INVESTIGATION AND ANALYSIS OF INFORMATION REMAINING ON USED HARD DISK DRIVES IN THAILAND

BY

MANASAWEE FUNGE-SMITH

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR
THE DEGREE OF MASTER OF SCIENCE IN COMPUTER AND INFORMATION MANAGEMENT
COLLEGE OF DIGITAL INNOVATION AND INFORMATION TECHNOLOGY

GRADUATE SCHOOL, RANGSIT UNIVERSITY
ACADEMIC YEAR 2023

Thesis entitled

INVESTIGATION AND ANALYSIS OF INFORMATION REMAINING ON USED HARD DISK DRIVES IN THAILAND

by

MANASAWEE FUNGE-SMITH

was submitted in partial fulfillment of the requirements

for the degree of Master of Science in Computer and Information Management

Rangsit University

Academic Year 2023

---	---
Assoc.Prof.Panjai Tantatsanawong, Ph.D.	Asst.Prof.Suthisak Chantawongso, Ph.D.
Examination Committee Chairperson	Member

	Asst.Prof.Chutima Beokhaimook, Ph.D.
	Member and Advisor

Approved by Graduate School

(Asst.Prof.Plt.Off. Vannee Sooksatra, D.Eng.)

Dean of Graduate School

September 30, 2023

Acknowledgements

The researcher wishes to extend heartfelt appreciation to the following:

The lecturers at Rangsit University for their invaluable assistance in enabling me to complete my Master's degree successfully.

Friends and family members for their unwavering support throughout this course.

Manasawee Funge-smith

Researcher

6404623 : Manasawee Funge-Smith

Thesis Title : Investigation and Analysis of Information Remaining on Used Hard Disk Drives in Thailand

Program : Master of Science in Computer and Information Management

Thesis Advisor : Asst. Prof. Chutima Beokhaimook, Ph.D.

Abstract

People rely on storing and processing their data and information on hard disks in this technological age. This research investigated whether the hard disks sold in the second-hand market had been completely erased or not and whether the disks contained readable data. The research further analyzed if data retrieved were remaining information belonging to previous owners. The disks that contained remaining information were identified. The results of the study were compared with the results from studies conducted abroad in order to explore any shared trends or differences. It was revealed that Thailand's results were in line with other countries from earlier studies. The findings presented that the majority of used HDD in Thailand still contained remaining information data that was not properly sanitized by previous owners, and some of the data belonged to international entities. The research concluded that it was very important to have greater awareness of the risks of incomplete data erasure on second-hand disks.

(Total 27 pages)

Keywords: Disk Analysis, Computer Forensics, Data Disposal, Data Privacy, Data Recovery, Data Sanitization.

Student's Signature……..…..……. Thesis Advisor's Signature…….……...……..

Table of Contents

Table of Contents (continued)

List of Tables

Page

Tables

List of Figures

Page

Figures

Chapter 1

Introduction

1.1 Introduction

People and organizations rely on storing and processing their data and information in this technological age. There are several ways to store data today, including localized physical storage such as hard disk drives, USB keys, and remote storage such as cloud servers. Each method has its strengths and weaknesses. Cloud storage does not risk loss or failure of the equipment, but requires access to a Wi-Fi internet connection making it more vulnerable to cyber-attacks. This may also have issues with connection failures during data uploads, and typically requires payment for access. Physical storage such as hard disk drives can now store terabytes of information locally, on individual computers, or within business networks or servers allowing remote access. The convenience of hard disks to store digital content, whether to store public or private information, remains both relevant and necessary in today's digital society.

The storage of data on hard drives does come with a risk that organizations and private individuals need to be aware of. Discarded hard disks that haven't been thoroughly formatted or cleaned may still harbor confidential and sensitive information. This is sometimes referred to as 'Remaining information'. If such information becomes available to an unintended third party, there are potential adverse outcomes including the humiliation of individuals and organizations and vulnerability to fraud, blackmail, and identity theft.

This potential risk has been identified by researchers and there have been several studies and analyses on the information safety of hard disks offered for sale in

the second-hand market worldwide (Jones, Valli, Dardick & Sutherland, 2009). However, this type of study has not been conducted in Thailand to date.

The results of international studies (Jones et al., 2009) indicated that there was sufficient information to conclude that many of the hard disks examined were compromised. They contained remaining information that could harm and embarrass the previous owners, making them susceptible to fraud, blackmail, and identity theft. Moreover, it highlighted the need for organizations to effectively deal with their discarded hard disks according to the statutory, regular, and legal obligations for privacy as also recommended in the ITU 2012 guidelines, and the confidentiality of information they recorded (e.g. customer information, trade-related information, and intellectual property).

1.2 Research Objective

This research investigates the situation of hard disk drives available in the second-hand market in Thailand and whether or not the data and information left on disks offered for sale had been completely erased. The research further analyzes whether the disks contain retrievable remaining information that could be identified as belonging to the previous owners. Finally, this paper compares the data obtained from this research in Thailand with the data gathered from abroad to see whether there are any shared trends or differences. The objectives of this research were as follows:

1.2.1 To assess whether used hard disk drives offered for sale on a second-hand market had been effectively formatted and did not contain retrievable data.

