Data Sanitization Framework for Computer Hard Disk Drive: A Case Study in Malaysia

Nooreen Ashilla Binti Yusof[1], Siti Norul Huda Binti Sheikh Abdullah[2], Monaliza Binti Sahri[5]
Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia
43600 Bangi, Selangor, Malaysia

Mohamad Firham Efendy bin Md Senan[3]
Nor Zarina binti Zainal Abidin[4]
Digital Forensic Department, CyberSecurity Malaysia
Level 5, Tower 1, Menara Cyber Axis, Jalan Impact
63000 Cyberjaya, Selangor, Malaysia

***Abstract*—In digital forensics field, data wiping is considered one of the anti-forensics' technique. On the other perspective, data wiping or data sanitization is the technique used to ensure that the deleted data are unable to be accessed by any unauthorized person. This paper introduces a process for data sanitization from computer hard disk drive. The process was proposed and tested using commercial data sanitization tools. Multiple testing has been conducted at accredited digital forensic laboratory of CyberSecurity Malaysia. The data sanitization process was performed using overwritten method provided by state-of-the-art data sanitization tools. For each sanitization tool, there are options for the wiping technique (overwritten) process. The options are either to wipe using single pass write or multi pass write. Logical data checking in the hard disk sector was performed during pre and post data disposal process for a proper verification. This is to ensure that the entire sector has been replaced by data sanitization bit pattern in correspondence to the selected wiping technique. In conclusion, through the verification of data sanitization it will improve the process of ICT asset disposal.**

Keywords*—*Data sanitization; anti-forensics; digital forensics; wiping technique

I. Introduction

Data security is nation major concern to curb data breach recklessly [1]. Several approach to handle security breach such as the introduction of steganography and cryptography [2] were tested. These techniques help to improve quality of the data and security [2] during data acquisition for forensic analysis. However, to protect data on media storage such as hard disk drive and magnetic media is depends on two recovery methods [3] [4], are: (i) hardware and (ii) software. The challenges faced on data protection techniques is data privacy and manipulation [1] of data which may lead to privacy violations such as electronic crime [5] for hard disk drive users.

The delete and format method are commonly used by users to dispose their data [6] from hard disk drive. Both methods of data disposal are provided by the computer operating system [6], [7]. Previous researchers [7], [8], [9], [10] suggested the data disposal by using data sanitization methods instead of the delete and format method before the hard disk drive been discarded or sold. Currently, the data sanitization follows the NIST Special Publication 800-88 (Revision 1) Guidelines for Media Sanitization but there is no process of data sanitization from hard disk drive that can be referred online. Hence, this paper introduces the data sanitization process including verification process to dispose the data from the hard disk drive.

The number of overwrite pass becomes an issue to researchers as some of them said single pass overwrite is sufficient [6] to delete the data in the hard disk drive. In fact, the overwriting method proposed by NIST 800-88 to dispose of the data from the hard disk drive is simply to perform at least single pass overwrite with a fixed data value, such as all null [7]. The controversial of the number of overwrite pass exists because some say that data can be recovered if the method of data deletion is done using single or two passes overwrite [6]. Therefore, the purpose of this study is to conduct the number of overwrite pass take in order to completely remove the data from the hard disk drive and secure from data recovery activities.

There are two objectives highlight in this research: i) to identify the data disposal methods from the hard disk drives to be disposed, and ii) to propose the best practise or standard of procedure for data disposal logically from hard disk drive that secure from any data recovery activities, easy-to-understand, follow the data sanitization guideline and standards. We organize this paper into five sections: Introduction, Research background, Methodology, Experimental Results and Analysis, and Conclusion and Future Work.

II. Research Background

There are four methods for deletion of data from digital devices which are: i) delete, ii) format, iii) data sanitization, and iv) physically destroying the media [7], [11], [12]. A generic approach for enterprises to automatically sanitize sensitive data in images and documents is browser-based cloud storage. CloudDLP utilizes deep learning methods to detect sensitive information in both images and textual documents [13]. FlashGhost [14], which is a software that apply a novel integration of cryptography techniques with the frequent colliding hash table is used to erase data in both client and server site. Consequently, data will be unreadable and unrecoverable by overwriting multiple times after its validity period has expired. In a shared IoT environment, [15] a data sanitization approach is present via hierarchical-cluster method to hide confidential information while finding the useful and meaningful information in the sanitized dataset

using multi-objective particle swarm optimization framework. Formatting [7] is the most common approach adopted to remove data in a hard disk. This is based on an interview among users where the results show that users are more prone to use the format method. The study on the comparison has been done [6], [8] between the three methods of deleting, formatting and sanitizing the data. A study [8] shows that the delete and format method are not safe due to lower security [8] compared to the method of sanitizing data which possess better security. Based on [7], [8], [9], [10] safest way to wipe data is by using sanitizing method. The sanitization of data is safer as both file navigator and the file are completely deleted from the media storage [8] by using the overwrite method by replacing the data with zero and one bit.

