Forensics analysis of USB device traces

Digital Forensics

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

June 2, 2017

1 Introduction

Nowadays, almost half of all households in Western Europe have a personal computer and the percentage increases over 90% by taking into account only young people (15 to 30 years old).

The number of computing devices as PCs, laptops and smartphones has increased exponentially in the past decade. Daily activities are organized on social media, works are performed on laptop and meetings on video-conference. Our entire life is managed through electronic devices and the number of connected user is going to grow in the future. The government's (most of them) and the public opinion do agree with these changes and support every initiative which increase the use of new technologies.

Nevertheless, several problems has to be faced and need to be managed in order to keep benefiting from the computing devices revolution.

Everyone can get access and interact with PCs and smartphones and also criminals are using them to perpetrate frauds and illegal activities. Indeed, the Digital forensic branch is becoming one of the most important sector in the forensics and investigation field. By inspecting and analysing computer systems, officers can retrieve essential evidence to prove and demonstrate criminal event.

This paper aims to contribute in this field and is focused on USB devices and the traces left on operating systems.

USB devices can be used to transfer valuable data in cases of data theft or possession of illegal material, and knowledge about when a USB device was connected can be really helpful in the investigation.

As stated in the Locard's exchange principle [6], copying data leaves traces. These traces are recoverable as reported for instance by several researches available in the literature. [10, 3].

In Section 2 is discussed how to access this information in both Windows and Linux systems. On windows environment, there are many tools which can help us in analysing and retrieving data. However, on Linux there are just few useful tools.

Windows is the most used operating systems but Linux usage is increasing [2] and actually most of the servers run on a Linux distribution [8]. In order to contribute in the digital forensic field on Linux systems, a tool was developed

by us and subsequently opensourced. This software will help Linux users in retrieving data about USB devices from an image of Linux installation.

The paper is structured as follow. In section 3 is described the methodology and the steps performed to analyse the images which were used to develop the tool. Then, the achieved goals are described in section 4 and the short discussion reported in section 5 ends the paper.

2 Log files and USB logging

Log files are one of the most important sources of information when trying to reconstruct the events that lead to a certain situation in a computer system. Indeed, they are constructed recording a series of timestamped messages, generated by the various components of the system, that, when considered as a whole, give a complete overview of the operations in execution at a given moment.

Given the information they contain, log files are also one of the most important sources of information during a forensics investigation since they allow to trace possibly malicious activity through time. As a consequence, it is essential to be able to retrieve and analize them in the fastest way possible. [5]

One of the main problems when analyzing log files is that they tend to be huge in terms of the number of messages collected in them. For this reason, forensics investigators usually rely on tools that automatize the process of extraction and parsing in order to extract immediately the relevant information.

Given that different operating systems generate log files structured in a different way and store them at different locations, the following subsections will provide an overview of where the files are located and which tools can be used to analyze them in Linux and Windows. Moreover, particular attention will be given to the information relative to USB devices, since it is the main focus of this study.

2.1 Windows

In the newest iterations of Microsoft Windows, all the log files are stored by default in the folder `%SystemRoot%\system32\winevt\Logs`. These files can be opened with a tool called *Event Viewer* in order to examine their content. This tool, however, allows only for simple automatic analysis, as a general keyword search, but it does not automatically extract the most relevant information stored.

From a forensics investigator perspective, the use of Event Viewer implies a tedious and error prone manual analysis that is surely not desirable. For this reason, other tools have been developed that allow the extraction and analysis of log files from system images in an automatic fashion, so that the investigator just needs to observe the relevant data and connect them to the evidence already collected.

The two positive consequences of the usage of these tools are that time is saved which can be dedicated to other activities and, most importantly, that the analysis of the evidence can be considered forensically sound. Indeed, in order to avoid damaging or contaminating the evidence collected, the system analyzed should always be imaged and the image should be hashed in order to allow for a subsequent verification of the investigative process. These tools allow for the

analysis of these images directly and guarantee the absence of contamination during the process. [7]

The open source tool that is most commonly used for this purpose is called *Autopsy*, developed by *SleuthKit*; between other things, it also analyzes the system logs and extracts a list of all the USB devices that were attached to the machine according to the information in the files. This allows an investigator retrieve important information, as the serial number of the device or the time of insertion and deletion. This information is important, for example, to track USB sticks across different machines. [4]

2.2 Linux

Regarding the Linux operating system, the kernel has an internal log on which every module, and thus also the USB drivers, can write on. This log, called internal ring buffer, is not directly stored in persistent memory; this task, indeed is demanded to other services that also collect logs from other sources, as the *X11* display server, and construct a general system log.

Unfortunately, different distributions use different log-handling daemons and even different versions of the same daemon which may store the log files in different locations. The most common ones are the *syslog* daemon, which stores the log in the `/var/log/syslog` file in plaintext, and the *journald* daemon, part of the systemd project, which stores the files in the `/var/log/journal/` directory in binary format. There are also other interesting combinations that include collecting the data using journald and then store them in a syslog compatible format, as Ubuntu and derivates do. [9]

All the USB related information flows from the kernel ring buffer to the log daemon and gets stored in one of these locations. Given the variety of locations and daemons that are currently being used, to the best of our knowledge, there is no automated tool that is capable of extracting automatically, from a disk image, information about USB devices; currently, the only option is manual analysis.

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

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. website with top10 distro https://brashear.me/blog/2015/08/24/results-of-the-2015-slash-r-slash-linux-distribution-survey/

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] S. B. Deb and A. Chetry. Usb device forensics: Insertion and removal timestamps of usb devices in windows 8. In *Advanced Computing and Communication (ISACC), 2015 International Symposium on*, pages 364–371. IEEE, 2015.

[5] R. Finlayson and D. Cheriton. *Log files: an extended file service exploiting write-once storage*, volume 21. ACM, 1987.

[6] E. Locard. Locards exchange principle, 2008.

[7] R. Murphey. Automated windows event log forensics. *digital investigation*, 4:92–100, 2007.

[8] 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.

[9] L. Poettering. Using the Journal. `http://0pointer.de/blog/projects/journalctl.html`, 2012.

[10] 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.