1.2.2 To analyze file types left on the hard disk drives to identify whether retrievable might be of the types that contain remaining information.

1.2.3 To compare the results obtained from this investigation with similar research conducted abroad in the United Kingdom, Australia, the United States, France, and Germany.

The structure of this paper is organized as follows. A review of relevant topics and previous research relevant to the conduct of this investigation is presented

in Chapter 2. In Chapter 3, the methodology of our investigation is introduced. Chapter 4 describes the results. Later, in Chapter 5, we draw conclusions from our work and also provide several suggestions and recommendations for further action.

1.3 Research Framework

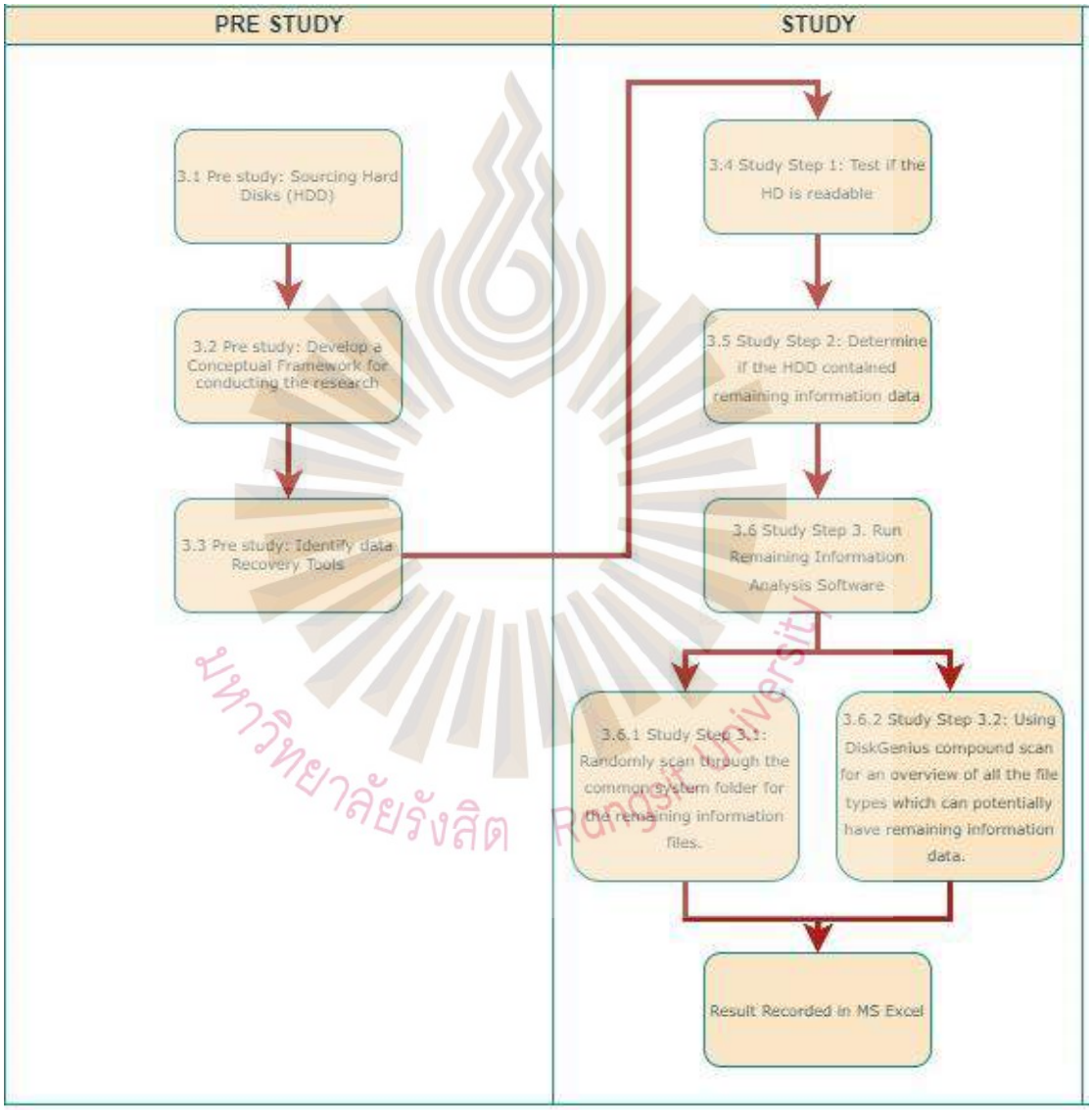

Figure 1.1 The Steps of the pre-study and study

Chapter 2

Literature Review

This section reviews relevant topics and research essential to conduct this investigation. The papers reviewed below were relevant to the study due to their focus and analysis on data sanitization and leakage from hard disk drives. The majority of the studies principally focused on hard disk drives that were sold second-hand.

