12-4-2013

An Investigation Into The Efficiency Of Forensic Data Erasure Tools For Removable Usb Flash Memory Storage Devices

Krishnun Sansurooah
Edith Cowan University

Haydon Hope
Edith Cowan University

Hani Almutairi
Edith Cowan University

Fayadh Alnazawi
Edith Cowan University

Yunhan Jiang
Edith Cowan University

DOI: 10.4225/75/57b3d94cfb875
11th Australian Digital Forensics Conference. Held on the 2nd-4th December, 2013 at Edith Cowan University, Perth, Western Australia

AN INVESTIGATION INTO THE EFFICIENCY OF FORENSIC DATA ERASURE TOOLS FOR REMOVABLE USB FLASH MEMORY STORAGE DEVICES

Krishnun Sansurooah, Haydon Hope, Hani Almutairi, Fayadh Alnazawi, and Yunhan Jiang
School of Computer and Security Science, Edith Cowan University
Security Research Institute, Edith Cowan University
Perth, Australia
k.sansurooah@ecu.edu.au

Abstract
Securely erasing data is of key importance to anyone that is concerned with the security of their sensitive information, whether an individual or an organization. Simply deleting the data in question or formatting the storage device is not enough to ensure that the data cannot be recovered. Furthermore, with the uptake of Universal Serial Bus drives (USBs) flash memory based storage devices have replaced previous portable secondary storage media. Therefore, it is of a major concern whether these tools and products developed for securely erasing data secondary storage Hard Disk Drives (HDDs) would be as efficient when targeting the USB flash memory storage devices. With a wide range of open source and commercial products available on the market, all claiming, among other things, to be able to securely delete your data, it is quite a difficult task for the consumer to pick the most efficient product. This paper therefore discusses the results of experiments conducted with both the open source and commercial tools which claim to securely delete data off USB flash memory storage devices.

Keywords
Digital forensics, USB flash memory storage devices, data recovery, data erasure, data disposal and remnant data.

INTRODUCTION

Portable digital data has shown an exponential growth with the evolution and advancement of electronic devices (Sudan, Badam, & Nellans, 2012). With increased mobility, individuals and corporate end-users need to travel light and be fully connected. As a result, there has been an increase in the number of portable devices that are being used such as laptops, notebooks, Universal Serial Bus (USB) flash memory storage devices, Personal Digital Assistants (PDAs) and advanced mobile phones which have gained enormous popularity and are used by millions of people across the world (Jones, Valli & Dabibi, 2009). Therefore, it is of no surprise that the above mentioned devices are now increasingly players in the evidentiary process (Choo, Smith & McCusker, 2009; Goodin, 2012). With individuals and employees using mobile devices and travelling with data whilst taking work home, organizations are continuously being exposed to unprotected data on USB flash memory storage devices. The repercussions can be catastrophic such as loss of jobs, loss of reputation and loss of profit to name a few. (Kingston, 2012).

USB flash memory storage devices, more commonly known as USB flash drives, are widely preferred because of their size, huge storage capabilities and their weight, all making them highly portable (Hu, 2004). However, with convenience and mobility come risks. These devices, along with the volume of confidential data they can potentially contain, are easily lost, stolen or misplaced. Personal or corporate data, business plans, financial information, patient's records and confidential information are only some instances of data that are commonly saved and transported on the USB storage devices. In fact, a large number of end-users are unconscious of their exposure to security risks if the contents of the USB flash memory storage device were to fall in the wrong hands.

For those who seek to completely and securely erase data on their USB flash memory storage devices, or more commonly expressed as "wiping" the data from their devices, there is a wide range of commercial and open source products available for the task. However, how efficient these products are, if the claims about these products are valid, and how these products compare to each

other is yet to be proven. The aim of this research is to test and evaluate the efficiency and effectiveness of both open source (Freely Available Ones - FAOs) and commercial (Commercially Based Ones – CBO) products to verify which one would be a better option from a consumer's point of view. It should also be noted that the research is aimed at targeting tools and products that claim to work on USB flash memory storage devices and ascertaining whether spending money on a commercial product means that the end-user has a better chance of having their data securely erased. To answer these questions, a series of experiments were conducted using a selection of ten available products, five Commercially Based Ones (CBOs) and five Freely Available Ones (FAOs) (refer to table below).

List of Commercially Based Ones (CBOs) Under Analysis

No.	Product Name	Product Version No	No. of Erasure Schemes
1	Remo Drive Wipe	33640-4	9
2	CyberScrub Security Media Wipe	1.0	1
3	Active@Eraser	4.1	6
4	O&O SafeErase	6.0.460	6
5	East-Tec Eraser 2013	2013-10.2	13

Table 1: Illustrates the CBO's that were used for analysis.

List of Freely Available Ones (FAOs) Under Analysis

No.	Product Name	Product Version No	No. of Erasure Schemes
1	Disk Wipe	1.7	7
2	Eraser	6.0.10	13
3	Hard Wipe	3.1.0	6
4	CCleaner	4.06.4324	4
5	Hard Drive Eraser	2.0	4

Table 2: Illustrates the list of FAOs under examination.