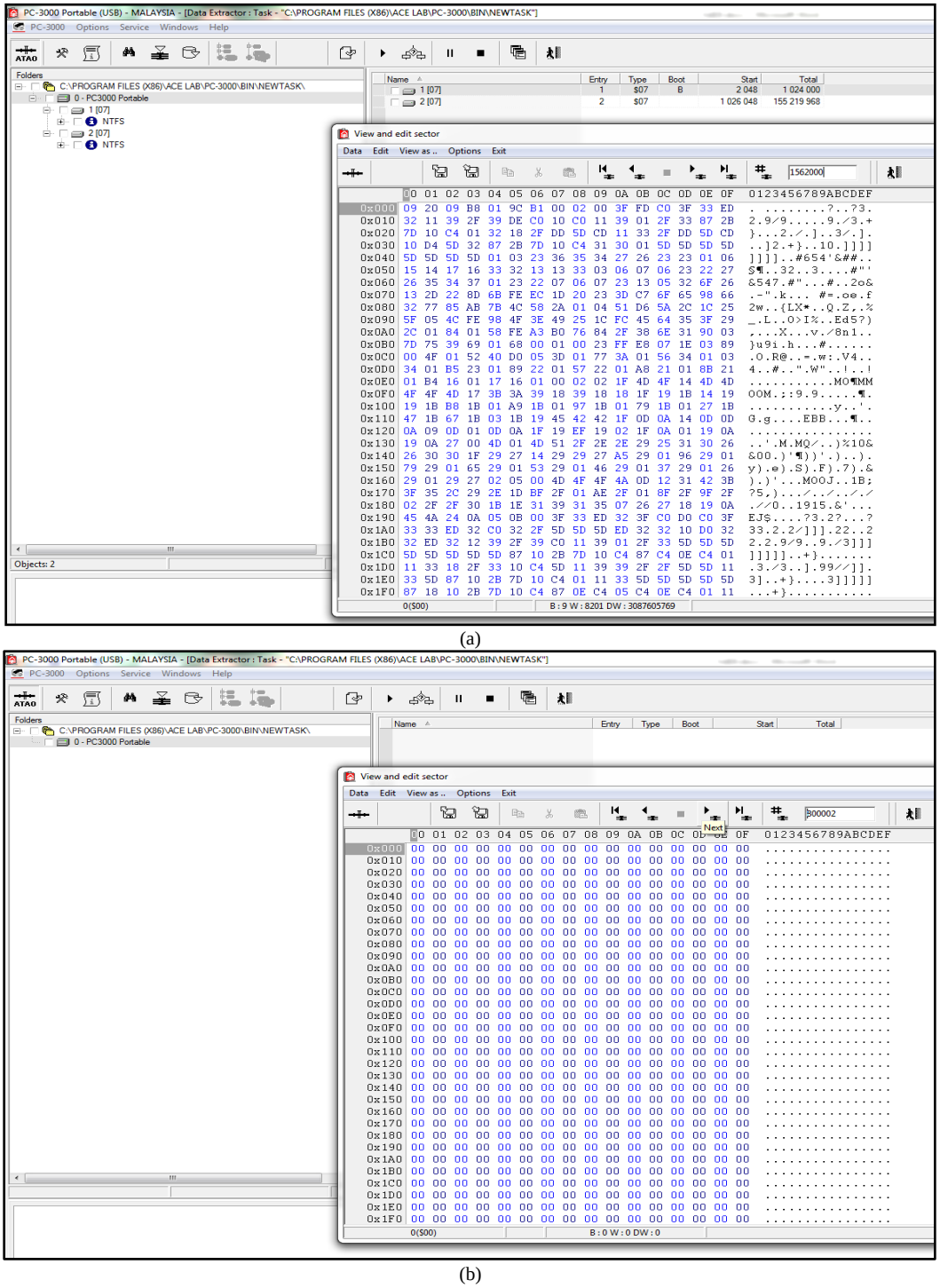

Fig. 1. The Pattern of Logical Data before Data Sanitization using Overwrite Technique. (b) The Pattern of Logical Data after Data Sanitization using Overwrite Technique.