2.1 Guides for Media Sanitization - National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) published the Guidelines for Media Sanitization (Kissel, Regenscheid, Scholl & Stine, 2014) as a general guide to data sanitization of any form of media (documents, images, hard drives etc.) that could be used universally. Sanitization, in this regard, refers to "a process that renders access to target data on media infeasible for a given level of effort" (Kissel et al., 2014). The guideline highlighted the importance of complex access controls and encryption to prevent third parties from retrieving information from discarded media. Protecting information should be of utmost ethical significance. The guideline summarized and categorized three sanitization methods: precision sanitization, purging of data, and destruction of the disk. As it is not possible to analyze a hard disk that has been physically destroyed, this research only focused on two methods: clear and purge. The straightforward ‘clearing’ method for hard disk drive sanitization uses software or hardware to overwrite target data with non-sensitive data using standard read-and-write commands. These include overwriting the location of a file and storage. The ‘purge’ method focuses on overwriting, blocking, erasing, and cryptographically erasing information through specific devices and techniques that are more advanced than standard read-and-write commands. According to the

guidelines, this method renders it almost impossible to recover leftover data, even in a state-of-the-art data recovery laboratory.

2.2 Tutorial on Disk Drive Sanitization (Hughes & Coughlin, 2006)

The summary of the Tutorial on Disk Drive Sanitization (Hughes & Coughlin, 2006) also provided comparisons of four primary methods of data erasure on hard disk drives. The four primary methods are as follows:

2.2.1 Weak Erase: the act of deleting files, considered a 'weak' level of data security and sanitization, the primary source of data leakage.

2.2.2 Block Erase: the act of overwriting files with external software, considered as having a 'medium' level of data security and sanitization.

2.2.3 Normal Secure Erase: using in-drive overwriting is considered a 'high' level of data security and sanitization.

2.2.4 Enhanced Secure Erase: using in-drive overwriting with the encryption key, considered as having a 'very high level of data security and sanitization.

The research considered that the second-hand hard drive disks that would be read and analyzed might be categorized into different primary data erasure methods. Investigation may indicate a correlation between leftover data information with the method used to erase data.

2.3 International Research

Perhaps the pioneering study for this investigation was in 2008, where a study (Jones et al., 2010) examined many hard disk drives purchased blindly and then forensically analyzed to determine whether they contained any sensitive information from the previous owners and whether the disks were effectively erased. The hard disk drives were purchased from a number of different countries (i.e., USA, Germany, France, and Australia). For consistency, the experiment was done under the same conditions, equipment, and tools (Windows Unformat, Undelete, Autopsy and Sleuthkid). Each disk was forensically imaged with software under two specific

requirements. First, preserving the original media and securely storing each hard disk drive was necessary. This was in case the hard disk drive needed to be handed to the authorities if it contained evidence of criminal activity. Second, there was a need to research in a non-intrusive method that would not alter any original data in case any anomalies were detected. The authors blindly bought 336 hard disk drives and the results were as follows in Table 2.1.

Table 2.1 The Results of the 2008 Studies

Country	Number of hard disk drives examined	Number readable	Percentage readable
United Kingdom	160 hard disk drives	60	37.5%
USA	63 hard disk drives	53	84.4%
Germany	28 hard disk drives	8	28.6%
France	44 hard disk drive	13	29.5%
Australia	43 hard disk drive	25	58.1%

Source: Hughes, 2008

It was found that sensitive data was left on the hard disk drives from private individuals. The study concluded that staff members within the organizations were required to be more aware of how to discard computer hard disks safely.

In 2010, (Jones et al., 2010) continued their study of information remaining on disks offered for sale on the second-hand market. The results showed that over a four-year period, there had been a small but steady reduction in the proportion of disks containing identifiable information. However, the storage capacity of individual hard disk drives had increased considerably. The number of disks that had been wiped did not show any consistent pattern, and the results were consistently lower than should be expected. This might be because of education and awareness of the potential risks of data leaking to the public domain, and the actions to remove or destroy this data, needed to be improved both within organizations and at the individual/home user level. The study concluded that despite the increased publicity about the issue,

organizations and individuals still needed to be fully aware of the risks of not taking suitable action to destroy or remove the data.

In a similar study in Indonesia (Lim, Firdausi, & Bresnev, 2014) blindly bought 50 hard disk drives randomly from a second-hand market and used the same premise and methodology as the previous paper by (Jones et al., 2009). They found out of 50 hard disk drive, 43 contained sensitive information, including personal images, personal user decompressed files, corporate enhanced metafiles, banking information, etc. It was concluded that individuals and organizations must follow the NIST-published guidelines on media sanitization to prevent data and information from leaking to third parties.

Hard disks offered for sale on the secondhand market in the United Arab Emirates had also been examined by (Jones, Martin, & Alzaabi, 2016). They sought to explore the types of information that remained on hard disk drives and determined whether there were any data sanitization changes compared to other previous research. They also introduced Malware scans to observe the potential risks of obtaining second-hand hard disk drives. It found that out of 40 hard disk drives, 26 contained data and information that could be traced back to the previous owner with varying sensitivity. Interestingly, 20 had enough data to be traced to a private individual, and 9 more overlapping hard disk drive contained enough data to be traced to an organization. Moreover, 17 out of the 26 had malware, further proving that obtaining a second-hand hard disk drive may not be safe for the new owner.

