THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 15 | Number 1 Article 2

June 2020

An Evaluation Of Data Erasing Tools

Andrew Jones
University of Suffolk, andy1jones.aj@gmail.com

Isaac Afrifa
University of Hertfordshire, isaac.afrifa3@yahoo.com

Recommended Citation

Jones, Andrew and Afrifa, Isaac (2020) "An Evaluation Of Data Erasing Tools," *Journal of Digital Forensics, Security and Law*: Vol. 15 : No. 1 , Article 2.
DOI: https://doi.org/10.15394/jdfsl.2020.1615
Available at: https://commons.erau.edu/jdfsl/vol15/iss1/2

AN EVALUATION OF DATA ERASING TOOLS

Isaac Afrifa[1], Andrew Jones[2]
[1] [2]Cyber Security Center, University of Hertfordshire
[2]Cyber Security CRC, Edith Cowan University
isaac.afrifa3@yahoo.com[1]
andy1jones.aj@gmail.com[2]

ABSTRACT

The permanent removal of data from media is a major area of concern mainly because of the misconception that once a file is deleted or storage media is formatted, it cannot be recovered. There has been the development of both commercial and freeware data erasing tools, which all claim complete file or disk erasure. This report analyzes the efficiency of a number of these tools in performing erasures on an electromechanical drive. It focuses on a selection of popular and modern erasing tools, taking into consideration their usability, claimed erasing standards, and whether they perform complete data erasure with the use of the Write Zero method.

Keywords: Data wiping, Write Zero, Data Erasing Tools

1. INTRODUCTION

Data in the 21st century has become an epitome of controversy due to the countless occurrences of crimes associated with data breaches and data loss. Most physical drives that are used to store either corporate or personal data usually end up being sold when they are no longer required, stolen, or lost. Examples include a report by `Historycoalition.org` (2009), that the US National Archives and Records Administration (NARA) reported the loss of an external hard drive from the NARA College Park facility in Maryland. This hard drive contained copies of sensitive personal information such as names and social security numbers of individuals who may have worked or visited the White House during Clinton's Presidency.

In another fairly recent incident, the Mirror (2017) also reported a massive data loss threat that involved a USB stick, which was found in the streets of London, containing highly confidential information belonging to Heathrow Airport. The drive consisted of 76 unencrypted folders, which included precise routes Her Majesty the Queen uses in the airport, maps showing the tunnel networks and escape shafts linked to the Heathrow Express, and many more. These pieces of information, in the wrong hands, can be used in malicious attacks.

A significant question that is related to data removal is, "Can data be completely erased if no longer required?" The perception that non-technical individuals tend to have is that once a file is deleted from the recycle bin or a drive is formatted, and the data cannot

be recovered. However, when the Recycle bin or Trash folder is emptied, the operating system only removes pointers to the deleted data. The information remains on the hard disk until another file overwrites it. With the formatting of drives, if the 'quick' format is used, data is not removed as formatting only reinitializes the file system of the drive, as explained by Rothke (2009). Even with new overwrites, some of the data might still be recovered. This misconception has led to numerous data breaches and loss of confidential information to identity thieves and hackers.

The aim of this research was to examine some of the most popular and easily accessible data erasing tools and evaluate their efficiency based on their performance and ability to completely erase drives with the Write Zero wiping method. The reasons for carrying out this study were that it had been some time since a comparative study was carried out, and in the intervening period, new tools have become available and existing tools have been updated. In view of this, standard experiments were conducted on an electromechanical hard disk using 8 data erasing tools, namely, Hard Wipe, Eraser, Macrorit Data Wiper, Active KillDisk, Disk Wipe, Puran Wipe Disk, Remo Drive Wipe, and Super File Shredder. Solid state drives were not included in this research because, with the wear leveling algorithms that are in use and the current state of the art, there is no scientifically proven method that can be used to ascertain that all sectors of the storage media have been accessed and overwritten. This issue will be examined in future research.

1.1 Motivation

With the surge in data related crimes, organizations and individuals are investing heavily in keeping data safe and secure from unwanted parties. Studies show that almost 5 million data items are reported missing or stolen worldwide every day, which implies 58 items are lost every second (Drolet, 2019). Corporate organizations are spending millions of pounds to avoid data breaches and losses. The general public also had their fair share of data loss due to the general lack of knowledge in relation to media sanitization. It is therefore essential to address the problem of data erasure and help identify the best and most easily accessible tools for media sanitization associated with storage devices notably hard drives, as they are considered as one of the most commonly used primary storage devices to store confidential and sensitive information (Valli and Jones, 2005).

1.2 Project Phases

The project started in February 2019 and was carried out in 5 phases:

- Literature review. This phase includes an investigation of past and recent papers that relate to erasing of data on storage media devices, the known data erasing standards, and other notable topics associated with data erasing;

- Research of Erasing Tools. This phase involves the study and investigation into free versions of data erasing tools that have the Write Zero method as one of the supported erasing standards. As a result, 8 tools were acquired and installed;

- Creation of dataset for evaluation. This phase consisted of the acquisition of different file types that were used as datasets for the research;

- Experimentation and Analysis. This phase involved the testing of all the selected erasing tools and also examines their wiped disk images to enable the analysis of the results and included, where relevant, an attempt to recover deleted data;

- Conclusion and Recommendations. In this phase, the results of the analysis and evaluation of the selected erasing tools are documented. Recommendations of the top performing tools are also made during this phase of the project.

2. RELATED WORK

The digital forensics area has witnessed a plethora of contributions confirming and disproving major data concepts, and data erasure is not an exception. Data storage has immensely improved from the days of magnetic tapes and floppy disks to the more current forms of storage devices such as flash drives, electromechanical hard drives, Solid-State Drives (SSDs), and cloud storage. Most forms of storage, at the end of their lifecycles, are sold, donated, or destroyed.

Sahri et al. (2018) argued how fragile software and hardware involved in data storage could be and estimated the lifespan to be about five years. Other reports on the life expectancy of data storage devices were provided by (Brook, 2017), which highlighted that the lifespan of such devices depends on a number of factors, including usage rates, environmental factors, and manufacturing. In addition, (Brook, 2017) provided an estimated life expectancy for hard disks to be 3 to 5 years and flash storage devices to be 5 to 10 years, depending on the number of write cycles, meaning the more you delete and write new data on the devices, the faster the devices deteriorate.

The sanitization of media is of great importance to both corporate organizations and individuals. The NIST SP 800-88 Guidelines to Media Sanitization by the National Institute of Standards and Technology (2006) addresses the need for adequate media sanitization and the impact it has, if not properly conducted. The document categorizes media into two types; Hard Copy, which includes paper printouts, and Electronic or Soft Copy, which include hard drives, Random Access Memory (RAM), Compact and Floppy Disks etc. The document further explained the different types of sanitization. It grouped sanitization into four types, namely, Discarding, Clearing, Purging, and Destroying. Discarding involves getting rid of media without any sanitization method.