SIGNIFICANCE OF STUDY

In a study conducted by the Ponemon Institute (2012) it was revealed that more than half of employees reported copying sensitive information to a removable USB flash memory storage device, even though 87% of those companies had policies prohibiting this practice. The same aforementioned employees confessed that to get rid of the existing data on the USB flash memory storage device they would just select the "DELETE" button to delete either the current data or previously recorded data (36%). The remaining 8% believed that when using the "FORMAT" function on the removable USB flash memory storage device, all the data on the device would have been deleted hence no traces would be left (ENISA, 2009). This factor underlines that employee knowledge on secure data erasure is very limited, if not non-existent.

Another study carried out by SanDisk (2010), revealed that employees are trained on policies revolving around data erasure and the use of USB flash memory storage devices: either once per year (33%); more than once per year (24 %); only once when they join the company (22 %); on demand (17 %); and never (3 %). It is therefore crucial to underscore that education and the awareness of the risks of not securely and permanently wiping your data while using USB flash memory storage devices could have a powerful effect on employee behaviour, and also lead to catastrophic outcomes which could be devastating for individuals, corporations and governments.

AMONG RECENT INCIDENTS

The number of recent incidents are on the rise as cited below including non-proper disposal of data erasure and USB flash memory storage devices becoming lost, misplaced, borrowed without permission or stolen

- In a more devastating and tragic event, the Mail Online News (2013) headlines read as follows: The memory stick killing: when police lost a data card with more than 1,000 informants names. An unarmed man shot dead by a police marksman as he sat in a car was wrongly suspected only weeks before of stealing a computer memory stick containing the names of 1,075 police informants. The missing stick was stolen after a detective had taken it home. It held a mass of highly confidential data about police inquiries into drug trafficking, plus hundreds of real names and addresses of secret contacts who gave information about gangsters to police.
- A Human Resources and Skills Development Canadian employee reported a lost USB key which contained personal data of thousands of Canadians. This included the social security number of approximately 5,000 Canadians. Many Canadians, who had their data stored on this USB key, were alerted to review their financial information. However, there has been no evidence to suggest that any fraudulent activity has taken place since the USB key was lost. (Prince George Citizen, 2013).
- A thumb drive was stolen from a Nurse's car in Denver on October 18, which had information such as names, birth dates, phone numbers and personal health information on hundreds of students (Greenberg, 2013).
- In an article reported by The Globe and Mail (2012), it stated that the personal information of as many as 2.4 million voters has vanished from an Elections Ontario warehouse. Elections Ontario warns voters of privacy breach as USBs holding personal data. Two USB flash keys that contained names, addresses, genders, birth dates and whether a person voted in the last election for residents.
- According to the Washington Post (2010), defence official discloses cyber-attack “Now it is official: The most significant breach of U.S. military computers was caused by a flash drive inserted into a U.S. military laptop on a post in the Middle East in 2008”. In an article published discussing the Pentagon's cyber strategy, Deputy Defence Secretary William J. Lynn III says malicious code placed on the drive by a foreign intelligence agency uploaded itself onto a network run by the U.S. military's Central Command.
- A report on the CBC NEWS in Canada (2010) reported that the University Health Network (UHN) sent letters to 763 patients who had undergone surgery at one of the three of its sites informingthem that their medical information has been compromised (CBC News, 2010).
- More recently, a USB stick containing more than 2000 pages of highly sensitive and confidential information intended to be seen only by senior officers ended up being found by a civilian. The USB was found on the pavement near a police station containing detailed strategies for acid and petrol bomb attacks, blast control training and the use of batons and shields together with a comprehensive list of officers' names, ranks and their divisions (Raywood, 2010).

With the occurrence of such incidents jeopardising individuals, organisations and governments no one is spared, hence there is a need for securely, efficiently and permanently erasing data from removable USB flash memory storage devices in order to prevent future data loss or leakage.

RESEARCH AND METHODOLOGY

To support a reasonable and scientific approach to the research, ten USB flash memory storage devices were acquired each of the same brand, model and size. The USB flash memory storage devices were then put through the process of sanitisation, such that the removable USB flash drives were cleared and wiped clean using the WinHex software prior to the start of the research. Clearing (or wiping) is the secure removal of all data from a media.

Media are cleared to shred private and confidential data, e.g. because they are to be passed to other users. After clearing, the data cannot be recovered using any common software (including WinHex itself), conceivably only by highly sophisticated laboratory techniques. Clearing can also be used to prepare a forensically sound mirror drive before cloning, to ensure that no data is left from a previous examination.

According to the US Department of Defense (2007), the standard DSS Clearing and Sanitization matrix outlined in the DoD 5220.22-M operating manual, method “h”, a removable USB flash memory storage device can be cleared by performing a full chip erase as per manufacturer’s data sheets and then overwriting (once) all addressable locations with a single character over a total of three times. This is usually the hexadecimal value 0x00, but can be any other value.

However to sanitize the removable USB flash memory storage devices according to method “h”, overwrite all addressable locations with a character, its complement, then a random character, and verify. (This method is not approved by the DoD for sanitizing media that contain top secret information.)

A research methodology normally simulates a model by considering all the technical details needed and how the proposed research will be carried out including the various stages. Gupta (2003) mentioned that research methodology can be categorised as qualitative, quantitative or a mixture of both. As mentioned earlier, this proposed research is targeted at establishing and legitimising a set of processes and guidelines in securely and efficiently erase evidentiary data from removable USB flash memory storage drives.

