# An Introduction to Windows Forensics & Tools

**Danny, Ryan, Brandon**

**Computer Forensics**

**Dr. Omar**

**11-1-18**

# Abstract

The forensic investigator should ideally look into a number of different places, but this report will cover three major locations to look: Windows Directory/Folder, Windows Registry, and the Window's logs. The Windows Directory/Folder is interesting because a number of different documents can be found including Downloads, Word Documents, and installed applications. The Windows registry is a hierarchical database that stores the configuration settings for all hardware and software. The important key to the Windows registry is that it can help the investigator look at the configurations of the system without having to look at each item specifically on the system. Finally, the logs are important because it is a central location that the Operating System puts data into regarding errors that have occurred within hardware and software. The logs can then be put into a report for the investigator to look into.

# Introduction

The Microsoft Windows operating system has evolved from its original use of being a graphical user interface (GUI) for DOS to be a fully operational operating system that currently dominates the world with the amount of user's it has on its platform. It is due to this popularity that many forensic investigators should be knowledgeable in this operating system. The Windows operating system has a number of different locations that can be important to a forensic investigator, but only the Directories/Folders, Registry, and Logs will be covered later. Before going into all of the tools the first thing that should be covered is the long history that Microsoft has gone through to develop the Windows operating system into the powerhouse it is today.

## 1. Windows History

### 1.1 Windows Operating System Introduction

The Windows operating system (OS) was developed by the Microsoft Corporation to be run on personal computers (PC). The Windows OS was the first operating system to introduce a GUI for PCs that were IBM compatible. Currently the Windows operating system has taken over the operating system market with approximately over 90 percent of owned PCs running some version of the Windows operating system. It is due to this popularity that the Windows operating system has many types of users. The Windows operating system has subsequently broken into two major versions. The first version is for personal use; while the other version is more functional for business use. (Britannica, T. E. )

## 1.2 The Evolution of Windows Through Time

The first version of the Windows operating system was released in the year 1985 and was a simple GUI that was created as an extension of the already existing Microsoft disk operating system (MS-DOS). The new operating system gave users the ability to visually navigate the virtual desktop. The new operating system made it possible for the user to use a mouse to click on the virtual files and folders. The new type of GUI did not make the use of typing in text prompts to navigate necessary. Future versions of the Windows operating system brought more functionality including: Windows File Manager, Print Manager, and Program Manager. The 1995 version of the Windows Operating system brought in functionality for the new hot ticket feature of the internet. The Windows 95 operating system came with built-in internet support as well as a pre-installed web browser named "Internet Explorer." In 2001 Microsoft brought the scattered software packages that the company offered under one umbrella and released Windows XP. Windows got rid of the original kernel and built a new more powerful one that offered a more practical interface, improved memory and application management. The Windows operating system has further evolved to include more features for user's and better management of resources with the latest Windows operating system being Windows 10. (Britannica, T. E. )

## 2.1 Windows Directories/Folders

When using computers, especially with modern operating systems one should make sure that they understand the techniques of creating, removing, and copying folders and directories for whatever operating system that you are currently using. First of all, we have to know what a Folder and a Directory are.

In Windows, a folder is something that provides a method for organizing all different types of files. When dealing with a folder someone could pretty much put whatever they think is

important in it whether it be music from the internet, a paper your writing for class, or even just some basic pictures. Folders in Windows lets you do a plethora of different things that make it easier for the user to access documents or whatever is in their organized folder. A folder is very easy to create as well. All a user has to do in Windows is right click on the blank screen and select “New” then name the folder and just like a folder was created.

A Directory in Windows is a place where you can store your folders on your computer. Usually when people use directories, they create one on a hierarchical file system such as Linux or Unix. The directory is everything about a computer, and in the directory, you are able to access hidden logs, program files, program data, and even access user information. In computer forensics accessing the directory lets you have access to all these folders and files and makes it easier for the investigator to find something that either a criminal is hiding or something secretive that they have hidden. File explorer is one of the main applications that can be used to access the folders in the directory and use it as a tool to navigate to the files that are needed. Sometimes criminals hide certain files that are encrypted and stored in a folder and this could be anything from child pornography to fraud.