There are a few standards that need to be followed in handling data sanitization [9] according to Department of Defense of United States of America. The first standard in handling data sanitization is DoD 5520 [9] from Department of Defense of United States of America. DoD 5520 states that clearing and sanitization matrix needs two ways to overwrite the data followed by validation [8]. However, revolution of hard disk renders DoD 5220 irrelevant as the first two ways did not function well and need to be updated [8], [9]. Next, DoD 5520.22-M is introduced to replace DoD 5220 in 1995 [12], [16]. Nevertheless, DoD 5220.22-M is not recognized by the Department of Defense of United State of America as the standard to sanitize the hard disk [12] and did not approve it as a secure method for hard disk drive [12]. DoD 5520.22-M is then improved to DoD 5220.22-M ECE in 2001 [12] by increasing the repetition of overwrite operation to seven times. However, DoD 5220.22-M ECE is also not applied as much as a single overwrite pass is already sufficient instead of overwriting it multiple times [12] to sanitize hard disk. Department of Defense of United State of America then replaced DoD 5220.22-M ECE with NIST 800-88 in 2006 [8]. NIST 800-88 emphasizes the method to sanitize the hard disk and other storage media electronic with minimum requirement of implementation of sanitization of media. NIST 800-88 [17] is rechecked again and improved to NIST 800-88 [11] in 2014. It has been used until today. NIST 800-88 [11] states that verification for each data sanitization process is a necessity. The use of tools or software for data sanitization that has been verified and recommended by organization [11]. There are two methods that can be used for verification by either doing: i) verification each time the re-write is performed, or ii) verification on sampling technique.

Data sanitization in theory is referring to overwrite technique [11], [18] to a logical data. Data sanitization method through overwrite technique, will overwrite all the existing logical data bit pattern with a fixed non-sensitive logical data bit pattern on the entire hard disk drives [11]. The following Fig. 1 shows the logical checks on the sectors in the hard disk drive before (Fig. 1(a)) and after the disposal of logical data (data sanitization) is executed (Fig. 1(b)).

In 1996 [10], Gutmann states theoretically, that data which has been overwritten can be restored by using specialized technique such as the magnetic force microscopy (MFM) technique. To avoid data recovery, Gutmann suggests that the secure data deletion method by overwrite pass is executed 35 times in order to make it difficult for recovery process. The overwrite method uses random passes before and after the erase process and in between it the bit is replaced with pattern as shown in Table I.

The Gutmann method takes too much time [6] [19] because the data needs to be overwritten up to 35 pass to delete the data. In 2014, NIST 800-88 [11] outline the minimum number of overwrite pass stated in the Minimum Sanitization Recommendation as in Table II.

NIST 800-88 [11] emphasizes that single pass is sufficient to prevent the deleted data from any data recovery attempts.

TABLE. I. GUTMANN THEORY [10]

Number of Overwrite Pass	Logical Data Bit Pattern
1-4	random value
5	01010101 01010101 01010101
6	10101010 10101010 10101010
7-9	10010010 01001001 00100100 01001001 00100100 10010010 00100100 10010010 01001001
10	00000000 00000000 00000000
11	00010001 00010001 00010001
12	00100010 00100010 00100010
13	00110011 00110011 00110011
14	01000100 01000100 01000100
15	01010101 01010101 01010101
16	01100110 01100110 01100110
17	01110111 01110111 01110111
18	10001000 10001000 10001000
19	10011001 10011001 10011001
20	10101010 10101010 10101010
21	10111011 10111011 10111011
22	11001100 11001100 11001100
23	11011101 11011101 11011101
24	11101110 11101110 11101110
25	11111111 11111111 11111111
26-28	same as overwrite pass 7-9
29-31	01101101 10110110 11011011 10110110 11011011 01101101 11011011 01101101 10110110
32-35	random value

TABLE. II. NUMBER OF OVERWRITE PASS RECOMMENDED BY NIST 800-88 [11]

Number of Overwrite Pass	Logical Data Bit Pattern
1	00000000 00000000 00000000

III. METHODOLOGY

There are two objectives to be achieved in this methodology, namely to propose a data sanitization framework and to perform a detail analysis on data disposal methods. Before proposing the data sanitization framework, a questionnaire is distributed to few agencies to gather information on how the agencies handle hard disk drive disposal and the current awareness on the importance of data sanitization. The data gathered is presented on the experimental results and analysis section. This questionnaire helped in proposing a better and secure data sanitisation framework. After that data disposal methods and data sanitization process will be tested and analysed. After the data sanitization process has been run and tested, an expert assessment and user acceptance is conducted by the expert from Cyber Security Malaysia (CSM) to verify the process.