There has also been a study on the information left on USB Storage Disks. (Adam & Clarke, 2009). The USB storage disks that were examined showed that users were unaware of leftover data and that such information could be traced to the previous owners. Out of ten USB keys bought from an auction website, eight contained up to 4,000 files that could be recovered via forensics software, with varying types of sensitive data. It was concluded that most private individuals were unaware of the need for formatting their USB devices and that deleting files does not mean every trace of their data and information would be entirely erased. As USBs are

more suitable for private individuals for day-to-day use, they may be more likely to contain data prone to hacking, identity theft, blackmail, and fraud.

A review of internet websites, research articles and university journals for Thailand revealed a small number of papers and articles related to hard disk drives. However, these were primarily focused on hard disk drive performance and none were related to data sanitization. Therefore, it would be good to determine if there was a higher percentage of leftover data on second-hand hard disk drives compared to the results of research conducted in other countries. Regardless of the results, an objective of the study was to raise awareness that hard disk drives must be formatted appropriately before being passed down or sold into the second-hand market. Any leftover information could harm the previous owners due to the lack of this awareness.

Chapter 3

Research Methodology

3.1 Pre study: Sourcing Hard Disks (hard disk drive)

The total number of second-hand hard disk drives stocked in stores in Bangkok is unknown, as is the number of second-hand retailers of hard disk drives in Bangkok. A non-probability sampling technique was used to select the samples for this study. A sample of 32 hard disk drives were randomly purchased from 20 stores offering second-hand hard disk drives for sale. The hard disk drives were purchased from a second-hand market in Bangkok, Thailand. This market is hugely accessible and well known, including to those who may not be knowledgeable about computers. The Bangkok second-hand hard disk drive market might source from a variety of locations (e.g., repaired, or obsolete private computers, office clearances), but it was not possible to determine these sources for this study.

3.2 Pre study: Develop a Conceptual Framework for conducting the research

The flow chart presented in Figure 1 shows this the general framework of this investigation. Starting from constructing hypotheses, sourcing hard disk drives from the second-hand market in Bangkok, using tools to recover any leftover data, analyzing any leftover data, and recording the findings into the research paper. From there on, the research compared the findings of this investigation with other similar investigations from abroad, described in Section 2.3 Background Theories and Literature Review.

3.3 Pre study Identify data Recovery Tools

From the review of the previous papers, there is no common or international standard methodology or tools for the scientific recovery of data from hard disk drives. The method used for this research was as follows in Fig 1.

3.4 Study Step 1: Test if the Hard disk is readable

The hard disk drive purchased were tested using the program Hard Disk Sentinel Professional Portable version 6.01.2 (12540) (Figure 3.1).

Figure 3.1 Interface of the Hard Disk Sentinel Professional Portable version 6.01.2 (12540)

This program provided a report of the condition of the hard disk. If the disk was undetected or unreadable, the result was recorded that the disk was not working. Due to the limited time for this study, if the hard disk drive could not be detected or was inaccessible due to bad sectors, the analysis for that hard disk drive would not proceed to the second step to run a full scan using DiskGenius.

3.5 Study Step 2: Determine if the hard disk drive contained remaining information

If the hard disk drive could be accessed, it was analyzed to see if it contained any retrievable remaining information data. The hard disk drives were accessed using a laptop computer running VMware as a firewall from potential viruses. Data recovery software was used to investigate whether data and information had been left on hard disks. The software used was DiskGenius V. 5.4.5.14.12 (x64) Professional. This program has many features for partition recovery, file recovery, disk management, data backup, and disk utilities. It can help manage storage space, recover lost data due to disk corruption, formatting, deletion and virus attack and also offers reliable backup solutions to prevent data loss (Hidayat, Sudarmaji, Irawan, Susanto & Mustika, 2018). The disk recovery step used the standard settings for recovery preset by the software company. During the scanning process, the image or recovered files remain intact without interfering with the hard disk drive, to prevent overwriting to the original disk. Once the full scan was completed, the scan results were saved. A compound search was used to count how many different types of files and sizes of the files could be recovered.

3.6 Study Step 3. Run Remaining Information Analysis Software

To analyze whether any remaining information can be traced back to the hard disk drive's original owner, the study followed the following steps.

3.6.1 Study Step 3.1: Randomly scan through the common system folder for the remaining information files.

3.6.1.1 [DISK#:] C:\$Recycle.Bin

3.6.1.2 [DISK#:] C:\USER\[NAME]\Desktop

3.6.1.3 [DISK#:] C:\USER\[NAME]\Documents

3.6.1.4 [DISK#:] D:\[Root Directory]\[Sub-Directory]

3.6.2 Study Step 3.2: Using DiskGenius compound scan for an overview of all the file types which can potentially have remaining information data.

If files were found, they were considered remaining information data if they are the following files types:

3.6.2.1 Documents: These files are created by office programs and may include text documents, spreadsheets, and PowerPoint presentations. Extensions include: DOCX, XLX, PPTX, PDF, TXT

3.6.2.2 Photographs: Photo files are types of digital images that contain visual information captured by a camera or other device (such as a scanner). Photo files typically use the file extensions JPEG, PNG, or TIFF.