Discarding has consequences as reported in a news article by BBC (2019), where the medical records of patients, which had sensitive information such as bank and contact details were found in an abandoned nursing home in Hampshire. The second type of sanitization, Clearing, entails high levels of data destruction, which include overwriting using hardware or software tools. Purging is similar to Clearing and includes methods such as Secure Erase and Degaussing. Lastly, destroying as the name implies involves physically destroying media by shredding, melting, disintegration etc.

Countless data wiping techniques, in the form of software or hardware, have been adopted to aid in data erasure from storage media devices. Companies and individuals tend to purchase or freely download erasing tools to remove data on storage devices. Sansurooah et al. (2013) revealed that the licensing of such data erasing tools, whether freely available or commercial based, does not reflect on their data wiping efficiency and further recommended some free and commercial tools for secure data removal.

Martin and Jones (2011) argued in their paper, how inefficient some eraser tools can be and further pointed out how some files after supposed total wiping were still accessible using recovery tools.

Similar to the recommendations of the NIST Guidelines to Media Sanitization (2006), experts advise that one of the best and safest ways to destroy data from storage devices is to destroy these devices phys-

ically. According to (Veritysystems.com, 2017), smashing storage devices such as hard drives with a hammer is a faster and more direct method of getting rid of data. However, this method is considered wasteful and costly, especially for private individuals, and is not environmentally 'friendly.'

There are numerous software-based data erasing standards currently being used. These include the Peter Gutmann's Algorithm, Bruce Schneier's Algorithm, the US Department of Defense (DoD) 5220.22-M standard, Secure Erase, Random Data, Write Zero, the Russian GOST R 50739-95, the German VSITR method and the British HMG IS5, both Baseline and Enhanced.

One of the earliest erasing standards was the Peter Gutmann Algorithm, proposed by Peter Gutmann in 1996. Gutmann (1996) proposed an algorithm for erasing magnetic media, which implements 35 overwrite passes, with the first and last four passes being random data overwrites. However, Gutmann's algorithm is considered by most experts to be overkill and not relevant to modern drives. With the increasing size of storage media, it is also impractical as the time taken to erase a drive would be considerable. Wright et al. (2008) indicated that one overwrite is required for data wiping and that the misconception that recovery tools can retrieve gigabytes of data from erased media drives is unfounded.

Several methods that were previously examined in Wright et al., (2008) for the recovery of data from electromagnetic disks, including the Bitter technique, Lorentz microscopy, and Magnetic Force Microscopy, were discounted as unachievable given the developments in data storage densities of modern disks. For completeness these are detailed below:

- "The Bitter technique involves the coating of the platter with a thin film of ferro-fluid. This fluid contains ferro-particles that associate most strongly with the field vectors on the drive providing a magnetization pattern. This is known as "Bitter patterns" and maps to the magnetic field vectors. Depending on the track density, either a high powered optical microscope or a scanning electron microscope (SEM) can be used to observe the platters. This technique has become far less effective in recent times due to the increasing drive density. The technique is invasive and will result in the destruction of the drive platter.

- Lorentz microscopy uses an electron beam that is fired at the drive platter. Magnetic fields produce an effect known as the Lorentz force. This force deflects the electron beam. These deflections can be measured using a Scanning Electron Microscope (SEM). The SEM will then return the deflection pattern, which can be used to "map" the encoded drive image. More recently, Transmission Electron Microscopes (TEM) have been used for this process. This is a slow process that is economically infeasible for use on most modern hard drives.

- Magnetic Force Microscopy is a variety of imaging techniques known as Scanning Probe Microscopy (SPM). This technique uses an enormously fine (and expensive to replace) point that is mounted on a flexible cantilever. This tip "raster-scans" the drive platter following the magnetic force vectors. As the reader is coated with a ferromagnetic material, the field interactions attract or repel the tip. These movements are measured through the cantilever, allowing an accurate map of the magnetization-induced field to be produced. Magnetic Force scanning Tunnelling Microscopy

(MFSTM) is one form of MFM. This method uses the tunneling currents that are created through the movement of the probe to produce a two-dimensional spatial map of the magnetic field coordinates. This map is used to decode the "bits" on the drive."

Another popular erasing standard, the DOD 5220.22-M, was developed by the US National Industrial Security Program (NISP). It involves the 3 passes, namely: writing 0's and verify for Pass 1, writing 1's and verify for Pass 2, and for Pass 3; writing random characters and verify. There are other forms of DOD 5220.22-M, such as DoD 5220.22-M ECE, which has seven passes. Also, the Random Data method, as the name implies, overwrites the drive sectors with pseudorandom data in order to disrupt data recovery. Another widely-known erasing standard is the Write Zero standard, which is sometimes known as Single Overwrite or Zero-fill. It is an erasing standard that overwrites all sectors on the media with zeros in order to prevent data recovery (Disk-partition.com, 2019). The Write Zero standard is one of the fastest erasing standards, as discussed by Sansurooah et al. (2013) in their paper "An Investigation Into The Efficiency Of Forensic Data Erasure Tools For Removable USB Flash Memory Storage Devices." This is the standard that has been adopted for this research for the primary reason that it is possible to examine a disk that has been 'zeroed' and have a level of confidence in the results, whereas a disk that has been overwritten with pseudorandom characters would be much more difficult and time consuming to analyze. A disk that has been 'zeroed' can also easily have the hash compared to the original cleaned disk.

3. EREASING TOOLS

There are a large number of data erasing tools available on the internet, either for free download or under a commercial license. These tools use the earlier stated erasing standards to wipe and dispose of data. It should be noted that the tools to be used in this research have been selected mainly because of their easy accessibility, free license, and their ability to use the write zero method. The tools selected for the research are:

- *Active @ KillDisk* (`https://killdisk.com/eraser.html`): This is produced by LSoft Technologies Inc. This product has both free and commercial versions. Some of the limitations of the freeware version are that: it only supports only one pass zeros, no verification after erasing, no customization for certificates, and erase methods, and it is limited to two parallel disk erases.

- *Eraser* (`https://eraser.heidi.ie/`): This is produced by Heidi Computers and is free to use. The software erases previously deleted data and supports any drive that works with Windows. The latest version of Eraser is `6.2.0. 2982` and it allows users to specify file targets to be erased. The free version only provides the one pass zeros option, while the paid version offers the options of the DoD `5220.22.M` 3 pass and 7 pass and Peter Gutmann's Algorithms.