Section 3.1, 3.2 and 3.3 illustrate the detailed steps taken for the methodology.

A. Questionnaire

There are two sets of questionnaires: Set A and Set B. The questionnaires were adapted from eight subsection under Section 4 Information Sanitization and Disposition Decision Making, NIST Special Publication 800-88 [6] Guidelines for Media Sanitization. Two agencies from government administrative agency, and an educational institution were selected as a respondent to this research. The questionnaires were distributed to the implementers (Set A) and supervisors (Set B) that involve in the agency ICT assets disposal.

B. Data Sanitization Tools used in this Research

19 units of hard disk drives to be disposed were obtained from two agencies for this work. All hard disk drives received with different size, manufacturer, type (SATA and IDE) and model [7]. Then, the hard disk drive was connected directly to the sanitization tool for sanitization process and format activity. Table III listed five data sanitization tools provided by CSM being used in this research.

In addition, PC-3000 which is a portable hardware software is used to perform logical checks and to perform data recovery on hard disk drives during this research to make sure that all the data in the drive that have been sanitized is completely removed.

C. Data Sanitization Process from Computer Hard Disk Drive

The proposed logical data disposal process is based on the results obtained from the six tests that have been performed. All the activities and processes are then organized into a proper flowchart. The chart shows the process of wiping the hard disk content logically. This is the proposed process without including the data recovery activity. Fig. 2 shows the proposed process to wipe the computer hard disk drive content logically.

1) Receiving hard disk drive: When a hard disk drive was received, all information such as the hard disk drive number, size, model and connection type (SATA / PATA) of the hard disk drives were recorded. The hard disk drive will then be tested whether it was working fine and readable by the computer. If the hard disk worked perfectly fine and could be read by the computer, then proceeded to next step.

2) Logical review of the content of the hard disk drive before the data disposal is conducted: PC-3000 was connected to a computer and then followed by the hard disk drive connected to the PC-3000 to check content of the logical drive and to check the number of partitions of the hard disk drive before disposing all of the data inside the hard disk drive.

3) Data disposal using commercial data sanitization tools: During the data disposal activity, all the data were wiped logically using special data sanitization tools. The data sanitization tools used provides single pass overwrite and multi pass overwrite. The hard disk drive was wiped using both the single pass overwrite and multi pass overwrite methods to compare the result. Information of the executors, data sanitization tools used, and result are all recorded in detail.

4) Implementation of logical data validation: Each data sanitization tool used had an indicator whether the operation performed successful or not. Nevertheless, NIST 800-88 recommends that verification methods to be performed using other tools than the original equipment used to dispose the data logically [11]. Logical data validation is implemented to ensure that data had been wiped entirely from the hard disk drive, and the existing bit had been overwritten by the data sanitization bit pattern. The validation exercise was based on logical data bit patterns after data disposal was carried out. The logical data validation that were performed in this research used the PC-3000 tools.

5) Formatting the hard disk drive: After the data in the hard disk drive had been disposed logically using the data sanitization tools, the hard disk drive could no longer be detected on the computer. This was because when the data sanitization tools wiping the data inside the hard disk drive and removing all the data, the file system of the hard disk drive was also wiped out. So, the hard disk drive needs to be formatted to re-install the file system. This scenario can be implemented in the agencies if the agencies desire to recycle their hard disk drives instead of disposing it physically.

6) File system review in the hard disk sector: The hard disk drive was then connected to the computer to check whether it was working fine, had a file system and could be read by the computer. If the computer could detect it, the hard disk drive was required to be format again.

7) Documentation: All the activities in Fig. 2 were recorded and then consolidated into a documentation for the revision of data disposal activities from the hard disk drive.

TABLE. III. DATA SANITIZATION TOOLS

No	Tools	Wiping Method	Purpose of Usage
i)	Ninja Y-1659	Erase All	i) Wiping the data logically from the hard disk drive.
ii)	Data Hapus	Sanitize	i) Wiping the data logically from the hard disk drive.
iii)	Tableau TD1	One Pass Write Multi Pass Write	i) Wiping the data logically from the hard disk drive. ii) Format the hard disk drive.
iv)	Tableau TD3	One Pass Write Multi Pass Write	i) Wiping the data logically from the hard disk drive. ii) Format the hard disk drive.
v)	Voom 3P Hardcopy	1 pass 4 pass	i) Wiping the data logically from the hard disk drive. ii) Format the hard disk drive.

