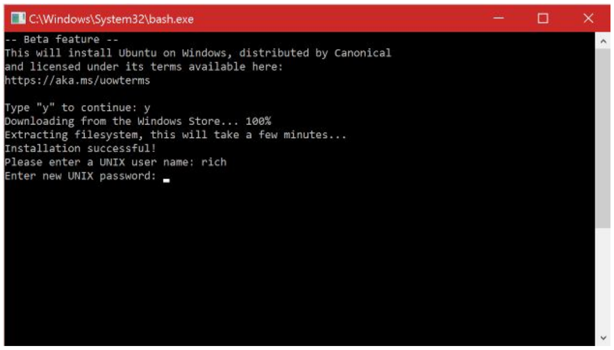
Read the Microsoft Services Agreement that applies to our services

Read the Microsoft Software License Terms

Fig.2 Requirements of WSL in OS

After that in PowerShell install WSL by using the command – "Enable-Windows Optional Feature -Online –Feature Name Microsoft-Windows-Subsystem-Linux" and also, we have to use Ubuntu from windows store after enabling the Developer mode from settings. [3]

You can get bash on windows 10 and create username and password for Linux.



```
-- Beta feature --
This will install Ubuntu on Windows, distributed by Canonical
and licensed under its terms available here:
https://aka.ms/uowterms

Type "y" to continue: y
Downloading from the Windows Store... 100%
Extracting filesystem, this will take a few minutes...
Installation successful!
Please enter a UNIX user name: rich
Enter new UNIX password: _
```

Fig.3 Linux User Creation Screen

III. PURPOSE AND SCOPE

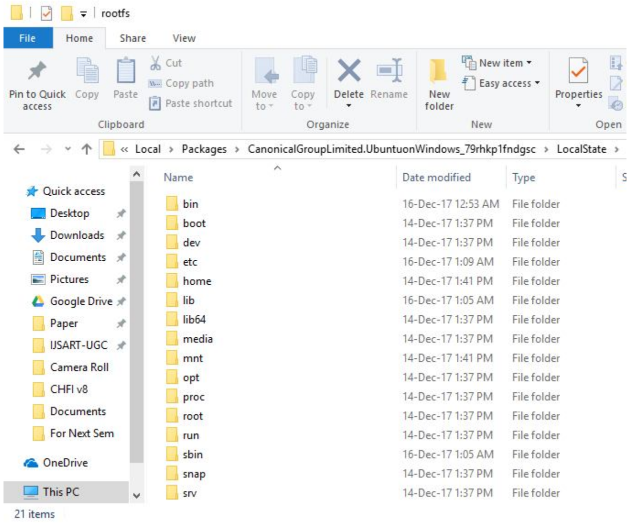
The main purpose behind Forensic Analysis of the Windows Subsystem Linux is to find and analyze attack vector. While this move makes easier for users who regularly use Windows and Linux systems, it looks like a replacement technique that leverages WSL may permit attackers to bypass security solutions installed within the user's system. Check Point Discover technique called "Bashware" which affect the system who run on Windows 10 Anniversary updates. It abuses the wsl foundation "Pico Processes" Attackers that use the Bashware technique will first load WSL elements on the target system, and change to developer mode. Bashware can then transfer and extract Linux from Microsoft's servers, the last step within the method involves the installation of Wine, that permits Windows applications to run on UNIX-based operative systems. The attacker will then use Windows malware to infect the system, whereas rendering them undetectable by ancient security software by initiating them via picoprocesses. [4]
So it is important to analysis WSL in the forensic context.

IV. METHODOLOGY

In this we have firstly install WSL – Ubuntu on the Windows 10 version 1709 and find out the forensic artifacts generated by windows subsystem Linux.