- *Disk Wipe* (`http://www.diskwipe.org/`): This is a free and portable erasing software for Windows. It supports DoD `5220.22-M`, Peter Gutmann's Algorithm, and other advanced erasing standards. It can be used to erase USB sticks, SD cards, and other portable memory devices.

- *Macrorit Data Wiper* (https://macrorit.com/): This is owned by Macrorit Inc and has both free and commercial software versions. Macrorit Data Wipe supports Windows and can also be used as bootable media (Commercial version only). The free version supports SSDs and does not include adware, spyware, and malware.

- *Super File Shredder* (http://www.kakasoft.com/): This is owned by Kakasoft Software Company Limited and is a free data destruction tool. It is compatible with Windows and supports Write Zero, DoD 5220.22-M, the Secure Erase algorithm with 7 passes, and Gutmann's Algorithm.

- Hard Wipe (https://www.hardwipe.com/): This is licensed by Big Angry Dog Ltd, is an erasing tool with both free and commercial versions. It supports Windows and bootable media (commercial version only). The free edition of Hard Wipe does not support verification of each pass. The latest version is 5.2.1 and is a 64-bit only software.

- *Puran Wipe Disk* (http://www.puransoftware.com/): This is owned by Puran Software and is a free software utility. The latest version of this tool is 1.2. Puran Software also provides other utility suites under its commercial license, such as a Registry Cleaner, a disk cleaner, a file recovery kit etc. Puran Wipe Disk is compatible with Windows and supports 1 pass, 3 passes, and 7 passes.

- Remo Drive Wipe (https://www.remosoftware.com/): This is licensed by Remo Software and has its latest software version as 2.0.0.25. It has both free and commercial versions. It is a Windows compatible tool and supports both 32-bit and 64-bit. The free version supports Write Zero, Random Data Overwrite, and the US DOD 5220.22-M.

It should be noted that two other erasing tools, namely, DBAN and CBL Data Shredder, were reviewed but not included in the experiments. Even though these tools are popular and easily accessible, there is a lack of technical support available, which implies that they are no longer supported. No recent updates were found for these tools.

Appendix A provides a visual summary of the selected erasing tools, giving details such as the name of the tool, the version number, their licenses, the Operating System (OS) needed to run the tool, the size of the downloaded setup file, and other relevant features of the tools:

3.1 Evaluation Tools

There are a number of tools that were used in the evaluation and analysis of the selected Data Erasers. These are detailed below:

- *USB Write Blocker*: This was used to prevent the operating system from writing to an attached device. This was used in the creation and analysis of the image of the wiped disk for analysis.

- *WinHex Editor*: This was used to examine, view, and analyze the physical contents of disk images.

- *Autopsy*: This is a forensic tool that is used in examining and viewing hex, strings, and metadata of files. It is the graphical interface to The Sleuth Kit and also used in providing search and data carving functions.

- *OSForensics*: This is a forensic software suite that performs similar functionalities as Autopsy. It was used in the

creation of images of wiped disks during the experiments.

- *Command Prompt "tasklist /v"*: this Windows CMD command was used to extract the CPU times and Memory Usage of the various data erasing tools.

3.2 Experimental Process

The experiments were conducted on a Windows 10 workstation with 64-bit Operating System, 2.5 GHz i7 CPU, and an 8 GB RAM. The Hard Disk used in the data wiping experiments was an 80 GB 3.5" electromechanical SATA drive. In addition, a Virtual Box, version 6.0.4, was used to run virtual workstations. During each experiment, the Hard Disk was initialized using the Master Boot Record (MBR) partition style and New Technology File System (NTFS) file system. In order to equally measure and evaluate each erasing tool, a known set of file types was copied onto the Hard disk for erasure. These are detailed below:

The file types occupied approximately 9 GB of the disk. This was done to allow for excess space on the disk, which would be evaluated when viewing unallocated clusters during the analysis of the various erasing tools. In evaluating each erasing tool, for consistency, individual experiments were conducted by following the processes listed below:

- Use a hardware tool to wipe a disk in which every sector was wiped with 0's and from which an MD5 hash value was created;
- Copy data set files onto the wiped disk and compare the MD5 sums of the files on the disk with their originals for verification;
- Run the erasing tool using the single-pass Write Zero method;
- Run tasklist[1] to capture the memory and CPU usage of the erasing tool;
- Disconnect disk on completion of disk erasure;
- Reconnect the Hard disk using the Write blocker software;
- Create an image of the erased disk;
- Import image of the erased disk for analysis, looking for details such as all zeros patterns, customized software signatures and any other unusual data in the disk sectors;
- Export and check the MD5 digests of the whole image and also any recovered files if found, comparing them to the original files;
- Analyze recovered files with Autopsy to carve fragments.

4. ANALYSIS OF TOOLS

The erasing tools were downloaded from their respective websites and installed. The analysis of each tool conformed to the following template:

- Review of claims made by the erasing tool;
- Assess how informative and user friendly the tool is;
- Record the running time, CPU time and Memory Usage of the tool;

[1]The TASKLIST command is used to display a list of currently-running tasks and displays the process ID number for each running task and the name of the executable program that started the task.

CATEGORIES	FILES TYPES
Image files	gif, png, bmp, psd, jpg
Executable files	exe, jar
Web files	html, htm, css, jsp ,json, js
System files	hiberfil, swapfile
Compressed files	zip, rar,
Disk Images	iso ,img
Backup files	tmp
Document and data files	txt, doc, docx, log, ppt, csv , pdf
Audio files	mp3, wav
Video files	mp4, avi, mkv
Database files	sql, sqlite
Spreadsheet files	xlsx
Uncategorized	md5, pm, cache files etc.

Figure 1. Summary of File Types used in the experiment

- Import wiped disk image to OSForensics, Autopsy and Win Hex for hash file comparison and raw disk viewing at sector level;
- Record outcome of disk analysis;
- Perform data recovery and carving from the wiped disk image if any artifacts found.

Below is the analysis of the data erasing tools:

4.1 Hard Wipe

Hard Wipe for desktop is a popular erasing tool that has a portable version, which enables users to boot from a USB drive. However, this functionality is limited to the professional version. The free version of Hard Wipe boasts support for Zero Overwrites, Random Data, GOST `R 50739-95`, `DOD 5220.22-M`, Schneier's Algorithm, German VSITR, and Gutmann's Algorithm. Hard Wipe claims permanent erasure of data on disks and other portable storage devices. It integrates with the Windows file explorer, which allows users to right-click in order to gain access to the software. The tool also has the facility for the cleaning of the recycle bin, page file, and free space. It has an informative and straightforward user interface that is easy to navigate. In addition to the benefits of Hardwipe, the tool provides a log report that informs users of vital information such as I/O Errors that occurred during wiping, failed items, and whether there was a verification pass. One disadvantage is that it contains an advertise-

ment panel, which is found in the window of the tool. Also, Hard Wipe does not allow the wiping of an active running Windows drive.

