Analysis Of Deletion Habits On Used USB Thumb Drives

Mojtaba Al Fardan • Dr. Sarah Diesburg
losst-group@uni.edu

Abstract

One important aspect of personal privacy is how to completely erase data from our personal storage devices. According to recent research, it is hard to verify if data is deleted from USB flash drives. USB flash drives are inexpensive, everywhere, and their uses have increased over the years.

The purpose of this research is (1) to find out the deletion habits of people, (2) to gain an understanding of the information that can be recovered from intact USB flash drives, and (3) take apart the drives to find out if any extra data can be recovered.

In this research we analyzed 119 used drives bought from Amazon and Ebay. From our analysis we found that the majority of people don’t use effective deletion methods. We also found a substantial number of people don’t delete their data before they sell the drive. Some of the data recovered from the drives contained personal and sensitive information about people and corporations.

Background and Methodology

USB flash drives contain a NAND flash memory chip for storage (fig1) and a microcontroller to communicate with the computer (fig2). Unfortunately the microcontroller can hide access to data stored on the NAND flash memory chip and that hidden data cannot be easily deleted [1,2].

We forensically investigated the drives using the following steps:

1. First we looked inside the intact drives to check if any deletion occurred at all, and we collected any data found at that stage.
2. Next we used forensic tools to look for more data that could be recovered.
3. Then we investigated the drive to check what deletion method was used (e.g. delete key, quick format, etc.).
4. Finally we recovered data from raw chips which were obtained by opening the flash drive and desoldering the NAND flash chip, and reading the chip using a special programmer that reads raw NAND chips.

Results

We investigated the deletion habits of drives sold on Amazon and Ebay (fig3). We found out that 29% of the drives were not deleted at all before being sold, 36% of the drives were deleted using the delete key, 20% did a windows quick format or something similar, and 10% did a windows full format or a similar zero overwrite mechanism. The data are recoverable by forensic tools if the deletion method was delete or a quick format. This means we could possibly recover data from 85% of the USB flash drives in our study.

We broke down the types of data found into categories (fig4).

- About 26% of the data were considered personal identifiable information, which is anything that could identify a person or considered a personal information (e.g. full names, date of birth, addresses, social security numbers, credit cards, id’s, photos of faces, tax forms, etc.).
- About 8% of the data obtained were considered corporate commercial information (which includes any information about a corporation that are public whether it was prices or ads or general information).
- About 5% of the data obtained were considered corporate confidential information (which includes any information about a corporation that shouldn’t be public like detailed information about employees, invoices, legal documents, etc.).
- About 3% of the data obtained are considered illicit (which includes pornographic material, anything illegal, etc.).

We also removed NAND chips from intact thumb drives and discovered more storage space and data. Results for two of the drives are shown in fig5. We will continue processing NAND chips as future work.

Acknowledgements

We would like to thank Nigel Ploof and Jonathan Schlicht for their creativity and continuing important contributions. We also would like to thank the Computer Science Department and the Student Undergraduate Research Program for the necessary support for this research.

References


Marcel Breeuwsma, Martien De Jongh, Coert Klaver, Ronald Van Der Knijff and Roeloffs, M., 2009. Forensic Data Recovery from Flash Memory, CiteSeerX.