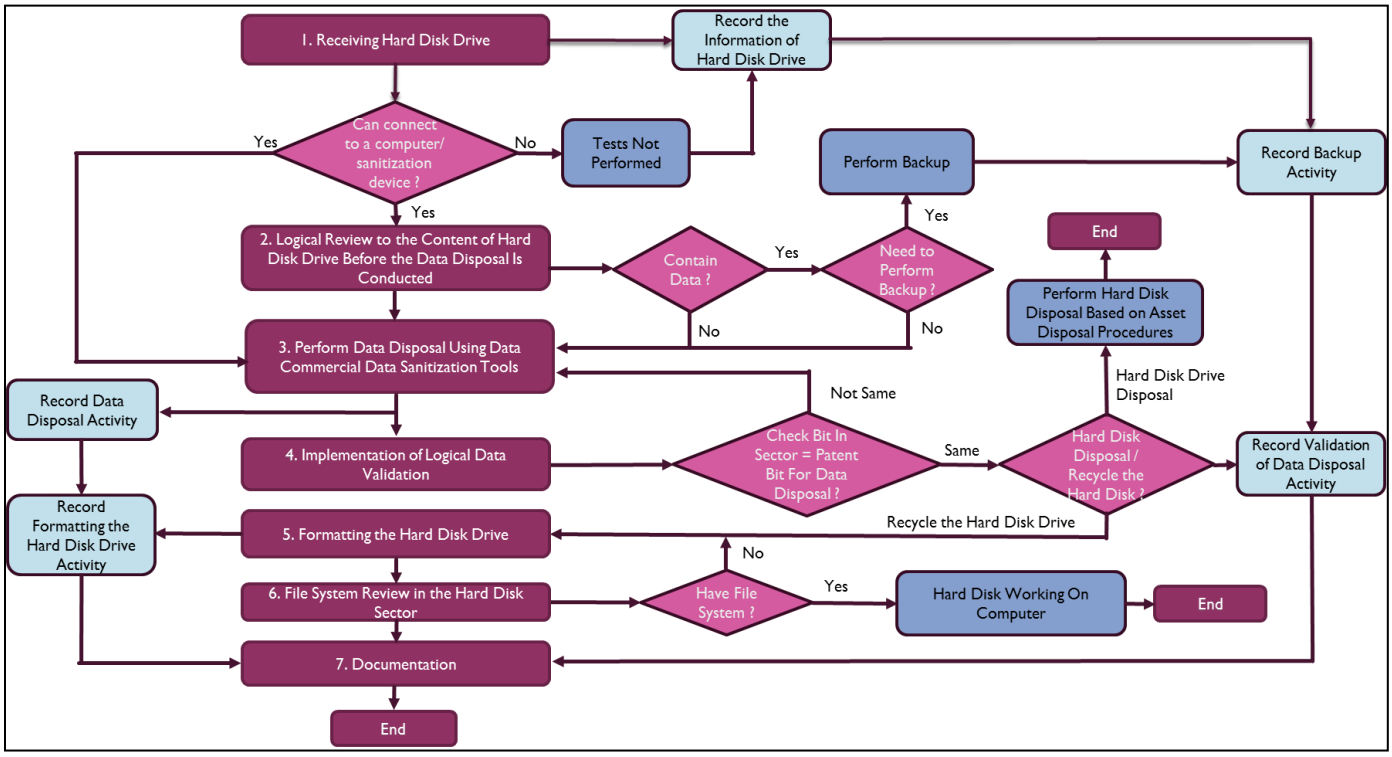

Fig. 2. Proposed Data Sanitization Process from Computer Hard Disk Drive.

IV. Experimental Results and Analysis

We have conducted a pre and post questionnaire for this experiment. The pre-questionnaire was to observe the method of data disposal from hard disk drive of the selected agencies, while the post questionnaire was to observe the relationship of the process of data disposal of hard disk drive between the implementer who conducted the data sanitization process and the supervisor who monitored the data sanitization process at two selected agencies. The result from the questionnaire shows the relationship between the data disposal implementation activities by the implementer and the monitoring activities by the supervisor at Agency B and Agency C and is presented in Table IV.