4.1.1 Analysis

During the analysis phase, the md5 checksum of the image of the wiped disk corresponded with that of the baseline hardware-wiped disk, *1b26c0e62b79f528793199a3d2de4034*. This initial outcome suggested complete disk erasure, but further analysis of the wiped disk was conducted to confirm this hypothesis. The run time, CPU time, and memory usage used by the tool in wiping the disk are shown below:

The wiped disk image, when viewed in WinHex showed a total of `80,026,361,856` bytes with every byte being 0's, including the boot sector. This outcome implied that the disk was wiped completely.

4.2 Eraser

Eraser is a free, simple, and easy to use erasing tool that possesses many features. It supports Windows XP (Service Pack 3), Vista, Windows Server 2003 (Service Pack 2), Server 2008, Server 2012, Server 2016, Windows 7, 8, and 10. Eraser is also regarded as a file eraser due to its ability to erase user-specified files and folders. It allows the erasure of the recycle bin, unused disk space, partitions, SSDs, and electromechanical drives. It possesses the ability for data erasure to be scheduled for a specified time and provides users the option to set recurring data erasure either daily, weekly, or monthly. Eraser boasts supporting a variety of erasing standards namely: Pseudorandom data, British HMG IS5 (Baseline), British HMG IS5 (Enhanced), Russian GOST P50739-95, US Army AR380-19, DOD 5220.22-M (E), DOD 5220.22-M (ECE), US Air Force 5020, Canadian RCMP TSSIT OPS-II, German VSITR, and Schneier's Algorithm. It should be noted that the British HMG IS5 (Baseline) is similar to the Write Zero method. Also, Eraser permits a user to unlock locked files for erasure and also replace erased files with user-selected folders or files. The downside of the tool is its high memory usage and CPU time as compared to the other erasing tools. Another demerit is its inability to provide ample information during data wiping. Lastly, it does not allow the wiping of an active running Windows drive.

4.2.1 Analysis

Below are the details of the run time, CPU time, and memory usage of the tool: During disk analysis, it was found that the md5 checksum of the wiped disk image was *1e74a04dc99e2d938458047a942db2df*, which differed from that of the hardware-wiped disk, *1b26c0e62b79f528793199a3d2de4034*, and as a result, warranted further examination. The Eraser-wiped disk image was analyzed, firstly using WinHex to determine what accounted for the md5 checksum discrepancy. It was observed that the boot sector still contained 512 bytes of data. Also, during the analysis of the disk image with OSForensics, it was discovered that there were data in the last sector of the disk. This observation denoted that Eraser did not wipe the FAT2 portion of the disk. The wiped disk image was subjected to data recovery and carving using both OSForensics and Autopsy, which yielded no results. There was no evidence of Images, Videos, Audio, databases, archives, and other deleted files. Indexes could not be created using OSForensics due to the absence of recovered file types from the image.

4.3 Macrorit Data Wiper

Macrorit Data Wiper is a data wiping software that has both free and commercial versions and supports Windows XP, Vista, Windows Server 2003, 2008, 2012, Home Server 2011, Windows 7, 8, and 10. Macrorit Data Wiper also supports bootable media, but this

Run Time (mm:ss)	CPU Time (h:mm:ss)	Memory Usage
28:37	0:00:15	37,920 K

Figure 2. Run Time, CPU Time and Memory Usage of Hard Wipe

Run Time (mm:ss)	CPU Time (h:mm:ss)	Memory Usage
28:39	0:04:03	84,004 K

Figure 3. Run Time, CPU Time and Memory Usage of Eraser

is limited to the commercial version. The tool allows users to wipe the recycle bin, partitions, external drives such as USB flash drives and memory sticks, and entire hard or Solid-State drives. Macrorit Data Wiper does not wipe optical storage media such as compact disks, optical disks (DVD) etc., and prescribes that these media should be physically destroyed. Macrorit Data Wiper claims permanent data erasure with no possibility of recovery. It also boasts of high-speed drive wipes and not using large amounts of system resources. Macrorit Data Wiper supports the following erasing standards: write zeros (1 pass), pseudorandom data (1 pass), zero and one writes (2 passes), DoD 5220.22-M (3 passes), DoD 5220.28-STD (7 passes), and the Gutmann's Algorithm (35 passes). The tool has a very simple and uncomplicated User Interface. Another advantage of the tool is that it provides users with a confirmation window before data wiping. This is to prevent the erasure of wrong storage media devices. Despite its advantages, Macrorit Data Wiper is unable to wipe the primary drive that has an active-running Windows OS installed.

4.3.1 Analysis

During the analysis phase, the erasing tool showed a minimal number of CPU cycles. Below are details of its system usage when the tool was run: The MD5 checksum of the wiped disk was *925860097154ed5eab45ec6724650a86*, which did not correspond with that of the Hardware wiped disk. Further disk analyses were conducted in an attempt to determine the reasons for the discrepancy. Firstly, the wiped disk was viewed in WinHex to view the individual sectors. WinHex showed that the boot sector contained data in the first 512 bytes, and the rest of the sectors were zeroed out. This implied that Macrorit Data Wiper ignored the first sector and started data sanitization afterward.

The hypothesis of Macrorit Data Wiper ignoring the first sector was confirmed again when the wiped disk was viewed using OSForensics' Raw Disk Viewer. The rest of the sectors were filled with 0's.

Lastly, the wiped disk was imported into Autopsy to confirm all files, including System Volume was erased completely. The unallocated blocks did not produce any contents hence confirming the hard disk was wiped clean with the exception of the first 512 bytes.

4.4 Active KillDisk

Active KillDisk is a feature-filled data sanitization software that has a detailed and attractive user interface. It is a portable erasing tool that provides complete data wiping on electromechanical disks, solid-state drives,

Run Time (mm:ss)	CPU Time (h:mm:ss)	Memory Usage
28:41	0:00:13	38,152 K

Figure 4. Run Time, CPU Time and Memory Usage of Macrorit Data Wiper

USBs and Memory sticks etc. It has both free and commercial versions with the freeware version supporting Windows, MacOS, and bootable media. Active KillDisk boasts of parallel erasing where multiple drives can be wiped simultaneously and independently. It also has its own "Disk Viewer", for analysis of specified devices, its own "File Browser", and the ability to wipe both unused drive clusters and slack space in file clusters.

Active KillDisk provides users with the option to customize the first sector with a user-specified fingerprint or signature. In addition, it provides a report and certificate of erasure, which comprises of notable information such as the duration and status of erasure, and the erase method used. Lastly, Active KillDisk allows users to have control of handling read/write errors by providing options, including aborting entire disk erasure or aborting only failed items from group processing.