V. FORENSIC ARTIFACTS

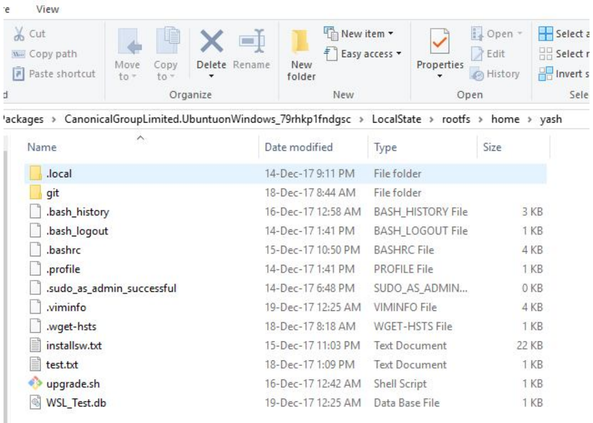
In the first step for the forensic analyst to identify whether target machine contains WSL or not. Enabling Windows subsystem for Linux and installing one of the accessible user land offerings causes a large number of changes to a system. There are the variety of things you will look out for to substantiate its installation. the best indicator of WSL being installed for a minimum of one user is that the presence of the Bash executable at %systemroot%\System32\bash.exe. In another method, the changes in the registry of windows prove the presence of WSL in the system. In windows, 10 version 1709 contain the registry: 'HKLM\COMPONENTS\CanonicalData'. You can install WSL for individual user created by windows. This is often of particular importance as we glance to forensically fascinating artifacts. On a multiuser system, every Windows user has to install Bash independently, the associated filesystem is inside the user's %localappdata% location and notable registry keys are keep inside their NTUser.dat. After, on disk you'll additionally look out for the presence of the Linux filesystem, for every individual user placed at: 'C:\Users\[Username]\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc\LocalState\rootfs'.[5]



Name	Date modified	Type
bin	16-Dec-17 12:53 AM	File folder
boot	14-Dec-17 1:37 PM	File folder
dev	14-Dec-17 1:37 PM	File folder
etc	16-Dec-17 1:09 AM	File folder
home	14-Dec-17 1:41 PM	File folder
lib	16-Dec-17 1:05 AM	File folder
lib64	14-Dec-17 1:37 PM	File folder
media	14-Dec-17 1:37 PM	File folder
mnt	14-Dec-17 1:41 PM	File folder
opt	14-Dec-17 1:37 PM	File folder
proc	14-Dec-17 1:37 PM	File folder
root	14-Dec-17 1:37 PM	File folder
run	14-Dec-17 1:37 PM	File folder
sbin	16-Dec-17 1:05 AM	File folder
snap	14-Dec-17 1:37 PM	File folder
srv	14-Dec-17 1:37 PM	File folder

Fig.4 Linux Files can be accessible via windows explorer

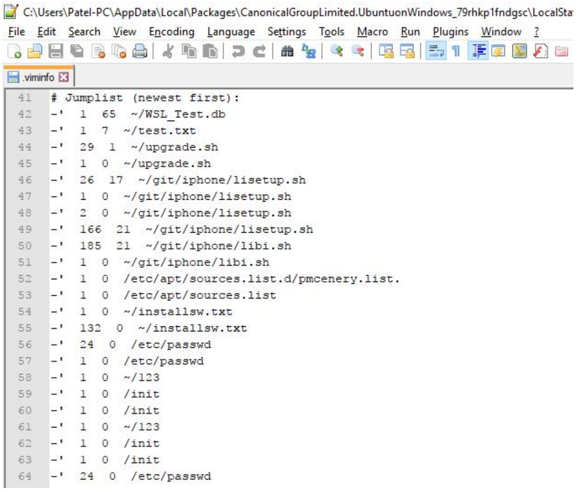
Also file which are made from WSL can be easily access from the windows explorer in: 'C:\Users\Patel-PC\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc\LocalState\rootfs\home\[Username]



Name	Date modified	Type	Size
.local	14-Dec-17 9:11 PM	File folder	
git	18-Dec-17 8:44 AM	File folder	
.bash_history	16-Dec-17 12:58 AM	BASH_HISTORY File	3 KB
.bash_logout	14-Dec-17 1:41 PM	BASH_LOGOUT File	1 KB
.bashrc	15-Dec-17 10:50 PM	BASHRC File	4 KB
.profile	14-Dec-17 1:41 PM	PROFILE File	1 KB
.sudo_as_admin_successful	14-Dec-17 6:48 PM	SUDO_AS_ADMIN...	0 KB
.viminfo	19-Dec-17 12:25 AM	VIMINFO File	4 KB
.wget-hsts	18-Dec-17 8:18 AM	WGET-HSTS File	1 KB
installsw.txt	15-Dec-17 11:03 PM	Text Document	22 KB
test.txt	18-Dec-17 1:09 PM	Text Document	1 KB
upgrade.sh	16-Dec-17 12:42 AM	Shell Script	1 KB
WSL_Test.db	19-Dec-17 12:25 AM	Data Base File	1 KB

Fig.5 File created in the home directory.