Moreover, Cohen, Manion & Morrison (2005) agreed that a fundamental aspect of any research, which combines a mix of pre-experiments and true experiments for the proposed study, should be based on a quasi-experimental approach.

This method suits the proposed research because the sample, i.e. the ten data erasure tools selected for the experiment, is to be procured from various vendors, five commercial ones and the remaining ones freely available from their respective websites. The data erasure products will be split into two main categories namely Commercially Based Ones (CBOs) and Freely Available Ones (FAOs) where they will then be subjected to the same rigorous testing procedures (refer to Methodology Flowcharts below).

The methodology used for this series of experiments was divided into three sections. These were the Preparation Phase, Erasure Phase and finally the Recovery Phase respectively. These different phases are explained in further details and a methodology flowchart of each phase is depicted below (see Methodology Flowcharts below).

METHODOLOGY FLOWCHARTS

Preparation Phase

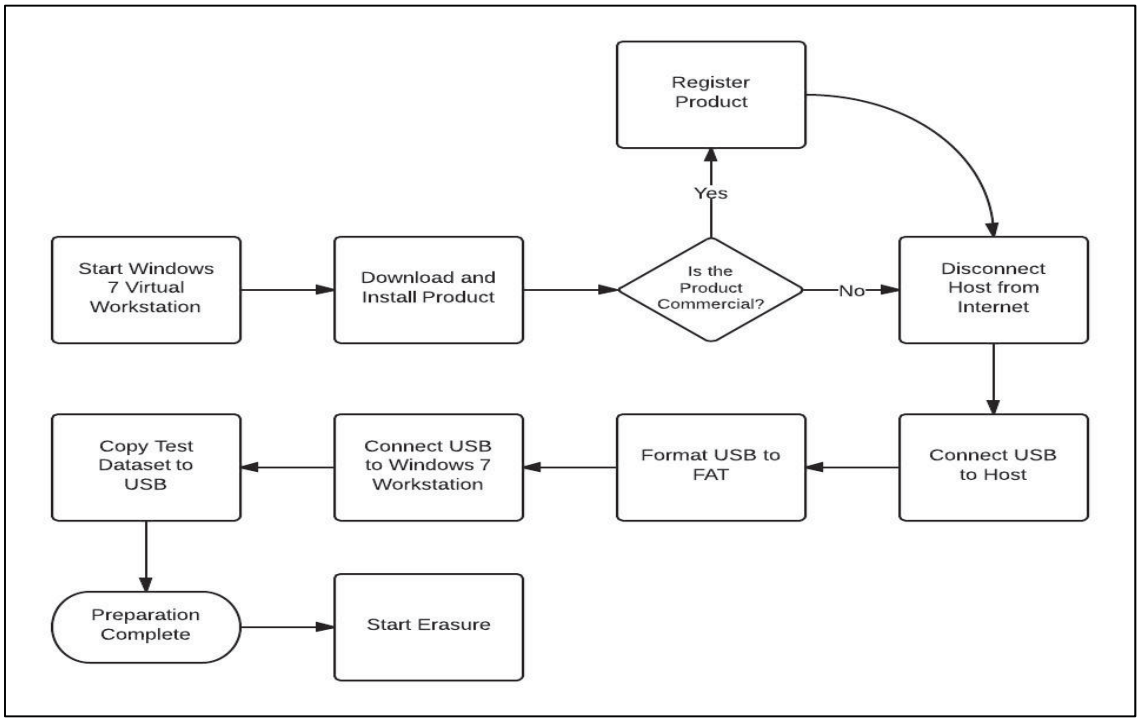

Figure 1. Illustrates the preparation phase of selecting either CBO or FAO and loading the "test dataset" prior to the Erasing phase.

Erasing Phase

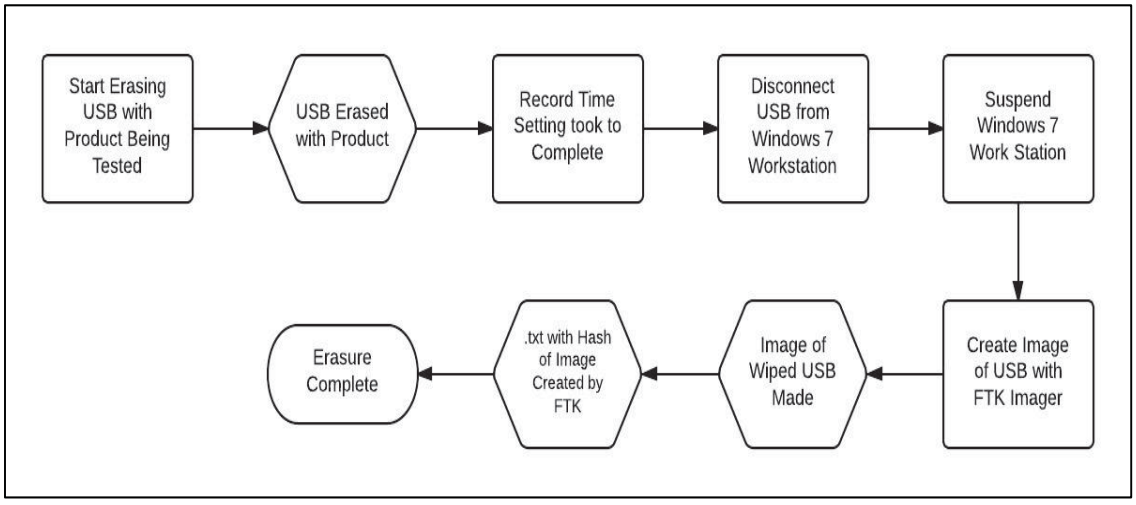

Figure 2. Explains the erasing cycle whilst recording the time for completion and preparing the removable USB flash memory storage device for the final recovery phase.