Even though Active KillDisk supports many erasing standards such as US DoD 5220.22-M and British HMG IS5 Baseline, the free version is limited to only the One Pass Zero.

4.4.1 Analysis

The results from running the "tasklist /v" command also showed an unfavorable quality in terms of its memory usage and showed that it uses enormous amounts of memory as compared to the other erasing tools. Below are details of the run time, CPU Time and Memory Usage of the erasing tool:

It was found that the md5 checksum of the wiped disk image was *948685d2633821f0533fdfc3fbcc86da*, which was different from that of the hardware-wiped disk image. Using WinHex, it was observed that all the sectors were zeroed, with the exception of the first 512 bytes. The disk image was imported into OSForensics' Raw Disk Viewer To confirm that all of the other sectors were 0's and that disk erasure started after the boot sector. The results from OSForensics were similar to those of WinHex showing O's in every sector apart from that of the boot sector.

4.5 Disk Wipe

Disk Wipe is a free and portable data sanitization tool licensed under a EULA license. It is designed for personal use and supports only the Windows Operating System. Disk Wipe claims permanent erasure of data on disk partitions and volumes and also erases complete electromechanical hard disks and Solid-State Drives. It has an attractive and easy-to-use User Interface. Disk Wipe provides users the option to view contents of specified drives and also allows users to skip some wizard pages such as the 'File System' page and 'Confirmation' page.

The tool supports seven erasing standards namely: One Pass Zeros, One Pass Random, Russian `GOST P50739-95 (2 passes)`, `British HMG IS5 (3 passes)`, `DoD 5220.22-M(E) (3 passes)`, `DoD 5220.22-M(ECE) (7 passes)` and `Gutmann's Algorithm (35 passes)`.

During the erasure of the disk using the One Pass Zero method, it was discovered that Disk Wipe performs an extraneous and

Run Time (mm:ss)	CPU Time (h:mm:ss)	Memory Usage
28:43	0:00:51	115,632 K

Figure 5. Run Time, CPU Time and Memory Usage of Active KillDisk

unneeded for wiping pattern (Secure Erase), which lengthens the run time of the tool.

4.5.1 Analysis

It was observed that the run time of Disk Wipe was almost twice that of most erasing tools under review; this is due to the extra Secure Erase performed during the disk wiping process. Below are details of the run time, CPU Time and Memory Usage of the erasing tool:

4.6 Puran Wipe Disk

Puran Wipe Disk is a data sanitization tool which is produced by the Puran Software group. It has both free and commercial software versions with the free version intended for personal and non-commercial use. It supports only Windows OSs and is compatible with Windows XP, Vista, Windows Server 2003, 2008, Windows 7, 8, and 10. Puran Wipe Disk claims complete wiping of disks, including the file system and all free disk space. It also supports the wiping of multiple disks simultaneously. The Puran Wipe Disk tool has a very simple and presentable user interface and supports three data erasing standards, namely: Write Zero, DoD 5220.22-M, and Schneier's Algorithm. However, the tool refers to the erasing standards differently as; 1 pass (faster and secure enough), 3 passes (slower and more secure), and 7 passes (extremely secure and slow).

The downside to using Puran Wipe Disk is the tool's inability to wipe an active running Windows drive. It also does not provide a log report after completion of erasure.

4.6.1 Anlysis

It was observed that the run time of Puran Wipe Disk was similar to that of the majority of the other tools being reviewed. It also had a fairly low CPU Time as compared to the other erasing tools. Below are details of the run time, CPU Time and Memory Usage of the erasing tool: On analysis of the disk image, it was discovered that md5 checksum of the Puran Wipe Disk was *f73fc8a0f499c5f226d87543d24a351d*, which did not match with that of the Hardware image. The wiped image was then imported into WinHex to determine whether the boot sector and the other sectors were completely wiped. WinHex showed that the boot sector and the remaining space on the disk were wiped clean with all bytes being 0's. OSForensics also showed all the disk sectors, including the boot sector to be zeroed. The reason for the discrepancy in the md5 checksums could not be determined.

The observation from the analysis performed on Puran Wipe Disk confirmed complete disk erasure.

4.7 Remo Drive Wipe

Remo Drive Wipe is a Windows based erasing tool that supports both 32-bit and 64-bit versions of Windows 10, 8, 7, Vista, XP as well as Windows 2003, 2008 and 2012. It has both free and commercial licenses; both intended to completely wipe disks and logical drives. The tool supports 9 data sanitization standards, but the free version is limited to just three standards, namely: Fast Zero Overwrite, Random Overwrite, and the US DOD 5220.22-M . Remo Drive Wipe has a simple

Run Time (mm:ss)	CPU Time (h:mm:ss)	Memory Usage
65:32	0:01:25	23,216 K

Figure 6. Run Time, CPU Time and Memory Usage of Disk Wipe

Run Time (mm:ss)	CPU Time (h:mm:ss)	Memory Usage
28:51	0:00:07	39,424 K

Figure 7. Run Time, CPU Time and Memory Usage of Puran Wipe Disk

and attractive design, and it provides an informative user interface that makes it easy for users to navigate the software. The tool also provides users with a log report to provide feedback after the completion of erasure.

4.7.1 Analysis

The observation made after the running of Remo Drive Wipe showed that the run time was longer as compared to most of the other erasing tools under review. Below are the run time, CPU Time and Memory Usage of the erasing tool:

The md5 checksum of the disk image from this tool matched with that of the Hardware-wiped disk image - *1b26c0e62b79f528793199a3d2de4034*. Analysis with WinHex confirmed that all sectors, including the boot sector, wiped and overwritten with 0's.

4.8 Super File Shredder

Super File Shredder, as the name implies, is a file shredder that is used to destroy and remove files from storage devices. It is a free erasing tool that supports only the Windows OS and is compatible with Windows 2000, XP, 2003, Vista, Windows 7, 8, and 10. It claims complete erasure of unwanted files, folders and free space on drives.

Super File Shredder supports 4 erasing standards, namely, Simple One Pass (Write Zero), DoD 5220.22-M, Secure Erasing Algorithm with 7 passes, and Gutmann's Algorithm (35 passes). Super File Shredder has a simple and an easy-to-use user interface, as shown above. The erasing tool also integrates with Windows Explorer, which allows users to right-click in order to gain access to the software.

4.8.1 Analysis

After the running of Super File Shredder, it was observed that the run time was similar to that of most of the other tools under review. Below are details of the run time and system resource usage of the erasing tool:

The md5 checksum of the wiped disk image, *4c0f90e5b4e87adc100fadd9fdf897f7*, varied from that of the Hardware-wiped disk image, and as a result, an additional, more comprehensive analysis was undertaken.

