Forensics analysis of USB device traces

Digital Forensics

I. Duits (1876171)
E. Geretto (1869426)
G. Iadarola (1879480)

June 2, 2017

1 Introduction

In digital forensics it is necessary to inspect certain computer systems to see what information they hold and how they were used. Knowledge about when a USB device was connected can be helpful in the investigation. USB devices can be used to transfer valuable data in cases of data theft or possession of illegal material. Copying data leaves traces, as A. Ramani and S. Dewangan demonstrated in their paper [3] and T. Roy and A. Jain in theirs. [8]

In Section 2, we show how to access this information in Windows and Linux systems. There are tools which can help for Windows. However, for Linux there are no tools like that. Linux is getting slowly more private users[2] and a lot of Internet servers run on a Linux distribution[5].

can get information from the log files on a Windows system, especially for an image of a disk, which is most used in digital forensics.

However, in this paper we will not focus on Windows machines or how data is copied. We will focus on how we can detect the use of a usb device on Linux. There is not a easy way to do this for a images created for a Linux machine.

2 Literature

The log files on a computer distribution can be used to track the use of usb devices on the system. Log files records the history of events and executions in detail, which can be used to see the earlier or current state of a system and to recover such a state [6]. They can be also used to detect unexpected behavior and track suspicious activities that may violate the system, this is useful for both private users and digital forensics.

2.1 Windows

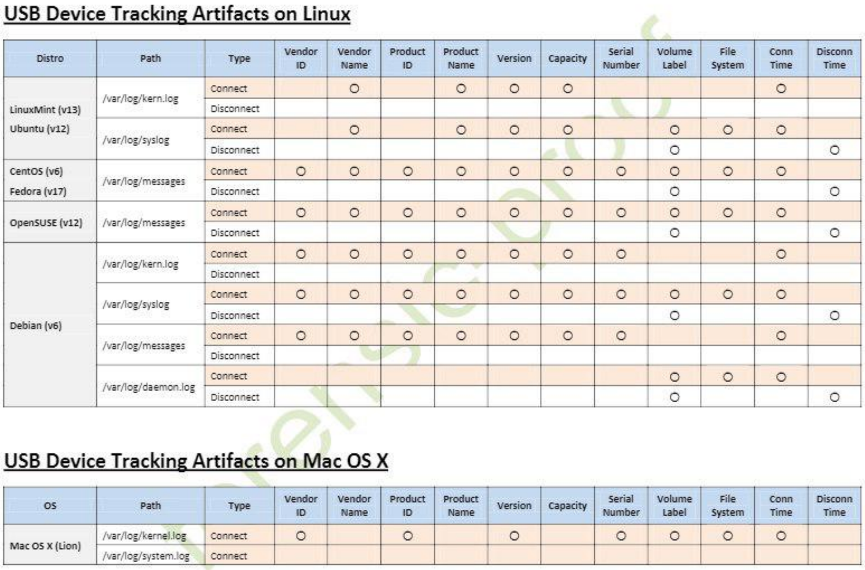
Windows 8 and 10 have a program installed, Event Viewer, which allows users to view the log and look up all the information. The tool can be used to track down the usages of usb sticks. For a detailed explanation on how to use it, go to [7]. For this tool the computer needs to be running.

In digital forensics it is not always possible to just boot the computer and look for the log file, that will make changes to the system. An image of the computer is therefore created, which can be investigated instead.

There are different kind of software tools which can help to search the log files of an image, and thus the connection of usb devices on a Windows system. For example the open source tool Autopsy[1] can be used to read the image and extract all kind of useful information from it. The connection time and usb serial number can be found really easily.

2.2 Linux

Less information can be found on how to obtain usb device tracking information on a Linux system. For example, figure 2.2 [4] shows where to find the log file, and which information the file holds. Unfortunately the information is way outdated. This file was published in 2012 and the paths to the log files is incorrect.