From the questionnaire, it could be seen that both agencies choose to format the hard disk drive to delete the data prior to disposal of the hard disk drive as opposed to performing a logical data sanitization. Both agencies also did not perform any validation after formatting the hard disk drive.

The analysis also shows that there seems to be discrepancies on the questionnaire between the implementation and monitoring activities in both agencies. Both agencies show a similar percentage of 37.50% and tend to agree to the point that data disposal is a must by the implementers while the percentage on monitoring data disposal exceeds 50.00% in both Agencies B and C. Section A to Section E questionnaire shows agencies implementing data disposal/ protection activities of hard disks drive by formatting it and/ or removing hard disk drives from ICT assets before it is disposed by the agency asset disposition procedure. Disposal of data in the agency does not take into account the level of security of hard disk content even though risk assessment is conducted periodically to determine the level of security of agency assets. Section F to Section H indicates the disposal of data in the agency does not cover the disposal of logical data/ data sanitization. This is because both agencies recognize that they do not have skilled and trained staff to carry out logical data disposal activities from hard disk drives.

The percentage of relationships and gaps between implementers and supervisors for the process of data disposal in both agencies are presented in Fig 3. Fig. 3 shows clear links between the two categories of respondents in data disposal of ICT assets in both agencies. Monitoring activity by the supervisors is at a high percentage for both agencies, which is 50% and 62.50%. Monitoring of data disposal of ICT assets in the agency refers to the method of data disposal using the format method for Agency B and the method of disassembling hard disk pieces for Agency C. All respondents from each agency acknowledged that no logical data disposal was conducted prior to the disposal of ICT assets including hard disk drives in accordance with the asset disposition procedure. The main factor is the absence of skilled and trained staff to carry out logical data disposal activities for hard disk drives. The lack of experts to conduct the logical data disposal makes the percentage of data disposal at both agencies low and equal to 37.50%. This is because the questionnaire developed take into account the good practices of data disposal that need to be taken when disposing data from hard disk based on NIST 800-800 [11].

TABLE. IV. A RELATIONSHIP BETWEEN THE DATA DISPOSAL IMPLEMENTATION ACTIVITIES BETWEEN AGENCIES

Section in Questionnaire	Agency B		Agency C		Average
	Implementer SET A	***Supervisor SET B***	***Implementer SET A***	***Supervisor SET B***	
Section A: Identifying the Needs for Data Disposal	Yes	Yes	Yes	Yes	Yes
Section B: Determination of Information Security Level	**No**	**No**	**No**	Yes	**No**
Section C: Reuse of Hard Disk Drive	Yes	Yes	No	Yes	Yes
Section D: Access Control to the Hard Disk drive	Yes	Yes	Yes	Yes	Yes
Section E: Hard Disk Drive Protection Based on DKICT	**No**	Yes	Yes	Yes	Yes
Section F: Logical Data Disposal of Hard Disk Drive (Data Sanitization)	**No**	**No**	**No**	**No**	**No**
Section G: Validation of Data Disposal	**No**	**No**	**No**	**No**	**No**
Section H: Documentation	**No**	**No**	**No**	**No**	**No**
Percentage Yes (%)	**37.50%**	**50.00%**	**37.50%**	**62.50%**	**50.00%**
Percentage No (%)	**62.50%**	**50.00%**	**62.50%**	**37.50%**	**50.00%**

