

Overwriting Hard Drive Data: The Great Wiping Controversy

Craig Wright¹, Dave Kleiman², and Shyaam Sundhar R.S.³

¹ BDO Kendalls, Sydney, Australia

Craig.Wright@bdo.com.au

² ComputerForensicExaminer.com, Florida, US

dave@davekleiman.com

³ Symantec, USA

shyaam@gmail.com

Abstract. Often we hear controversial opinions in digital forensics on the required or desired number of passes to utilize for properly overwriting, sometimes referred to as wiping or erasing, a modern hard drive. The controversy has caused much misconception, with persons commonly quoting that data can be recovered if it has only been overwritten once or twice. Moreover, referencing that it actually takes up to ten, and even as many as 35 (referred to as the Gutmann scheme because of the 1996 Secure Deletion of Data from Magnetic and Solid-State Memory published paper by Peter Gutmann) passes to securely overwrite the previous data. One of the chief controversies is that if a head positioning system is not exact enough, new data written to a drive may not be written back to the precise location of the original data. We demonstrate that the controversy surrounding this topic is unfounded.

Keywords: Digital Forensics, Data Wipe, Secure Wipe, Format.

1 Introduction

Often we hear controversial opinions on the required or desired number of passes to utilize for properly overwriting, sometimes referred to as wiping or erasing, a modern hard drive. The controversy has caused much misconception, with persons commonly quoting that data can be recovered if it has only been overwritten once or twice. Moreover, referencing that it actually takes up to ten, and even as many as 35 (referred to as the Gutmann scheme because of the 1996 Secure Deletion of Data from Magnetic and Solid-State Memory published paper by Peter Gutmann, [12]) passes to securely overwrite the previous data.

One of the chief controversies is that if a head positioning system is not exact enough, new data written to a drive may not be written back to the precise location of the original data. This track misalignment is argued to make possible the process of identifying traces of data from earlier magnetic patterns alongside the current track.

This was the case with high capacity floppy diskette drives, which have a rudimentary position mechanism. This was at the bit level and testing did not consider the accumulated error.

The basis of this belief is a presupposition is that when a one (1) is written to disk the actual effect is closer to obtaining a 0.95 when a zero (0) is overwritten with one (1), and a 1.05 when one (1) is overwritten with one (1). This we can show is false and that in fact, there is a distribution based on the density plots that supports the contention that the differential in write patterns is too great to allow for the recovery of overwritten data.

The argument arises from the statement that “each track contains an image of everything ever written to it, but that the contribution from each “layer” gets progressively smaller the further back it was made”. This is a misunderstanding of the physics of drive functions and magneto-resonance. There is in fact no time component and the image is not layered. It is rather a density plot.

This is of prime importance to forensic analysts and security personal. The time needed to run a single wipe of a hard drive is economically expensive. The requirements to have up to 35 wipes [12] of a hard drive before disposal become all the more costly when considering large organisations with tens of thousands of hosts. With a single wipe process taking up to a day to run per host through software and around an hour with dedicated equipment, the use of multiple wipes has created a situation where many organisations ignore the issue all together – resulting in data leaks and loss.

The inability to recover data forensically following a single wipe makes the use of data wiping more feasible. As forensic and information security professionals face these issues on a daily basis, the knowledge that a single wipe is sufficient to remove trace data and stop forensic recovery will remove a great deal of uncertainty from the industry and allow practitioners to focus on the real issues.

1.1 What Is Magnetic Force Microscopy¹

Magnetic force microscopy (MFM) images the spatial variation of magnetic forces on a sample surface. The tip of the microscope is coated with a ferromagnetic thin film. The system operates in non-contact mode, detecting changes in the resonant frequency of the cantilever induced by the magnetic field's dependence on tip-to-sample separation. A MFM can be used to image naturally occurring and deliberately written domain structures in magnetic materials. This allows the device to create a field density map of the device.

1.2 MFM Imagery of Overwritten Hard Disk Tracks

The magnetic field topography (Fig. 2A below) was imaged with an MFM to measure the magnetic force density. This image was captured using the MFM in Lift Mode (lift height 35 nm). This results in the mapping of the shift in the cantilever resonant frequency.

¹ The MFM senses the stray magnetic field above the surface of a sample. A magnetic tip is brought into close proximity with the surface and a small cantilever is used to detect the force between the tip and the sample. The tip is scanned over the surface to reveal the magnetic domain structure of the sample at up to 50 nm resolution.