USB Device Tracking Artifacts on Linux

Distro	Path	Type	Vendor ID	Vendor Name	Product ID	Product Name	Version	Capacity	Serial Number	Volume Label	File System	Conn Time	Disconn Time
LinuxMint (v13) Ubuntu (v12)	/var/log/kern.log	Connect		○		○	○	○				○	
		Disconnect											
	/var/log/syslog	Connect		○		○	○	○		○	○	○	
		Disconnect								○			○
CentOS (v6) Fedora (v17)	/var/log/messages	Connect	○	○	○	○	○	○	○	○	○	○	
		Disconnect								○			○
OpenSUSE (v12)	/var/log/messages	Connect	○	○	○	○	○	○	○	○	○	○	
		Disconnect								○			○
Debian (v6)	/var/log/kern.log	Connect	○	○	○	○	○	○	○			○	
		Disconnect											
	/var/log/syslog	Connect	○	○	○	○	○	○	○	○	○	○	
		Disconnect								○			○
	/var/log/messages	Connect	○	○	○	○	○	○	○			○	
		Disconnect											
	/var/log/daemon.log	Connect								○	○	○	
		Disconnect								○			○

USB Device Tracking Artifacts on Mac OS X

OS	Path	Type	Vendor ID	Vendor Name	Product ID	Product Name	Version	Capacity	Serial Number	Volume Label	File System	Conn Time	Disconn Time
Mac OS X (Lion)	/var/log/kernel.log	Connect	○		○		○		○	○	○	○	
	/var/log/system.log	Connect											

3 The research preparation

3.1 General plan

For this research we will create a few images of different Linux distributions, which ones will be discussed in section 3.2 and how we create them is discussed in section 3.3. We will then analyze the created images' log files by a python program we wrote, which is explained in section 3.4

[1] http://www.autopsy.com/

3.2 Used Linux distribution systems

We are using the following Linux distributions.

- Fedora 25, kernel 4.8.6
- OpenSUSE
- Ubuntu
- Debian

For each Linux we used the last stable version, we start installing the distributions on May 29 2017. With these distributions mentioned above, we cover most of the popular Linux distro's [1], as we can see that some other Linux distro's are part of these. Distributions like Elementary, Linux Mint and Zorin are all Ubuntu based and thus covered in our research.

3.3 Creating the images

The following steps were taken to prepare for the research:

- Clear the computer
- Install the Linux Distribution (default installation, version as mentioned in Section 3.2)

  Make sure all drives work correctly (Note: this influence the log file)
- Then we repeat 5 times, the following sequence

  Start up

  Plug in mouse

  Plug in USB 2.0

  Plug in USB 3.0
- Create image of the machine

3.4 The program in Python

4 Found results

5 Conclusion

Analyzing the log fies of a system could besides tracking usb usages, be very useful for other digital forensic applications, like finding unexpected behavior and track the use of the computer.

References

[1] 10 top most popular linux distributions of 2016. https://www.tecmint.com/top-best-linux-distributions-2016/. Accessed: 29-05-2017.

[2] Desktop operating system market share worldwide - apr 2011 to apr 2017. http://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-201104-201704. Accessed: 30-05-2017.

[3] S. K. D. Abhijeet Ramani. Registry keys to track the traces left out in copying files from system to external usb device. *International Journal of Computer Science and Information Technologies*, 2014.

[4] K. Jinkook. Usb device tracking on linux, mac os x. http://forensic-proof.com/archives/3744. Accessed: 29-05-2017.

[5] D. Nagel. Linux leads server growth. https://thejournal.com/articles/2012/06/05/linux-based-systems-lead-server-growth.aspx, 2012. Accessed: 30-05-2017.

[6] D. R. C. Ross S. Finlayson. Log files: An extended file service exploiting write-once storage. *ACM SIGOPS Operating Systems Review*, 21:139–148, 1987.

[7] G. Shultz. How to track down usb flash drive usage in windows 10s event viewer. http://www.techrepublic.com/article/how-to-track-down-usb-flash-drive-usage-in-windows-10s-event-viewer/. Accessed: 29-05-2017.

[8] A. J. Tanushree Roy. Windows registry forensics: An imperative step in tracking data theft via usb devices. *International Journal of Computer Science and Information Technologies*, 2012.