Recovery Phase

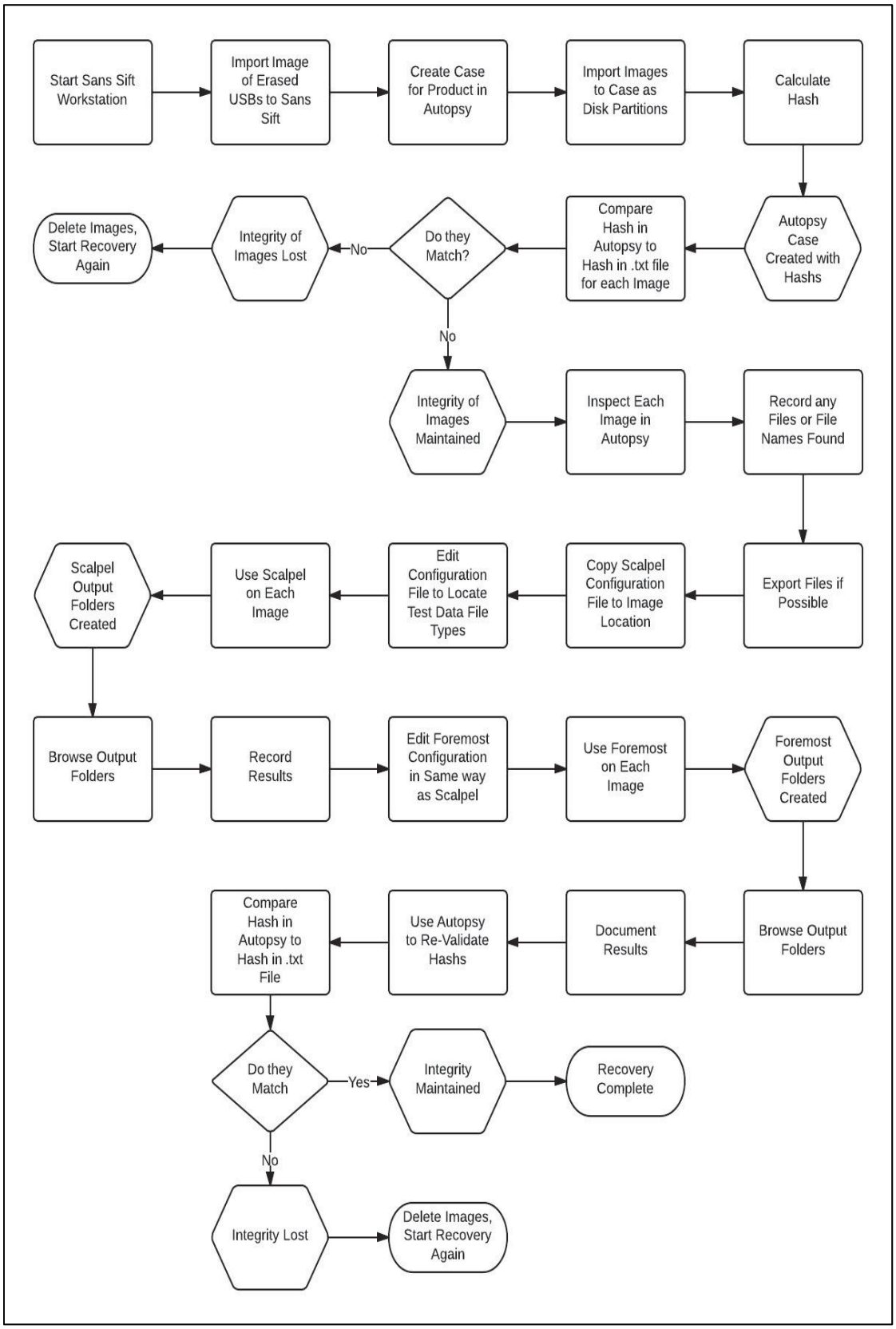

Figure 3.Depicts the final recovery phase from the image created in erasing phase.

The research methodology leveraged the tools and techniques used in a previous similar study undertaken on hard disk drives (HDDs) (Valli & Patak, 2005). As a result, the imaging of each removable USB flash memory storage device was undertaken by using the freely available software AccessData Forensic Toolkit Imager 3.1.3 (FTK Imager, 2013). Recovery and analysis was subsequently processed with WinHex 17.2 - File Recovery by Type function (Reischmann, 2013), analysis tool Autopsy 3.0.8 (Carrier, 2013), Scalpel and Foremost.