The wiped disk image was imported into WinHex, and it was observed that the boot sector contained data. OSForensics also confirmed this hypothesis, which meant that Super File Shredder did not wipe the boot sector. Interestingly, OSForensics recovered a number of files from the disk image. The Searched Indexes, which included pre-defined types such as emails and attachments, zip and compressed archives, images, and text files, produced 30 results. The results from the search included System Volume Infor-

Run Time (mm:ss)	CPU Time (h:mm:ss)	Memory Usage
35:17	0:06:24	34,624 K

Figure 8. Run Time, CPU Time and Memory Usage of Remo Drive Wipe

Run Time (mm:ss)	CPU Time (h:mm:ss)	Memory Usage
24:33	0:01:19	31,992 K

Figure 9. Run Time, CPU Time and Memory Usage of Super File Shredder

mation files, $Extend files, $RECYCLE.BIN files, $LogFile , $MFT, $Volume, $Bitmap, and other NTFS metadata files. The System Volume Information folder comprised of IndexerVolumeGuid and WPSettings.dat files. The $Extend folder included the $TxfLog.blf file and other log files. Also, the $RECYCLE.BIN folder contained a desktop.ini file, which is a Windows file that stores customization details of folders (Computerhope.com, 2018).

In attempts to recover more system files and possibly known user files, the disk image was imported into Autopsy and scanned. Autopsy recovered 2035 Orphan files from unallocated clusters, which had no data stored in them but had valid modified, accessed, and created dates.

Autopsy also confirmed the results from OSForensics by showing the $Extend files, $RECYCLE.BIN folder, and System Volume Information files. In addition to the system files, Autopsy recovered four known directories, but these directories had no files in them apart from one that had one known video file. The video file showed a known filename and type but had a size of 0 bytes and null metadata dates.

Lastly, Autopsy recovered an additional 30 PNG image files, two archive files, one office document file, and one database file. These recovered files, similar to the previously recovered video file, had known filenames but null metadata dates. Also, the md5 sums of all the known recovered files were not the same as those of the original files.

Based on the analysis of the disk image, it can be concluded that some files, even though having a size of 0 bytes, had valid filenames and could be recovered after erasure using Super File Shredder. Super File Shredder also failed to erase a number of system files from the disk.

5. CONCLUSIONS

The experiments conducted on each erasing tool produced a range of results. Some tools completely wiped the entire disk, including the boot sector. Other tools also wiped the disk but excluded the boot sector, and one tool, while removing the content of a number of files, still contained a number folder and file names. Appendix B gives a summary of the analyses of the erasing tools under review.

There are several conclusions that can be drawn from the analysis performed on the data erasing tools. First and foremost, the successful and complete wiping of the disk by some of the erasing tools such as Hard Wipe and Puran Wipe Disk confirmed that the write zero method is sufficient for disk erasure. Also, a single overwrite pass is enough

to completely wipe a disk as Wright et al. (2008) indicated in their paper, "Overwriting Hard Drive Data: The Great Wiping Controversy". Although one pass overwrite is not necessarily sufficient to make any potential future recovery of the data infeasible, it is adequate for the cleaning of personal disks. It is advised that all erasing tools should have verification after each pass they perform and that this should be displayed to users to provide feedback on erasure.

Another conclusion derived from the analysis relates to the system resources of the host machine. Based on the experiments performed, it can be deduced that there is no direct correlation between the system resources (CPU time and Memory Usage) and the effectiveness of the erasure tool.

It was observed that Active KillDisk had the highest memory usage of 115 MB while Remo Drive Wipe had the highest CPU time of 6 minutes 24 seconds.

In addition, it was concluded that some erasing tools do not address the boot sector of the disk that is being erased and start the overwrites after the first sector. This can be seen in tools such as Macrorit Data Wiper and Active KillDisk. In this context, data found in the boot sector of a disk does not infer that files, either user or system files, can be recovered or carved from the disk being erased.

After compiling the summary of the analysis, it was also observed that five of the erasing tools (i.e., Hard Wipe, Eraser, Macrorit Data Wiper, Active KillDisk, and Puran Wipe Disk) had similar run times ranging from 28 minutes 37 seconds to 28 minutes 51 seconds. This may suggest that these tools use either an identical or very similar base code or algorithm in building their erasing software.

Lastly, the results of the analysis confirmed some of the conclusions drawn by Sansurooah et al. (2013) and one by Martin and Jones (2011). Sansurooah et al. (2013) concluded that free erasing tools could securely and permanently erase storage devices. This theory was confirmed in the outcome of the analysis of tools such as Hard Wipe and Puran Wipe Disk, where the disks were wiped clean, and no data was recovered. In the case of Martin and Jones (2011), it was discussed that file erasers fail to erase some system generated files. This hypothesis was confirmed when Super File Shredder, a well-known file eraser, failed to completely wipe system files such as $Extend files and the $RECYCLE.BIN folder. It was also deduced that the file eraser removed files but ignored some directories, thereby keeping the file structure.

5.1 Recommendations

Based on the results of the various experiments, it can be recommended that for an effective and secure erasing of an entire disk, Hard Wipe, Remo Drive Wipe, and Puran Wipe Disk should be considered. Complete disk erasure means total wiping of the entire disk, which includes the boot sector. The three previously mentioned erasing tools achieved this by wiping the entire disk completely.

Secondly, file erasers should be avoided if the intention is to wipe an entire disk since they have the tendency of ignoring the file system, some directory names, and system generated files. As a result, Super File Shredder was the least effective erasing tool that was reviewed. The disk image wiped by Super File Shredder still contained known directory names and even some known file names. This can be detrimental to owners who want to permanently erase unwanted traces of activity from their storage device.

Lastly, it is advised that users avoid data erasing tools that are obsolete and not being supported and updated. The reason behind this recommendation is that outdated tools no longer receive technical support, hence

during instances where there are software errors and bugs, expert assistance cannot be consulted, and as new versions of operating systems are brought into use, there is no guarantee that the tools will work effectively on them.

5.2 Future Work

The area of the forensic analysis of data on storage media is far from exhausted. From the analyses and experiments performed in this project, it is our hope that improvements can be made to enhance testing in order to make more concrete conclusions and recommendations. Future experiments will involve a number of adjustments, such as using other popular erasing standards, for example, DoD 5220.22-M, pseudorandom data, and Schneier's Algorithm for disk wiping. This is to test if the recommended tools from this report perform equally well using other methods.

Secondly, future experiments in data erasing will include a Solid-State Drive (SSD) in place of an electromechanical hard drive. The rationale behind this notion is because of the different ways these two types of storage drives store data. SSDs store data on interconnected microchips and have wear levelling software embedded while hard drives store data on a rotating platter, which implies there may be a need for different ways of wiping these two types of drives. Similar tests performed in this research will be conducted to determine if SSDs can be easily and completely erased, and the results verified. In addition, future tests will include an assessment of the base codes of multiple erasing tools. This is because of the suspicion derived from the research in relation to the very similar run times of the reviewed tools and to determine if the erasing tools use a similar production code.