3.6.2.3 Music: Some common file extensions for music files include .mp3, .m4a, .wav, and .flac.

3.6.2.4 Video: Some common file extensions for video files include .mp4, .m4v, .mov, and .avi. These extensions indicate the format of the video file and determine which programs can be used to open and play the video.

3.6.2.5 Internet: .htm, .html, .url, and .swf are just a few examples of file extensions that are commonly used on the Internet.

3.6.2.6 Graphics: Digital images that have been created or edited using specialized software (e.g., Adobe Photoshop Illustrator, GIMP). Graphic files may use file extensions such as EPS, SVG, or AI

3.6.2.7 Archive files: Some common file extensions for archive files include .zip, .rar, and .7z. These file formats are used to compress and combine multiple files into a single, smaller file for easier storage.

3.6.2.8 Email archive files: These are email archives the most common extension for Windows is PST.

Other files: That is not classified from the above criteria such as .dll, .exe, and .jar for example.

Chapter 4

Results

4.1 Results for objective 1: Hard disks sold on a second-hand market are not effectively formatted and contain data and information that could be traced back to the previous owners.

The results indicate that 24 out of 32 of the hard disks analyzed were fully in working condition according to Hard Disk Sentinel Professional software.

The size of the files and folders recovered from these disks in total is, on average 43% for all across working drives.

The data analysis of the file types shows that:

1) The total disk size of all the disks was 7,471.7 GB

2) The total number of files that could be recovered was 4,680,024 files

3) Music and Archive type files had the largest disk usage with 1,410.6721 and 2,980.8056 GB, respectively.

4) Graphic-type files had the highest number of files, with 2,682,135 files.

4.2 Results for objective 2: The data and information left on the hard disks offered for sale can be retrieved, and some of this data is of files types associated with remaining information that may be sensitive and could present privacy risks to the previous owner, such as breach of privacy, embarrassment, fraud, identity theft, and blackmail.

Using the basic forensic investigation on DiskGenius software. We randomly searched and recovered the remaining information files in the preview. Most of them

were in the following directories, part of the common system folder for the Windows Operating System (OS), or backups on another partition that did not contain the OS.

1) [DISK#:] C:\$Recycle.Bin
2) [DISK#:] C:\USER\[NAME]\Desktop
3) [DISK#:] C:\USER\[NAME]\Documents
4) [DISK#:] D:\Data

The data analysis performed examined the usage of various types of files stored on a computer system. The results are present in Fig. 4.1.

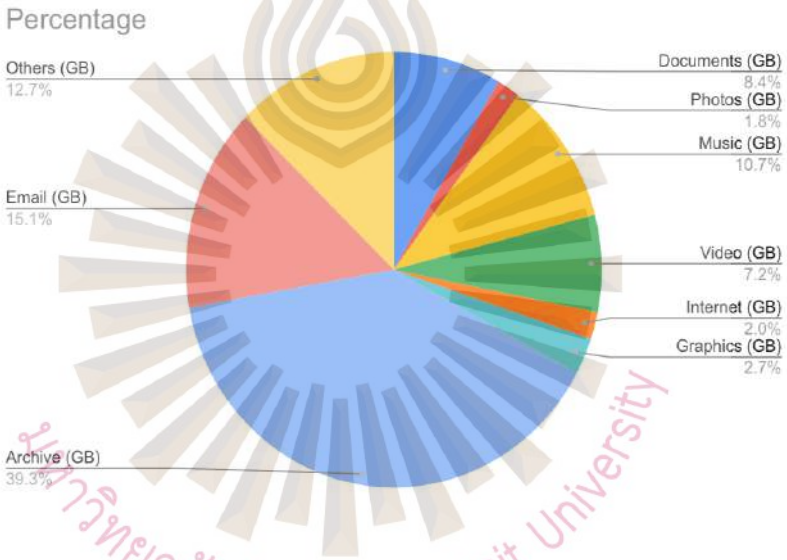

Figure 4.1 The Percentage of the Different Types of Data from the Recovered Disks

The results indicate that the most common type of file stored on the system are Archives, accounting for 39.9% of the total files. This is followed by Music at 18.9%, Video at 11.3%, Documents at 10.7%, and Graphics at 1.5%. The other types of files, including Internet, Photos, Email, and Others, account for a smaller portion of the total files stored on the system. In total, 4,680,024 files were recovered from the 32 hard disk drives analyzed. These results indicate that the users of these hard disk drives were mostly storing and using documents, music, video, and archive files. This suggests that the users were probably using the hard disk drives for work or school-

related purposes or for leisure activities such as watching videos and listening to music.