The research aimed to uncover whether either the Commercially Based Ones (CBOs) or the Freely Available Ones (FAOs) were actually securely, efficiently and permanently wiping the data from the removable USB flash memory storage devices. Secondly, should data be present the research aimed to evaluate to what extent was the information recovered useful. Various online and print media publicity has been given to individuals and organisations (Lee, 2011; Moscaritolo, 2010) that the disposal of storage media in an insecure manner can result in leaked private and confidential data. Despite these warnings, it was assumed that end-users would continue to be negligent in securely, effectively and permanently wiping their removable USB flash memory storage devices prior to discarding them.

TESTING PLATFORM SPECIFICATIONS

- **Host Machine**: 2.8 GHz Dual Core, 4 GB RAM.
- **Forensic Tool Kit (FTK) Imager Version 3.1.3** - Free software for creating images of the removable USB flash memory storage devices after erasure.
- **Windows 7 Professional, 32 bit workstation image -** For installing and running the data erasure products whilst allowing the tools to be used in a clean environment, free of any potential threats to the execution of the products.
- **SANS SIFT workstation image Version 2.14b -** pre-loaded with the tools necessary for the data recovery of the test dataset loaded on the removable USB flash memory storage device prior to the Erasing Phase.
- **VM Ware Player Version 5.02 -** running virtual workstations on the host system. The player has been set to allow the workstations access to one processor core and 1GB RAM, this ensures that every program has access to the same resources, so time efficiency can be measured accurately.

LIMITATIONS

Due to time constraints, there were a few limitations as explained below:

1) A new removable USB flash memory storage device could not be used for every pass of all data erasure products under investigation. To balance off the wear and tear on the USB flash memory storage device, one USB flash memory storage device was used for one particular data erasure product hence a total of ten removable USB flash memory storage devices were procured for this series of experiments.

2) A Virtual Workstation of Windows 7 Professional was used in the experiment due to the fact that both the CBO's and the FAO's were Windows based platforms and also to ensure that the testing environment was clean and sanitized i.e. nothing that was already present on the workstation or the host machine would interfere with the experiments.

3) When a data erasure program claimed to have completely erased all files on the removable USB flash memory storage device, this accounts for a Total Erasure (TE). If fragments or remnants of data were recovered at the Recovery Phase, this claim would be classified as 'UNTRUE' regardless of whether the fragments are useable or not.

TEST DATA SET USED

For the purpose of this research, a known data set was used so that it would ease the recovery process and also allow the researchers to flag and classify the data erasure product as soon as a partial or full recovery of any of the known data set was recovered.

The known data set comprises of common file types as illustrated in the table below.

File No.	File Name	File Extension	File Size (KB)
1	avi	.avi	826
2	Blackbuck	.bmp	769
3	Bng_strip	.png	18
4	Create	.sql	1
5	gif	.gif	1025
6	ipeg	.ipg	5381
7	jpg	.jpg	77
8	Mp4	.mp4	500
9	New Microsoft Excel Worksheet	.xlsx	10
10	New Text Document	.txt	1
11	Presentation 1	.ppt	232
12	refguide	.pdf	864
13	Robin_Thicke_Feat._T.I._and_Pharrell_Blurred_Lines_(Itunes)_[32]	.mp3	1314
14	Type the company name	.docx	23
15	xls	.xls	24
16	Zipped	.zip	10196

Table3: Set of Known Data Set

RESULTS AND COMPARISONS

The efficiency of any data erasure product under investigation in this research has been conducted and based on two aspects:

1) Time Efficiency (TE) – which is the period or length of time the data erasure product took to erase a removable USB flash memory storage device with its particular method.

2) Total Erasure Efficiency (TEE) – to which extent all the various data erasure product modes (i.e. the number of passes e.g. 1,3,5,7,9,13) erased all the contents of the known data set from the removable USB flash memory storage device.

Therefore if one of the data erasure products has two possible modes/passes, if one of the modes deletes all the data and nothing is recovered from the image, but the second mode fails to properly delete the known data set and fragment or full data can be recovered then the TEE will result in a 50% efficacy.

The Time Efficiency (TE) and Total Erasure Efficiency (TEE) of the data erasure product are then compared against either the CBOs or the FAOs. The following table illustrates the comparison between the CBOs and the FAOs in terms of their Total Erasure Efficiency (TEE). This is a measure to test whether the data erasure products was successful in deleting the set of known data. The same

set of known data was written to the removable USB flash memory storage devices prior to investigating the efficiency of the forensic data erasure tools.

Products	Number of Schemes	Schemes with total erasure	TEE	Rank
Hard Drive Eraser 2.0	4	4/4	100%	1
Disk Wipe	7	7/7	100%	1
CCleaner	4	4/4	100%	1
East-Tec Eraser	13	13/13	100%	1
Eraser	13	8/13	61%	2
O&O SafeErase 6	6	2/6	33%	3
HardWipe	6	1/6	16%	4
Remo Drive Wipe	9	1/9	11%	5
CyberScrub	1	0/1	0%	6
Active@ Eraser	6	0/6	0%	6

Table 4 depicts the Total Erasure Efficiency (TEE) – i.e. capacity to fully delete the known dataset from the removable USB flash memory storage device.

Table 5 below shows the data erasure products efficiency to execute and accomplish common erasure schemes. The most time efficient product is the one that executes the scheme the quickest.