**3.1 Definition of Windows Registry**

Windows registry is one of the first places a forensics investigator will look. Before we understand why let's first understand what a Windows registry is. Windows registry is a hierarchical database that stores configuration settings for low-level applications and the Windows operating system. These settings are stored as keys and values. Whenever a user installs new applications, hardware, or device drivers on a Windows-based computer system the registry is updated. Anytime a windows component, application, or hardware is executed, it retrieves the keys or entries from the registry. These keys or entries will have the latest

configuration settings. Data uploaded to the registry is sorted by computer-specific and user-specific data. This allows the registry to support multiple users. All registry files are stored in the Windows System32 config folder. Microsoft windows has a built-in registry editor called regedit. In the registry editor, there are files called *hives*. Inside each hive, we have something called *keys*. Inside the keys, there are *subkeys* and data entries called *values*. The five hives a forensic investigator needs to understand to properly investigate are HKEY_CLASSES_ROOT (HKCR), HKEY_CURRENT_USER (HKCU), HKEY_LOCAL_MACHINE (HKLM), HKEY_USERS (HKU), and HKEY_CURRENT_CONFIG (HKCC). HKCR is where all the file extension association information is stored. This means the information stored here is used to correctly open a program when it is executed in File Explorer. HKCU stores settings that are specific to the user that is currently logged. HKLM is where information on hardware that is detected and software that is installed is stored. HKU is where the configuration information is for all active users stored on the computer. HKCC isn't stored on the hard drive it is only created when the computer first boots up. It is a shortcut/pointer to the HKLM hive.

**3.2 The Use of Windows Registry in Forensic Investigations**

Once a forensic investigator understands how the Windows registry works, they can start their investigation. Through the use of the Windows registry the investigator can find out important details pertaining to the investigation such as when was the last time the user was logged on, what files did they access, most recent software that was used, and many other details. To see what websites the user accessed through internet explorer, the investigator can go through the HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs path in regedit. Another important use of the Windows registry is being able to find out what ip addresses the user connected to through the HKEY_LOCAL_MACHINE\System\Services

\CurrentControlSet\services\Tcpip\Parameters\Interfaces path in regedit. The windows registry is extremely useful when the investigator is trying to find the evidence for their investigation that that may be needed to prove someone is guilty in the court of law.

### 4.1 Windows Logs

The Windows operating system comes with the application called Event Viewer pre-installed. The Windows Event Viewer handles all of the logging that takes place on the user's system. The Window's operating system logs are important for system administrators because it is a centralized location of all the records that the operating system has recorded. The records that can be found include application/hardware errors, proprietary errors, as well as a complete log of application or hardware related events that have taken place. The cause of an error can be difficult to diagnose, so to help with the diagnosing process when an error occurs the error is recorded into a log. Some common errors that may occur are: excessive attempts to access a disk, low-memory conditions, and security related errors such as failed login attempts. The security related events can be critical for forensic investigators. The logs can be created into a fully encompassing report that the system administrator can view to diagnose problems. Microsoft has also included an API that can be programmed to help create reports. Window's logs are critical for forensic investigators to help investigate systems. (Satran, M.)

### 4.2 Windows Logging Tool - QRadar

An important aspect of logging that should be considered is the potential that the Window's log may be changed by the malicious actor. To combat this potential a number of tools were created to actively report any critical logs. One of these tools was created by IBM called QRadar. QRadar is a tool that is installed on the system that actively interprets logs. QRadar has a number of options to customize reporting. QRadar reads the Window's logs and

alerts security personnel of any important logs. QRadar has the option to store the log in the cloud making it a preferred option for forensic analysts to help investigate systems. QRadar aids in retracing the step by step actions of the malicious actor and is preferred by many forensic investigators for their investigation. (IBM QRadar)

## Conclusion

The Window's operating system is the most popular operating system, and forensic investigators must be knowledgeable in this operating system to be a sufficient investigator. Numerous areas exist that the investigator should look into, but the areas covered throughout this paper are the Window's Directory/Folders, Window's Registry, Window's Logs. Each of these areas should be of interest due to the amount of information that the investigator could find and should be some of the first places that the investigator should look at.

# References


Britannica, T. E. (2017, February 21). Windows OS. Retrieved October 29, 2018, from https://www.britannica.com/technology/Windows-OS

IBM QRadar Incident Forensics. (2018, October 29). Retrieved from https://www.ibm.com/us-en/marketplace/ibm-qradar-incident-forensics

Satran, M. (2018, October 29). Event Logging. Retrieved from https://docs.microsoft.com/en-us/windows/desktop/eventlog/event-logging

Mendelsohn, Y. (June 23). Disk Drive. Retrieved November 1, from http://condor.depaul.edu/ymendels/tutorials/directories/default.htm

Farmer, D. J. (n.d.). A Forensic Analysis Of The Windows Registry. Retrieved October 31, 2018, from http://www.forensicfocus.com/a-forensic-analysis-of-the-windows-registry

Digital Forensics, Part 5: Analyzing the Windows Registry for Evidence. (2018, August 24). Retrieved October 31, 2018, from Hackers-Arise Citation