Lastly, GUID Partition Table (GPT) will be used as a partition style in place of Master Boot Record(MBR). This is because GUID drives use Unified Extensible Firmware Interface (UEFI) BIOS, which supports more than four partitions on a disk and also supports disk partitions that are larger than 2 TB. GPT can support up to a maximum disk capacity of 9.4 ZB. As a result of using the GUID partition style, a larger number of files can be used as datasets, and also larger storage devices can be used in conducting experiments. This will aid in checking if these popular erasing tools have a maximum storage capacity they can wipe.

6. GLOSSARY

- **CPU Time:** is the measure of how much CPU cycles have been used since the start of a process (Intel, 2019).
- **Degaussing:** involves the introduction of strong magnetic fields to a magnetic media in attempts to destroy the magnetic components of the device (National Institute of Standards and Technology, 2006).
- **GUID Partition Table:** GUID stands for Globally Unique Identifier, and it is a new disk partition architecture that acts as an improvement of the MBR partition scheme because of its partition size capacity and other advantages (Diskgenius.com).
- **MBR:** stands for Master Boot Record and is a type of boot sector stored in storage devices that holds information on how to start the boot process (Fisher, 2018).
- **Media Sanitization:** is the process of ensuring confidentiality by effectively erasing unwanted data from media sources (National Institute of Standards and Technology, 2006).

- **Orphan files:** are deleted file items that still have their metadata in the file system.
- **System Volume Information:** is a hidden system location on computer partitions that is used by the system's repair tools to save restore points and other related data of the computer system (Verma, 2017).
- **$Bitmap:** is a volume representation which indicates the clusters that are allocated (NTFS.com)
- **$LogFile:** is a log file used by NTFS in recovery after a system crash (NTFS.com).
- **$MFT:** is a file that contains information of all files on the NTFS volume (NTFS.com).
- **$TxfLog.blf:** TxF stands for Transactional NTFS, and it is a temporary log file used in backing up transactions to prevent sudden crashes.
- **$Volume:** is a file that stores volume details such as volume version, flags, and labels (NTFS.com).

REFERENCES

[1] Brook, M. (2017). Data storage lifespans: how long will media really last? - Media Releases - CIO. [online] CIO. Available at: https://www.cio.com.au/mediareleases/29049/data-storage-lifespans-how-long-will-media-really/ [Accessed 8 Mar. 2019].

[2] Computerhope.com. (2018). What is the Windows desktop.ini file and can I delete it? . [online] Available at: https://www.computerhope.com/issues/ch001060.html [Accessed 25 Apr. 2019].

[3] Datasecurityinc.com. SSD vs. HHD. [online] Available at: http://datasecurityinc.com/solid_state_storage_devices.html [Accessed 28 Apr. 2019].

[4] Diskgenius.com. MBR VS GPT, which is the best choice for your computer? . [online] Available at: https://www.diskgenius.com/how-to/mbr-vs-gpt.php#03-2 [Accessed 28 Apr. 2019].

[5] Disk-partition.com. (2019). How to Write Zeros to a Hard Drive Effortlessly? . [online] Available at: https://www.disk-partition.com/articles/write-zeros-to-hard-drive-8523.html [Accessed 17 Apr. 2019].

[6] Diskwipe.org. Disk Wipe - Free software. [online] Available at: http://www.diskwipe.org/ [Accessed 8 Mar. 2019].

[7] Eraser. Eraser – Secure Erase Files from Hard Drives. [online] Available at: https://eraser.heidi.ie/ [Accessed 8 Mar. 2019].

[8] Fisher, T. (2019). 40 Free Programs to Completely Wipe Data From Hard Drives. [online] Lifewire. Available at: https://www.lifewire.com/free-data-destruction-software-programs-2626174 [Accessed 7 Mar. 2019].

[9] Fisher, T. (2018). Data Sanitization Methods: Everything You Need to Know. [online] Lifewire. Available at: https://www.lifewire.com/data-sanitization-methods-2626133 [Accessed 8 Mar. 2019].

[10] Fisher, T. (2018). What's an MBR and How to You Repair MBR Problems? . [online] Lifewire. Available at:

https://www.lifewire.com/what-is-a-master-boot-record-mbr-2625936 [Accessed 30 Apr. 2019].

[11] Gutmann, P. (1996). Secure Deletion of Data from Magnetic and Solid-State Memory. In: The Sixth USENIX Security Symposium.

[12] Hardwipe.com. Hardwipe - Data Sanitization Security Toolset. [online] Available at: https://www.hardwipe.com/ [Accessed 8 Mar. 2019].

[13] Historycoalition.org. (2009). NARA Provides Update on Missing Clinton Hard Drive – National Coalition For History. [online] Available at: http://historycoalition.org/2009/07/24/nara-provides-update-on-missing-clinton-hard-drive/ [Accessed 7 Mar. 2019].

[14] Kakasoft.com. Kakasoft: USB Security, Copy protection, File/Folder Locking Software. [online] Available at: http://www.kakasoft.com/ [Accessed 19 Apr. 2019].

[15] Killdisk.com. How to erase hard drive by Active@ KillDisk? Disk Eraser, Disk Wiper, Disk Format Disk Sanitizer. [online] Available at: https://killdisk.com/eraser.html [Accessed 8 Mar. 2019].

[16] Macrorit.com. Permanently Erase Data with Free Data Wiper. [online] Available at: https://macrorit.com/free-data-wiper.html [Accessed 8 Mar. 2019].

[17] Martin, T. and Jones, A. (2011). An evaluation of data erasing tools. In: 9th Australian Digital Forensics Conference. [online] Perth Western Australia: Edith Cowan University, pp.85-92. Available at: https://ro.ecu.edu.au/adf/ [Accessed 8 Mar. 2019].

[18] Moore, B. (2019). Medical records left in abandoned nursing home. [online] BBC News. Available at: https://www.bbc.co.uk/news/av/uk-england-hampshire-47860424/thousands-of-patient-files-left-in-westbury-house-nursing-home?intlink_from_url=https\%3A\%2F\%2Fwww.bbc.co.uk\%2Fnews\%2Ftopics\%2Fc0ele42740rt\%2Fdata-breaches&link_location=live-reporting-map [Accessed 18 Apr. 2019].

[19] National Institute of Standards and Technology (2006). NIST SP 800-88, Guidelines for Media Santification. Gaithersburg, Maryland: U.S. Government Printing Office.

[20] NTFS.com. NTFS System Files. [online] Available at: http://www.ntfs.com/ntfs-system-files.htm [Accessed 25 Apr. 2019].