Scheme	Disk Wipe	Eraser	HDE	CCleaner	Hard Wipe	O&O	Remo Wipe	Cyber Scrub	East Tec	Active@ Eraser
Zero Write	0:21	0:03	1:04	0:01	0:01	0:02	0:04	N/A	0:01	0:09
Random Data	0:21	0:04	N/A	N/A	0:01	0:03	0:04	N/A	0:01	0:11
DoD 3	0:12	0:08	1:21	0:02	0:02	0:05	0:15	0:03	0:02	0:12
DoD 7	0:34	0:16	N/A	0:07	N/A	0:10	0:05	N/A	0:10	N/A
Gutmann	2:24	1:12	2:12	1:45	0:40	0:55	0:50	N/A	1:00	0:15

Table 5 shows the time taken to perform a common data erasure mode.

DATA ERASURE TOOLS ANALYSIS RESULTS

To best explain these results, a picture is worth a thousand words hence graphs have been used to represent the findings of the various experiments. The first set of data represented in the graph below is showing the various data erasure products from the CBOs group and how they compare to each other.

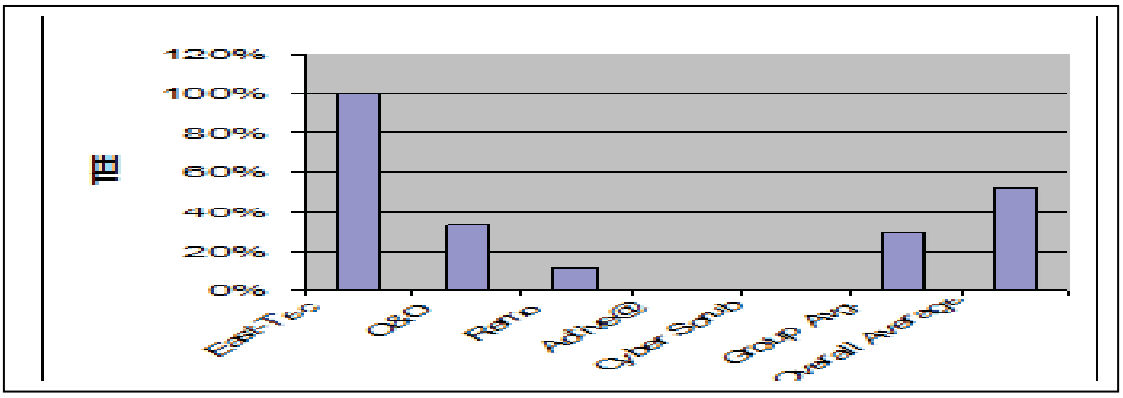

Figure 4: Commercially Based Ones (CBOs) Products Erasure Comparison table to illustrate the TEE.

In figure 4 above, the graph shows that out of the five CBOs under analysis, there were two data erasure products that had a zero percent in TEE, namely Active@ Eraser and Cyber Scrub Media Wiper which means, that these two data erasure products were classified as "UNTRUE". Therefore the two aforementioned data erasure products did not perform according to what they claimed. In other words fragments and partial datasets were recovered even after going through the wiping process. On the other hand the most effective CBOs proved to be East-Tec Eraser 2013 which registered a 100 % in TEE.

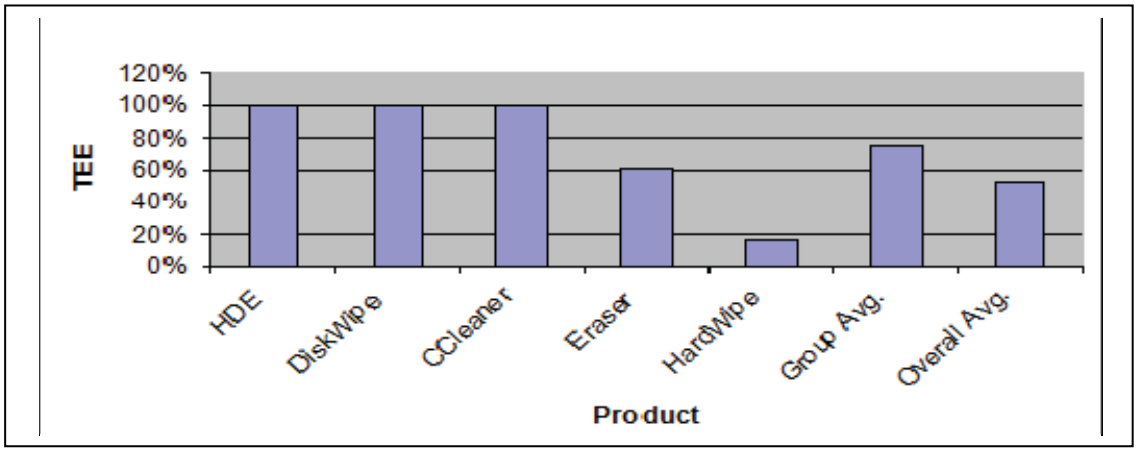

Figure 5 represent the FAOs - Products Erasure Comparison to illustrate the TEE.

In the FAOs category, three out of the five data erasure products hit the 100% TEE. One very interesting observation was that none of the FAOs hit the zero percent mark in comparison to the CBOs. This now leads us to believe that the FAOs are more likely to perform a better job at securely, efficiently and permanently wiping remnant data making it less worthwhile investing in one of the CBOs.