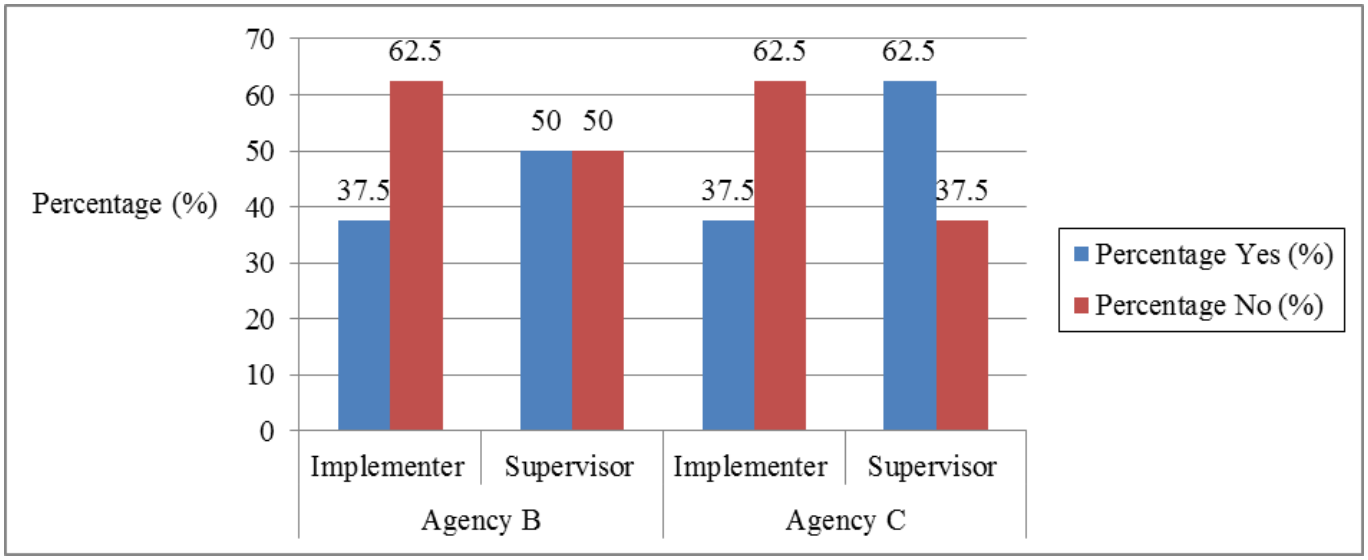

Fig. 3. Analysis Gap between Implementation and Monitoring for the Disposal of ICT Assets in the Agency.

A. Types of Testing

There are five types of tests performed on all hard disk drives received to achieve the second objective, including: i) checking the contents of the logical data before data sanitization, ii) data sanitization using commercial tools, iii) verify whether the logical data has been completely overwritten by bit pattern on the entire hard disk drives, iv) re-format the hard disk drives, and v) data recovery test. All these tests have been conducted at an accredited digital forensic laboratory of CSM using commercial and special hardware and software provided by the Digital Forensics Department. The result on the logical data checks shows that all hard disk drives received, still contains confidential information belong to the agencies which provided the hard disk drives. This study suggested that secure data deletion needs to be done properly by sanitizing the data using overwriting technique. This method wiped the data logically. Data sanitization method through overwrite technique will overwrite all the existing logical data bit pattern to a non-sensitive logical data bit pattern on the entire hard disk drives. Therefore, based on the results and observations from the five tests that have been conducted, a data sanitization process of hard disk drive has been developed. The data recovery test proved that this data sanitization method and process are able to completely wipe all the contents of the hard disk drive. Nineteen hard disk drives provided by selected agencies from

government sector and educational sector are used in the tests. Table V shows that from 19 unit hard disks, two of them still contain data and another two hard disk drives cannot be checked due to hard disk damage and connection failure. Total numbers of hard disk drives used for data sanitization experiment are 17 units.

After the data sanitization process was implemented on all the functioning hard disk drives, the process was then assessed by experts and a user acceptance test was conducted.

B. *Expert Assessment and user Acceptance on the Developed Data Sanitization Process*

This section shows the result of expert assessment and user acceptance analysis.

1) Expert assessment: The proposed data sanitization process had been presented to four experts from the field of digital forensic and data recovery from CSM. Evaluation was based on the presentations and the results of the research presented. The experts then gave their evaluation and feedback on the Expert Assessment Form provided. The evaluations of the four experts were analyzed based on the justifications and feedback options provided on the Expert Assessment Form. This form was filled by each panel with representatives as shown in Table VI.

All four experts agreed 100% on the justification provided in the Expert Assessment Form. The expert agreed that this proposed logical data disposal process complied with technical specifications of the logical data disposal from hard disk drive. It is also successfully adapted to the existing asset disposition procedure in Malaysia, and is suitable for continued implementation at the agency to protect the confidentiality of the information in the hard disk drive to be disposed of.

2) User acceptance: Three (3) agencies were selected for this user acceptance: i) Agency A, ii) Agency B, and iii) Agency C. Agency A refers to government laboratory that provides data sanitization services to the government agencies. They test and run the proposed data sanitization process and fill their evaluation in User / Agency Acceptance Form. The test results show that this proposed process helps them to run data sanitization activities work more systematically. User acceptance for Agency B and Agency C were based on briefing and without actual training. Three (3) agencies were selected for this user acceptance: i) Agency A, ii) Agency B, and iii) Agency C. Agency A refers to government laboratory that provides data sanitization services to the government agencies. They test and run the proposed data sanitization process and fill their evaluation in User / Agency Acceptance Form. The test results show that this proposed process helps them to run data sanitization activities work more systematically. User acceptance for Agency B and Agency C were based on briefing and without actual training. This was because both agencies did not have special data sanitization equipment and tools but they performed ICT asset disposal. The result of analysis and assessment on user acceptance for these three agencies shows in Table VII.