The study found that 18 out of 24 working readable drives had remaining information data. The random analysis of files also found a variety of sensitive remaining information data on the hard disk drive. Types of sensitive remaining information data that were found include:

Table 4.1 The Category of Remaining Information Files

Category	**Documents**
Email	Login and password are stored in MS Word
Job Application	Resume/CV
Housing	House contract (In the Chinese language)
Contact Information	Draft and contact details
Health	Lab Test report
Company Documents	Company's Presentation, Company's payment structure, KPI, Request for approval letter, Company's letter, Receipt template of a company, Company's report, Company's non-conformity report
Construction	Construction BOQ
Travel	Flight dispatch details, Photo of the boarding pass
Personal Documents	Photographs and scanned images, Passport, Land titles, Thai national identification, Thai house registration, Birth certificate, Degree certificate, Medical record
Financial Documents	Bank account front page, Bank transfer slips, Bank statements, Financial certificate (Very Large amount)
Academia	Thesis
Lottery	Thai underground lottery
Security	SOP Read and understand Memo, CCTV footage
Email Data	Email archives, Internet files such as web-cache and graphic content (contain personal information and, importantly, confidential or sensitive attachments)

These positive findings indicate that the disks did contain potentially sensitive data which could identify the previous owner and present privacy risks to the previous owner. Such as breach of privacy, embarrassment, fraud, identity theft, and blackmail

4.3 Results for objective 3: The lack of awareness of data security and risks of poorly formatted hard drives in Thailand suggests that the proportion of drives that contain remaining information will be higher than that found in research conducted in other countries.

Compared with the results of other international studies in Table 1, this study had a relatively small sample size with fewer hard disk drives than other international studies undertaken previously, although at the country level, the sample size in this study is comparable with some of the previous international studies. The results of this study reveal that of 32 hard disk drives analyzed, 10 were unreadable and of the remaining 22 readable hard disk drives, all had retrievable data. This suggests that up to that 100% of second-hand hard disk drives accessed in Thailand will contain some retrievable data.

Table 4.2 The Comparison Results of Related Research

Year	Subject	Location	No. of hard disk drive	No. of drives with leftover data and information detected	% of drives with leftover data and information detected
2007 Analysis (Jones et al., 2009)	hard disk drive	UK	74	46	62%
	hard disk drive	USA	31	25	81%
	hard disk drive	Germany	12	7	58%

Table 4.2 The Comparison Results of Related Research (Cont.)

Year	Subject	Location	No. of hard disk drive	No. of drives with leftover data and information detected	% of drives with leftover data and information detected
	hard disk drive	Australia	71	48	68%
USB Analysis 2009 (Adam and Clark, 2009)	USB	N/A	10	8	80%
2009 Analysis (Jones et al 2010)	hard disk drive	UK	114	82	72%
	hard disk drive	USA	61	38	62%
	hard disk drive	Germany	41	15	37%
	hard disk drive	France	9	5	56%
	hard disk drive	Australia	37	23	62%
2013 Analysis (Lim and Bresnev, 2013)	hard disk drive	Indonesia	50	43	86%
2016 Analysis (Martin et al., 2016)	hard disk drive	UAE	40	26	65%

Table 4.2 The Comparison Results of Related Research (Cont.)

Year	Subject	Location	No. of hard disk drive	No. of drives with leftover data and information detected	% of drives with leftover data and information detected
2022 Our Study	hard disk drive	Thailand	22	22	100%

This study detected a higher high percentage of hard disk drives containing leftover data than any other country so far studied with 18 out of 22 (82%) of readable hard disk drives containing files types associated with remaining information.

Chapter 5

Conclusion and Suggestions

5.1 Conclusion

The results of the Thailand study are higher than the results from other countries in the earlier international studies. The majority of hard disk drives analyzed were not low-level formatted to sanitize them. The findings also indicate that the majority of used hard disk drives in Thailand still contain files types associated with remaining information data that was not properly sanitized by the previous owners. Some of the data belongs to international entities and the language of the recoverable files suggests that some of the previous owners of the hard disk drives were international/non-Thai. Most of the remaining information data retrieved was contained in the recycle bin directory.

These results highlight the need for more stringent regulations and enforcement of data sanitization of used hard disk drives in Thailand in order to protect the privacy of individuals. It is possible that the risks detected in this 2022 Thailand study may now be increasing, as the rise in home-based teleworking during COVID-19 may see organizations implementing more liberal policies for the personal use of corporate computers or the use of home computers for work. This was previously suggested by Jones et al. (2009) to explain a trend in their results. Although information may be stored in the cloud or on secure office servers, any files downloaded to local home computers will be stored on local hard disk drive.

5.1.1 Disposal of old ICT equipment and e-waste management:

There is some international guidance on the end-of-life information and communication technology equipment, which indicates that it is the responsibility of

the organization that is selling or scrapping its equipment to ensure that data is properly removed.

In relation to data security, it is the duty of organizations under the local data protection acts which require all information collected by an organization to be destroyed when the media (in this case computer hard drives) in which it is stored comes to the end-of-life. Organizations and individuals within these organizations must ensure that all confidential data is dealt with at the time when the storage media is disposed of and non-compliance can lead to significant fines as well as the risk to damage the organization brand image. (International Telecommunication Union [ITU], 2012)

The Waste Electrical and Electronic Equipment (WEEE) Directive is a European Union directive that requires manufacturers of electronic equipment to take back their products at the end of their life and this includes hard drives. The EU WEEE Directive also requires manufacturers to provide information on how to dispose of their products safely. This information must be included in the product's user manual. (European Commission., n.d.).