The following two graphs show a comparison of how quickly both the CBOs and the FAOs were at executing the five most common erasure passes. A very important aspect while interpreting these findings are that the smaller the bar is the better the product, based upon timely efficiency and as to how quickly the data erasure product completed the test. If there are no bars associated with the product this indicates that the data erasure product did not support that particular erasure pass.

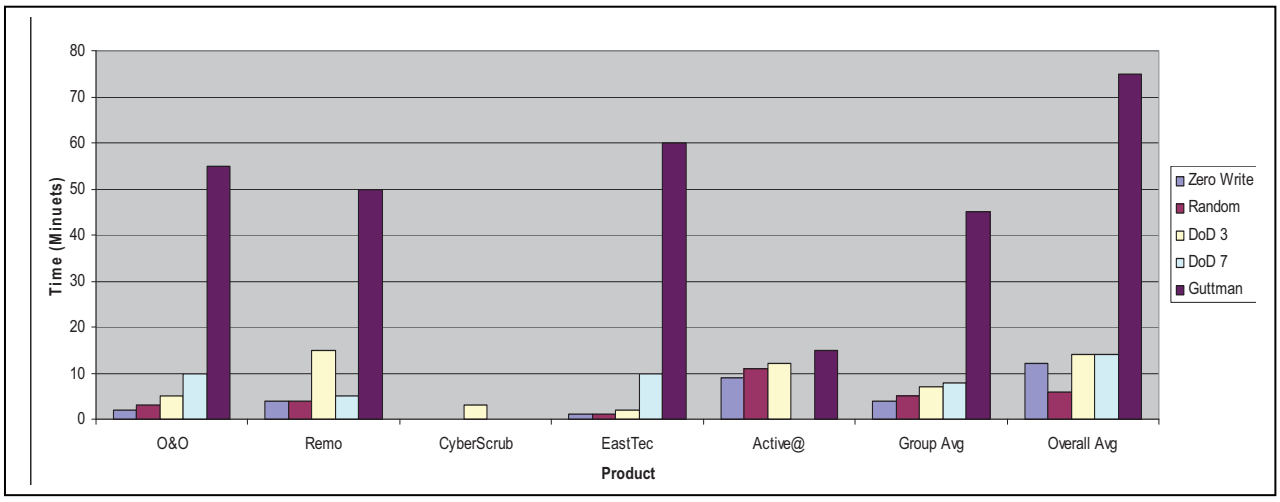

Figure 6 emphasized on the CBOs time comparison in respect to the most common modes of erasure.

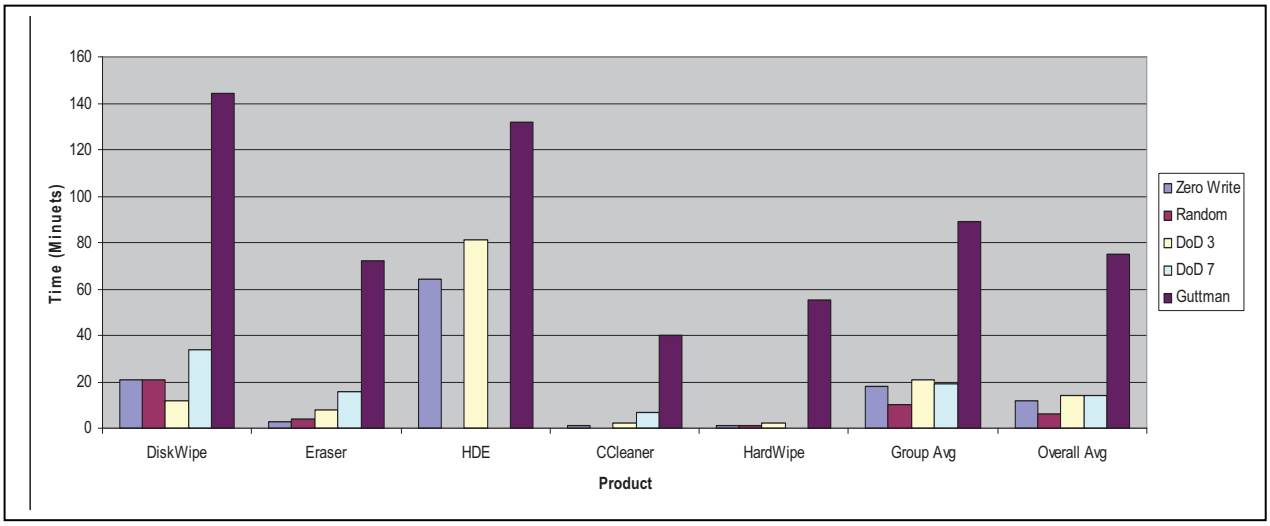

Figure 7 represent the time comparison of the most common modes of erasure among the FAOs.

RECOMMENDATIONS

Based on the various experiments conducted during this research, it revealed that after comparing and analysing all the findings that some of the CBOs category performed better in a timelier, efficient manner compared on average to the FAOs. However, the FAOs category revealed that the products did securely, efficiently and permanently erase remnant data from removable USB flash memory storage device. In light of these findings, it is difficult to recommend one single product based on both the products erasure efficacy and its time efficiency. If an end-user opted to purchase a CBO data erasure product East-Tec Eraser 2013 would be the recommended product, however if time is not of the essence then choose one among the FAO category. The study agreed that since these products all had different level of passes for securely, efficiently and permanently erasing data the use of any of these three FAOs, in order of priority, would be suitable: CCleaner, DiskWipe and Hard Drive Eraser.

