When it comes to Linux and Windows forensics the first thing that pops up in my mind is the file structures in which passwords are stored. In a previous posting I had mentioned how windows passwords are stored within the HKEY\_LOCAL\_MACHINE\_SAM folder in the forms of hashed values while in contrast on a Linux machine the hashed value is stored in the etc/shadow file. (ComputerNetworkingNotes, 2019) This is where you can retrieve the hash value of a password to later be extracted via programs such as John the Ripper or Cain and Abel.

Moving beyond that, when it comes to analyzing the two Operating systems, one must also know how traverse the systems using different commands but with similar outcomes. So just knowing how to get around in a Linux machine is imperative because the CLI is different than that of a traditional windows machine.

Below are some useful examples of commands that are similar in both languages.

|  |  |
| --- | --- |
| Windows commands | Linux Commands |
| Ipconfig | Ifconfig |
| tasklist | Ps -a |
| dir | Ls -a |
| tracert | traceroute |

In regards to collection and preservation on a Linux machine one can create an image of the file by performing the command “dd” (DataDump) and then creating a hash value of the image to be referenced for validity. This is a quick and simple way to create an image on Linux system. (Vince, 2020)

Another fun thing about Linux forensics is the vast majority of open source tools and framework such as Kali Linux having a myriad of tools for forensics that is free and open to the public. This make learning about the subject matter easier since users don’t have to pay for expensive software.

So in conclusion Linux forensics is different from windows by its files structure, CLI commands, and abundance of free and open source programs.

Thanks again!

-Eric Webb

ComputerNetworkingNotes. (2019, January 4). /etc/shadow file in Linux Explained with Examples. Retrieved March 9, 2020, from <https://www.computernetworkingnotes.com/rhce-study-guide/etc-shadow-file-in-linux-explained-with-examples.html>

Vince. (2020, March 1). Data Dump(dd) to Create a Forensic Image with Linux. Retrieved March 9, 2020, from http://vcodispot.com/data-dump-dd-create-forensic-image-linux/