The United States Electronic Product Stewardship (EPSA) Act It is a federal law that requires manufacturers of electronic products to develop and implement plans to manage the end-of-life of their products. Although the EPSA does not specifically mention hard drives, it is likely that hard drives would be considered electronic products under the act. (U.S. Environmental Protection Agency., n.d.).

The National Television and Computer Recycling Scheme NTCRS is an Australian government-backed scheme that requires manufacturers of televisions and computers to take back their products at the end of their life and this includes hard drives. The NTCRS also requires manufacturers to provide information on how to dispose of their products safely. This information must be included in the product's user manual. (Victoria Government Gazette, 2018)

While the countries mentioned above (the European Union, the United States, and Australia) have specific regulations and initiatives in place to manage electronic waste and end-of-life electronic equipment, it is evident that the level of effectiveness can vary. This difference could be attributed to the level of public awareness, enforcement mechanisms, and cultural attitudes towards recycling.

In the case of Thailand, it may be inferred that the significantly higher percentage of hard drives containing remaining data could be due to several factors. Unlike the aforementioned regions, Thailand may not have as stringent or as broadly enforced regulations for electronic waste management.

Thailand does have regulations for electronic waste management, but they are not as stringent or as broadly enforced as in some other countries. The main regulation governing electronic waste management in Thailand is the Enhancement and Conservation of National Environmental Quality Act B.E. 2535 (1992). This act prohibits the disposal of hazardous waste, including electronic waste, in a manner that could harm the environment. The Pollution Control Department (PCD) is responsible for enforcing the act. However, the PCD has limited resources and enforcement has been lax. As a result, electronic waste is often disposed of illegally in Thailand, often in landfills or incinerators. (Thailand's Pollution Control Department, 2022).

Thailand has taken steps to address the issue of WEEE management. For example, a National strategy on WEEE was approved by the cabinet in 2007, and the WEEE Management Bill was proposed, drafted, and recently revised to cope with this problem. In 2021, the Pollution Control Department published a draft version of the WEEE Integrated Management Action Plan for the years 2022 to 2026.

The draft Action Plan included measures to improve WEEE management, such as promoting the procurement of environmentally friendly goods and services and drafting an action plan to promote the procurement of environmentally friendly products and services from 2021 to 2027.

The WEEE Directive, EPSA, and NTCRS are all initiatives that mandate manufacturers to manage the end-of-life of their products. This may include instructions for proper sanitization of data before disposal or recycling.

The higher prevalence of remaining data on second-hand hard drives in Thailand could be due to the absence or ineffective implementation of similar regulations. Moreover, the country's electronics recycling infrastructure might not be as mature or widespread, increasing the likelihood of hard drives being sold on the second-hand market without proper data sanitization.

Additionally, a possible lack of public awareness about the importance of data sanitization before disposing of or selling used electronics might exacerbate the situation. This could stem from an information or education gap concerning the potential privacy risks of not properly erasing data from hard drives.

It is therefore essential for Thailand to bolster its electronic waste and data sanitization regulations and standards, and to heighten public awareness about these critical issues. It would be beneficial for Thailand to consider the guidelines and standards set by international bodies like the ITU. A holistic approach that combines regulation, enforcement, infrastructure development, and public education could help alleviate this problem and align Thailand more closely with the standards observed in regions such as the European Union, the United States, and Australia, and as recommended by the ITU.

5.1.2 Data Destruction Methods:

Secure deletion refers to tools that overwrite data with random or meaningless information, making it difficult to retrieve the original data. On the other hand, physical destruction can include methods like degaussing, incineration, or pulverization. Cryptographic erasure involves deleting the encryption key of encrypted data, effectively rendering it unreadable. Finally, data wiping is a thorough method that overwrites all addressable locations with zero or random data (Kissel et al., 2014).

One key standard often followed for data destruction is the NIST Special Publication 800-88, "Guidelines for Media Sanitization," method. These standards provide detailed procedures for securely disposing of various data types.

5.1.3 Practical Application:

Many companies, particularly those in the IT, finance, and healthcare sectors, employ professional data destruction services. These companies offer secure data destruction services, including hard drive shredding, degaussing, and data wiping. These vendors often provide a certificate of destruction, which serves as evidence of compliance with data protection regulations and is crucial for audit purposes. Real-life applications include companies like Google and Facebook, which have rigorous data destruction policies in place to protect user information when hardware is decommissioned. Many organizations, especially those in sectors like healthcare, finance, and government, also follow strict data destruction protocols to comply with regulations like HIPAA, SOX, and GDPR.

The selection of a data destruction method should be made in consultation with information security experts or legal counsel, who can guide decision-making based on relevant regulations, the company's risk tolerance, and the potential costs associated with data breaches. Moreover, the chosen vendor should ensure a secure chain of custody for data from the moment it leaves the company until it is destroyed.

The use of laboratory equipment for forensic recovery can physically access and examine data storage devices, such as hard drives, USB drives, and other digital media. Laboratory equipment can also be used to extract data from damaged or corrupted devices, as well as to bypass security measures that may be present on the device. This can allow for more accurate and thorough data recovery than software-only methods.