FUTURE RESEARCH

Given that this research has helped to shed some light on the myths of whether the CBOs are better than the FAOs, it is clear that based on the outcomes and findings that the FAOs category in this particular research – i.e. based on the products and tools used prevails as the better product. This research also has the potential to help the various vendors, especially those in the CBOs category, to re-evaluate their data erasure products in regards to the removable USB flash memory storage devices and hence address their weaknesses. Future experiments would encompass testing the data erasure products on other media such as SD Cards or Solid State Drives SSDs to observe how effective the tools would be. Also a longitudinal study conducted over a period of time could be utilised to test different versions of the same product to see improvements had been made.

CONCLUSION

This paper tested ten data erasure products of which five were Commercially Based Ones (CBOs) and five were Freely Available Ones (FAOs). This research has indicated that there are a range of factors and issues that can affect the ability of removable USB flash memory storage devices to be erased forensically. Indications from this initial study are that USB flash memory storage devices size and capacity can definitely effect erasure times significantly.

This paper has presented the rigorous method developed to test the features of various data erasing products, as well as the results from the experiments. The number of failings was unexpectedly high. These products give the impression that with multiple overwrites they will remove the data to avoid recovery from all but the most sophisticated forensic techniques. However, it was found that in some cases, data remains in plain view and is easily recoverable. These findings provide some credence to the argument that not all data erasure products are created equal.

REFERENCES

Carrier, B. (2013).The Sleuth Kit. Retrieved August 20, 2013, from http://www.sleuthkit.org/autopsy/download.php

Choo, R. K., Smith, R., McCusker, R. (2007-2009). Future directions in technology-enabled crime.Australian Institute of Criminology. Retrieved August 11, 2013 from http://www.aic.gov.au/documents/9/3/6/%7B936C8901-37B3-4175-B3EE-97EF27103D69%7Drpp78.pdf

Cohen, L., Manion, L. & Morrison, K. (2005). Chapter 12: Experiments, Quasi-Experiments and Single Case Research. In *Research Methods in Education* (5thed, pp. 211-225) New York, NY: RoutledgeFalmer.

US Department of Defense.(2007). DSS Clearing and Sanitization Matrix.Retrieved September 10, 2013 from http://www.oregon.gov/DAS/OP/docs/DSS%20Clearing%20and%20Sanitization%20Matrix.pdf

FTK Imager.(2013). Forensic Toolkit Imager.Retrieved March 31, 2013, from http://accessdata.com/support/adownloads#FTKImager.

Goodin, D. (2011). Self-erasing flash drives destroy court evidence. Retrieved September 10, 2013 from http://www.theregister.co.uk/2011/03/01/self_destructing_flash_drives/

Greenberg, A. (2013). Student Data from Denver elementary schools at risk after thumb drive stolen. Retrieved October 20, 2013 from http://www.scmagazine.com/student-data-from-denver-elementary-schools-at-risk-after-thumb-drive-stolen/article/316885/

Jones, A., Valli, C., & Dabibi, G. (2009). The 2009 Analysis of Information Remaining on USB Storage

Devices Offered for Sale on the Second Hand Market. Paper presented at the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth, Western Australia.

Kingston (2012). Flash Memory Guide: Portable flash memory for computers, digital cameras, mobile phones and other devices. Retrieved March 24, 2013 from http://media.kingston.com/pdfs/FlashMemGuide.pdf

Lee, K. (2011). The Dangers of Second Hand Hard Drives. Retrieved September 19, 2013, from

https://www.infosecisland.com/blogview/16105-The-Dangers-of-Second-Hand-Hard-Drives.html

Moscaritolo, M. (2010).Security risk to office equipment disposal. Retrieved October 20, 2013, from

http://www.adelaidenow.com.au/business/security-risk-to-office-equipment-disposal/story-e6fredj3-1225877502647

Ponemon Institute (2012). 2011 Cost of Data Breach Study: United States. Retrieved September 9, 2013 from http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf

Prince George Citizen. (2013). Fed's Loss of USB key containing personal info to be probed. Retrieved October 28, 2013 from http://search.proquest.com.ezproxy.ecu.edu.au/docview/1266686408

Reischmann, S. (2013).X-Ways Software Technology. Retrieved May 23, 2013, from

http://www.winhex.com/winhex/

Sacks, K. (2011) "Patient Data Posted Online in Major Breach of Privacy." Retrieved October 12, 2013 from http://www.nytimes.com/2011/09/09/us/09breach.html

SanDisk (2010). Unsecured USB Flash Drives; Usage is More than Double Corporate IT Expectations. Retrieved May 30, 2013, from http://www.sandisk.com/about-sandisk/press-room/press-releases/2008/2008-04-09-sandisk-survey-shows-organizations-at-risk-from-unsecured-usb-flash-drivesusage-is-more-than-double-corporate-it-expectations.

Sudan, K., Badam, A & Nellans, D. (2012). NAND-Flash: Fast Storage or Slow Memory? Non-Volatile Memory Workshop (NVMW-2012) , San Diego, March, 2012