[21] Puransoftware.com. Puran Software - Quality First. [online] Available at: http://www.puransoftware.com/ [Accessed 19 Apr. 2019].

[22] Remosoftware.com. Remo Software - Tools to Recover, Repair, Erase, Manage Optimize Data. [online] Available at: https://www.remosoftware.com/ [Accessed 19 Mar. 2019].

[23] Rothke, B. (2009). Why Information Must Be Destroyed, Part Two. [online] CSO Online. Available at: https://www.csoonline.com/article/2123985/why-information-must-be-destroyed--part-two.html [Accessed 18 Apr. 2019].

[24] Sahri, M., Huda Sheikh Abdulah, S., Firham Efendy Md. Senan, M., Yusof, N., Zarina Binti Zainal Abidin, N., Bin Shaiful Azam, N. and Josalmin Bin Tajul Ariffin, T. (2018). The Efficiency of Wiping Tools in Media Sanitization. In: 2018 Cyber Resilience Conference (CRC). [online] IEEE. Available at: https://ieeexplore.ieee.org/document/8626824 [Accessed 8 Mar. 2019].

[25] Sansurooah, K., Hope, H., Almutairi, H., Alnazawi, F. and Jiang, Y. (2013). An Investigation Into The Efficiency Of Forensic Data Erasure Tools For Removable Usb Flash Memory Storage Devices. In: 11th Australian Digital Forensics Conference. Perth, Western Australia: Edith Cowan University.

[26] Software.intel.com. (2019). CPU Time. [online] Available at: https://software.intel.com/en-us/vtune-amplifier-help-cpu-time [Accessed 19 Apr. 2019].

[27] Stiennon, R. (2017). Everything You Need to Know About DoD 5220.22-M Wiping Standard. [online] BTG English. Available at: https://www.blancco.com/blog-dod-5220-22-m-wiping-standard-method/ [Accessed 8 Mar. 2019].

[28] Valli, C. and Jones, A. (2005). A UK and Australian Study of Hard Disk Disposal. In: 3rd Australian Computer, Network and Information Forensics Conference. [online] Perth, Western Australia: School of Computer and Information Science, ECU, pp.74-78. Available at: https://ro.ecu.edu.au/ecuworks/2763/ [Accessed 17 Apr. 2019].

[29] Veritysystems.com. (2017). What is the best way to destroy a hard drive? | VS Security. [online] Available at: https://www.veritysystems.com/uk/news-blog/what-is-the-best-way-to-destroy-a-hard-drive/ [Accessed 8 Mar. 2019].

[30] Verma, A. (2017). What Is System Volume Information Folder In Windows? How To Access And Shrink It? . [online] Fossbytes. Available at: https://fossbytes.com/system-volume-information-folder-windows-shrink/ [Accessed 24 Apr. 2019].

[31] Warburton, D. (2019). Terror threat as Heathrow Airport security files found dumped in the street. [online] Mirror. Available at: https://www.mirror.co.uk/news/uk-news/terror-threat-heathrow-airport-security-11428132 [Accessed 7 Mar. 2019].

[32] Wright, C., Kleiman, D. Sundhar R.S, S. 2008“ "Overwriting Hard Drive Data: The Great Wiping Controver”y" in Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 243-257.

[33] Drolet, M. (2019). What does stolen data cost [per second]. [online] CSO Online. Available at: https://www.csoonline.com/article/3251606/what-does-stolen-data-cost-per-second.html [Accessed 17 Apr. 2019].

Figure 10. Appendix A - Summary of Data Erasing Tools evaluated

NAME	VERSION	LICENSE	OS	SETUP SIZE	FEATURES
Remo Drive Wipe	2.0.0.25	Free and Commercial	Windows	15.6 MB	-Free version supports Write Zero, Random Overwrite and the US DOD 5220.22-M. -Commercial version supports DoD 5220.22-Mtmann's's's Algorithm, VSITR etc.
Active KillDisk	11.1.23.0	Free and Commercial	Windows, Mac (Freeware) and Bootable (Commercial)	72.9 MB	-Freeware supports only one pass Zeros. -Commercial versions support DoD 5220.22-M, DoD 5220.22-M (ECE), DoE M205.1-2, German VSITR, British HMG IS5 Baseline , British HMG IS5 Enhancedtmann's's's Algorithm etc.
Puran Wipe Disk	1.2	Free and Commercial	Windows	1.37 MB	-Supports 1 pass (Write Zero), 3 passes and 7 passes.
Super File Shredder	4.2	Free	Windows	2.18 MB	-Supports Simple One Pass, DoD 5220.22-M, Secure erasing algorithm (7 passes) anGutmann's's Algorithm.
Eraser	6.2.0.2982	Free	Windows	8.67 MB	-Supports pseudorandom data, British HMG IS5 (Enhanced), British HMG IS5 (Baseline), DoD 5220.22-M, DoD 5220.22-M (ECE), US army AR380-19, German VSITR, Bruce Schneier's Algorithm etc.
Disk Wipe	1.7	Free	Windows	1.05 MB	-Portable, no installation needed. -Supports DoD 5220.22-Mtmann's's's Algorithm, One Pass Zeros, Pseudorandom data etc. -No adware
Macrorit Data Wiper	4.6.0.0	Free and Commercial	Windows & Bootable (Commercial only)	9.09 MB (.zip)	-Supports pseudorandom data, DoD 5220.22-M, Gutmann's Algorithm, etc.
Hard Wipe	5.2.1	Free and Commercial	Windows & Bootable (Commercial only)	9.67 MB	-Supports pseudorandom data, Write Zero, DoD 5220.22-Mtmann's's's Algorithm, Bruchneier's's's Algorithm etc.

Figure 11. Appendix B - Results from the analysis of the data erasing tools

Erasing Tool	Run Time (mm:ss)	CPU Time (mm:ss)	Memory Usage	Ability to erase boot sector	Ability to erase all files	Ability to erase System Volume Information	Recovered file/folder
Hard Wipe	28:37	00:15	37,920 K	Pass	Pass	Pass	No
Eraser	28:39	04:03	84,004 K	Fail	Pass	Pass	No
Macrorit Data Wiper	28:41	00:13	38,152 K	Fail	Pass	Pass	No
Active KillDisk	28:43	00:51	115,632 K	Fail	Pass	Pass	No
Disk Wipe	65:62	01:25	23,216 K	Fail	Fail	Fail	No
Puran Wipe Disk	28:51	00:07	39,424 K	Pass	Pass	Pass	No
Remo Drive Wipe	35:17	06:24	34,624 K	Pass	Pass	Pass	No
Super File Shredder	24:33	01:19	31,992 K	Fail	Fail	Fail	Yes