5.2 Suggestions

Using different types of software to recover data can provide more timespan for recovery. This is beneficial because it increases the chances of successful recovery and reduces the amount of time needed to recover data. Different types of software can also provide different levels of accuracy, which can be beneficial depending on the type of data being recovered.

The timespan for buying the hard disk in different periods is also important when designing a study. As trends in sales of hard disk drives may vary, disks should be purchased over a defined period. Repeat studies can also reveal trends in the PC user disk sanitization behavior, as described in (Jones et al., 2010) should be taken into account.

In the case of Thailand, improved communication of the risks associated with sale of second-hand hard disk drives and inadequate data cleaning may be considered.

References

Adam, A., & Clarke, N. L. (2009). Information Security Leakage: A Forensic Analysis of USB Storage Disks. Advances in *Communications, Computing, Networks and Security: Proceedings of the MSc/MRes programmes from the School of Computing, Communications and Electronics, 2007-2008*, 6, 171.

DiskGenius. (n.d.). *DiskGenius Version 5.4.5.14.12 (x64) Professional*. Retrieved October 1, 2023, from https://www.diskgenius.com/aboutus.php

European Commission. (n.d.). *Waste from Electrical and Electronic Equipment (WEEE).* Retrieved from https://environment.ec.europa.eu/topics/waste-and-recycling/waste-electrical-and-electronic-equipment-weee_en.

Fortune. (n.d.). *Secondhand clothing sales to hit $350 billion by 2027*. Retrieved from https://fortune.com/2023/06/19/secondhand-clothing-sales-to-hit-350-billion-by-2027/

Hidayat, A., Sudarmaji, D., Irawan, D., Susanto, L. J., & Mustika, H. P. (2018). Comparative Analysis of Applications OSforensics, GetDataBack, Genius, and Diskdigger on Digital Data Recovery in the Computer Device. *International Journal of Technology & Engineering*, 7(4.7), 445-448.

Hughes, G., & Coughlin, T. (2006). *Tutorial on disk drive data sanitization*. Retrieved from https://www.researchgate.net/publication/229003088_Tutorial_on_Disk_Drive_Data_Sanitization

International Telecommunication Union. (2012). *End-of-life management for ICT equipment*. Retrieved from https://www.itu.int/dms_pub/itu-t/oth/4B/04/T4B0400000B0013PDFE.pdf

Jones, A., Martin, T., & Alzaabi, M. (2016). The 2016 analysis of information remaining on computer hard disks offered for sale on the second hand market in the UAE. *Journal of Digital Forensics, Security and Law*.

Jones, A., Valli, C., Dardick, G. S., & Sutherland, I. (2009). The 2007 Analysis of Information Remaining on Disks offered for sale on the second hand market. *International Journal of Liability and Scientific Enquiry*, *2*(1), 53-68.

References (Cont.)

Jones, A., Valli, C., Dardick, G. S., Sutherland, I., Dabibi, G., & Davies, G. (2010). The 2009 analysis of information remaining on disks offered for sale on the second-hand market. *Journal of Digital Forensics, Security and Law, 5*(4), 3.

Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014). *NIST Special Publication 800-88 Revision 1: Guidelines for Media Sanitization.* National Institute of Standards and Technology.

Lim, C., Firdausi, I., & Bresnev, A. (2014). Forensics analysis of corporate and personal information remaining on hard disk drives sold on the secondhand market in Indonesia. *Advanced Science Letters, 20*(2), 522-525.

Thailand's Pollution Control Department. (2022). *Draft Action Plan for Integrated Management of Waste Electrical and Electronic Equipment (WEEE) (2022-2025).* Ministry of Natural Resources and Environment. Retrieved from https://www.pcd.go.th/wp-content/uploads/2021/07/pcdnew-2021-07-19_06-41-36_736367.pdf

U.S. Environmental Protection Agency. (n.d.). *Basic Information about Electronics Stewardship*. Retrieved from https://www.epa.gov/smm-electronics/basic-information-about-electronics-stewardship.

Victoria Government Gazette. (2018, June 28). *No. G 26*. Retrieved June 19, 2023, from www.gazette.vic.gov.au.

Weinschenk, C. (2010, July 20). *Hardware Today: Shopping the Second-Hand Server Market. Server Watch*. Retrieved from https://www.serverwatch.com/hardware/hardware-today-shopping-the-second-hand-server-market/

Biography

Name	Manasawee Funge-Smith
Date of birth	11 January 1989
Education background	University of Reading, United Kingdom Bachelor of Science in Biological Sciences, 2011
Address	Bangkok, Thailand
Work position	Cybersecurity Consultant ISO/IEC 27001:2022 Lead Auditor IRCA Project+, CASP+, ECHv11, Security+, PenTest+, CySA+, CSIE, CSAE, CNSP, CSAP, CCIE, CPSP, CCSS. Google IT Support Specialization Google Data Analytics Specialization Google Project Management: Specialization Google Digital Marketing & E-commerce Specialization