S.M.A.R.T.

by

Christine Casey

Patrick Leahy Center for Digital Investigation

Champlain College

2/22/12

Contents

1 Introduction

1.1 Research Problem

Self-Monitoring Analysis Reporting Technology, S.M.A.R.T., is a system for hard disk drives that reports different attributes about the hard drive and warns the user about drive failure. The overall purpose of S.M.A.R.T is to alert the user if their hard drive has been powered on or off, and in the event of drive failure, so that measures can be taken to save data and back it up. S.M.A.R.T. is considered to be an anti-forensic tool.

1.2 Field of Research

S.M.A.R.T. technology was developed in 1992 by IBM, but was actually implemented into hard disk drives in 1995. In regards to digital forensics, there are three important attributes that S.M.A.R.T. captures from the hard drive: the start/stop count, the power on hours, and the power cycle count. These three attributes are potentially what would allow a person to know if their hard drive had been used and or accessed. S.M.A.R.T. is also a tool that is used in a laboratory setting, which the system administrator can monitor the hard drives on the workstations without the knowledge of the users.

1.3 Research Questions

Is S.M.A.R.T. data accurate?

Is S.M.A.R.T a reliable tool?

Will a person be able to know if their hard drive could have been taken to be forensically imaged?

1.4 Report Overview

This report will reference other research completed on S.M.A.R.T. It will explain the methodologies and procedure of the testing completed. The report will also explain and analyze the data collected from the testing.

2 Literature Review

There has been previous research conducted on S.M.A.R.T. in May of 2005 by Steven McLeod. The report is published on Forensic Focus and is entitled “Smart Anti-Forensics.” The research question asked was if an attacker would be able to determine if their hard drive was taken to be forensically imaged. The overall goal of the research was to determine if there was a way that S.M.A.R.T. attribute values could be prevented from being modified. In the experiment there were numerous tests conducted on numerous brands of hard drives. The tests were conducted to see what causes modifications to the values of the power cycle count and the power on hours. All tests were conducted using Knoppix. The tests involved using a program called smartmontools. With this program the user inputs commands into a command prompt to view the S.M.A.R.T. attributes. To view all the S.M.A.R.T. attributes, the user inputs the command smartctl –a /dev/hda. The first test involved disabling S.M.A.R.T. using smartmontools. The command to do this is smartctl –s off /dev/hda. After the command was inputted, the workstation was then powered off and then powered back on. It was discovered that even though S.M.A.R.T. was disabled, every hard drive modified the power cycle count attribute.

3 Methodology and Methods

For determining if S.M.A.R.T. data is accurate, a test was conducted, sampling S.M.A.R.T. data from workstations in the lab.

3.1 Overarching methodology

Smartmontools was installed on each of the workstations in the lab. This tool is used to collect the S.M.A.R.T. attributes recorded for each hard drive.

3.2 Table 1

Workstation #	Date	Time	Start/Stop Count (#4)	Power-On Hours (#9)	Power Cycle Count #12)
5	1/22/2012	12:12 PM	423	1346	311
5	1/26/2012	11:05 AM	424	1350	312
1	2/1/2012	11:18 AM	208	1038	186
3	2/1/2012	11:25 AM	255	844	191
5	2/2/2012	11:29 AM	427	1462	315
1	2/3/2012	2:09 PM	208	1041	186
2	2/3/2012	12:29 PM	179	799	173
3	2/8/2012	11:10 AM	265	915	201
3	2/9/2012	12:14 PM	265	917	201
5	2/9/2012	12:18 PM	430	1569	318
3	2/9/2012	12:20 PM	266	921	202
5	2/13/2012	2:17 PM	430	1691	318
5	2/22/2012	11:31 AM	432	1883	320
3	2/22/2012	12:17	283	970	219

		PM			
1	2/22/2012	12:21 PM	444	1045	214
2	2/22/2012	12:25 PM	188	1104	182

3.3 Data Collection

Data for this test was collected over a time span of one month. Data was collected using the utility smartmontools. Smartmontools presented the administrator with a command prompt and, to view all S.M.A.R.T. attributes, the command smartctl –a /dev/hda was entered. When the command was entered, all S.M.A.R.T. attributes about the hard drive were listed in a table. There were three numeric values that were collected for this test: the start/stop count, power-on hours, and power cycle count. Once the command was entered, these specific values were found in the table and recorded into a table, this table is found above in section 3.2.

3.4 Analysis

Workstations 1, 2, 3, 5 in the lab were tested using the smartmontools utility. Workstation 5 was the first workstation that was tested. Workstation 5 had an initial start/stop count of 423, power-on-hours of 1436, and power cycle count of 311. Workstation 5 had a final start/stop count of 432, power-on-hours of 1883, and a power cycle count of 320. All of the values for Workstation 5 increased over the period of time the test was conducted. The value that increased the greatest for Workstation 5 was the power-on-hours. Workstation 1 had an initial start/stop count of 208, power-on-hours of 1038, and a power cycle count of 136. Workstation 1 had a final start/stop count of 444, power-on-hours of 1045, and a power cycle count of 214. All of the values for Workstation 1 increased over the period of time the test conducted. The value that increased the greatest for Workstation 1 was the start/stop count. Workstation 2 had an initial start/stop count of 179, power-on-hours of 799, and a power cycle count of 173. Workstation 2 had a final start/stop count of 188, power-on-hours of 1104, and a power cycle count of 182. All of the values for Workstation 2 also increased over the period of the testing. The value that increased the greatest for Workstation 2 was power-on-hours. Workstation 3 had an initial start/stop count of 255, power-on-hours of 844, and a power cycle count of 191. Workstation 3 had a final start/stop count of 283, power-on-hours of 1104, and a power cycle count of 182.

4 Results

S.M.A.R.T. recorded all of the attributes about the hard drive every time the command was entered, and the attributes were shown neatly in a table. For each of the workstations tested, all of the S.M.A.R.T. attribute values increased over the testing time. S.M.A.R.T. was never disabled, so it was functioning properly. Disabling S.M.A.R.T was attempted, but every time it was disabled, the workstation's operating system failed.

5 Conclusion

S.M.A.R.T. is a reliable tool based on the data taken from the testing. All of the data collected is accurate. The changes in the data over time also are reasonable based on how the workstations in the lab are used. The workstations are rarely turned off, which is why there is a high increase in power-on-hours for all the workstations tested over the period of time. This tool is a reliable tool for network administrators to use to monitor the hard drives of workstations in a lab setting to monitor computer usage and possible hard drive failure. Also, a person would only know if their hard drive was accessed if they were using the utility smartmontools to monitor the attributes. They would then see that the attributes were modified and their computer was used without their consent or knowledge.

6 Further Work

Further work that can be conducted with S.M.A.R.T. can be figuring out exactly how to stop S.M.A.R.T. from recording attributes about hard drives when it is disabled. This could entail research and experimentation on where the S.M.A.R.T. attributes are being stored on the hard drive. Testing for this can be conducted by disabling S.M.A.R.T. on hard drives. Although disabling S.M.A.R.T. using smartmontools caused the operating system to fail during the testing, S.M.A.R.T. can be disabled through the bios, and further testing can be completed if the operating system does not fail.

7 References

McLeod, Steven. “Smart Antiforensics”. Forensic Focus. 2005. http://www.forensicfocus.com/Content/pid=53/page=1/