The records maintained by Jump Lists have the potential to supply a rich source of proof concerning users' historic activity to the forensic investigator. The structure and artifacts recorded by Jump Lists are widely mentioned in varied forensic communities since its debut in Microsoft Windows 7. However, this feature has a lot of capabilities to reveal proof in Windows 10, because of its modified structure. Activity timeline made over an amount of your time using Jump Lists. [6] So in WSL the directory containing the home user's data has file .viminfo which records the Jump Lists, which can easily accessible by the text editor.


C:\Users\Patel-PC\AppData\Local\Packages\CanonicalGroupLimited.UbuntuonWindows_79rhkp1fndgsc\LocalSta
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
.viminfo

```
# Jumplist (newest first):
-'  1  65  ~/WSL_Test.db
-'  1  7  ~/test.txt
-'  29  1  ~/upgrade.sh
-'  1  0  ~/upgrade.sh
-'  26  17  ~/git/iphone/lisetup.sh
-'  1  0  ~/git/iphone/lisetup.sh
-'  2  0  ~/git/iphone/lisetup.sh
-'  166  21  ~/git/iphone/lisetup.sh
-'  185  21  ~/git/iphone/libi.sh
-'  1  0  ~/git/iphone/libi.sh
-'  1  0  /etc/apt/sources.list.d/pmcenery.list.
-'  1  0  /etc/apt/sources.list
-'  1  0  ~/installsw.txt
-'  132  0  ~/installsw.txt
-'  24  0  /etc/passwd
-'  1  0  /etc/passwd
-'  1  0  ~/123
-'  1  0  /init
-'  1  0  /init
-'  1  0  ~/123
-'  1  0  /init
-'  1  0  /init
-'  24  0  /etc/passwd
```

Fig.6 Jump List store in .viminfo

By using WSL user can easily install multiple flavors of Linux which is available on windows Store such as Ubuntu, openSUSELeap, SUSELinuxEnterpriseServer. All the installed flavors of Linux make significant changes in the registry. So we can detect the distro via a registry. Analysis of the contents of the HKEY_CURRENT_USER\ Software\Microsoft\Windows\CurrentVersion\Lxss key can permit you to spot the different Linux flavors presently installed for any specific user. For that distro_guid keys you may observe:

{b651c2ea-ab01-46ae-8c95-09209e4272fd} - SLES-12
{d4085d24-9def-43b3-9a17-de87d9bba371} - openSUSE-42
{ff9afada-c0e4-4c9c-ac50-e5fb13b4b142} - Ubuntu

VI. FUTURE WORK

More than 100 system calls that can now result in possible local privilege escalation. If you have configured the firewall on your system but still Ubuntu of WSL can access full network. Also, it provides full disk access. Windows software could modify the Linux apps and vice versa, which provided new routes for exploitation. So, in future tools or scripts to be developed that can easily detect the WSL system and identify memory content. There need more work to be done in the filesystem - DriveFs and VolFs used by WSL.

VII. CONCLUSION

In this review paper we have concluded that the WSL provide great access and privileges to the user on the filesystem. Also, we can easily locate the location where WSL- Ubuntu is installed. As forensic prospective it supports various forensic tools but need to configure according to flavors of Linux. To access the history and other files generates by using of WSL we can simply use Windows File explorer.

REFERENCES

[1] https://www.microsoft.com/en-us/research/wp-content/uploads/2013/01/posix-emulation-submitted.pdf

[2] https://blogs.msdn.microsoft.com/wsl/2016/04/22/windows-subsystem-for-linux-overview/

[3] https://media.readthedocs.org/pdf/wsl-guide/latest/wsl-guide.pdf

[4] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/bashware-attack-targets-windows-system-for-linux-wsl

[5] http://blog.1234n6.com/2017/10/windows-subsystem-for-Linux-and.html

[6] A forensic insight into Windows 10 Jump Lists, Bhupendra Singh, Upasna Singh, In Digital Investigation, Volume 17, 2016, Pages 1-13, ISSN 1742-2876, https://doi.org/10.1016/j.diin.2016.02.001. (http://www.sciencedirect.com/science/article/pii/S1742287616300202)