Analysis shows that five out of seven respondents accept 100% with the provided seven justifications of acceptance for the proposed data sanitization process. Two more respondents from Agency C accept 85.71% and 28.57% based on justifications of acceptance options provided in the User/ Agency Acceptance Form. This disadvantage may contribute to a lesser percentage of respondents C2 and C3 from Agency C.

TABLE. V. HARD DISK DRIVE USED FOR THE TESTING PHASE

Item	Government Sector	Educational Institution	Total
Total number of hard disk drives received	15	4	19
Number of hard disks that still have undeleted files/ unformatted	1	1	2
Number of hard disks damaged	2	0	2
Total hard disk used for testing	13	4	17

TABLE. VI. THE DEVELOPED INSTRUMENT FOR EXPERT ASSESSMENT FORM

	Justification (Agree or Disagree)
i.	This proposed data sanitization process is suitable to implement at all agencies.
ii.	This proposed data sanitization process is easier to understand and to implement.
iii.	The proposed data sanitization process is based on the guideline for media sanitization NIST 800-88.
iv.	The testing has been conducted on the actual hard disk drive that agency wanted to disposed
v.	The proposed data sanitization process including the verification process.
vi.	The proposed data sanitization process has been tested with data recovery testing.
vii.	The proposed data sanitization process including documentation activities.
viii.	The proposed data sanitization process makes the data disposal activity more organized based on the checklist provided.
ix.	Data disposal from hard disk drive using special data sanitization tools is easier.
x.	The proposed data sanitization process and documentation can be applied to the existing government ICT asset disposal process
xi.	Employees who involved with logical data disposal do not require high skills to use the proposed data sanitization tools.

TABLE. VII. USER ACCEPTANCE ANALYSIS

Justification for User Acceptance	Agency A	Agency B			Agency C			
	A1	*B1*	*B2*	*B3*	*C1*	*C2*	*C3*	*C4*
i. This proposed data sanitization process is very useful at my agency.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ii. This proposed data sanitization process is easier to understand and to implement.	Yes	Yes	Yes	Yes	Yes	Yes		Yes
iii. The proposed data sanitization process including the verification process.	Yes	Yes	Yes	Yes	Yes	Yes		Yes
iv. The proposed data sanitization process including documentation activities.	Yes	Yes	Yes	Yes	Yes	Yes		Yes
v. The proposed data sanitization process makes the data disposal activity more organized based on the checklist provided.	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
vi. Data disposal from hard disk drive using special data sanitization tools is easier.	Yes	Yes	Yes	Yes	Yes	Yes		Yes
vii. Employees who involved with logical data disposal do not require high skills to use the proposed data sanitization tools.	Yes	Yes	Yes	Yes	Yes			Yes
Percentage (%) of user acceptance based on the justifications provided	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**85.71%**	**28.57%**	**100.00%**

Based on the analysis on Table VII, Agency A fully accepted the proposed data sanitization process since they are given the chance to fully test and run the data sanitization process. Hence, Agency A can fully experience and understand the process of data sanitization which aids in the acceptance of the proposed data sanitization process. Next, Agency B also fully accepted the proposed data sanitization method only based on the briefing without experiencing the data sanitization process and this is because they are experienced in ICT but they do not have the proper data sanitization tools. Other than that, Agency C, two of the respondents which is C2 and C3 respectively do not fully satisfied the proposed data sanitization process due to the lack of experience along with the absence of the data sanitization tools in the agencies. Besides that, other factor that might contribute to not fully accepted the data sanitization proposed method is because the respondents are not technical groups.

V. CONCLUSION AND FUTURE WORK

This research has found that logical data disposal methods using data sanitization methods by overwriting existing logical data bits into data sanitization bit patterns able to remove data permanently and securely from hard disk drives including file system. From the previous research [3], data can be recovered from hard disk drive through files system [3]. Based on the activities and tests carried out in this paper, the proposed logical data disposal framework has been developed in order to guide agencies/ implementers who carry out data disposal from hard disk drives.

This study has achieved both objectives set. The developed data sanitization framework for computer hard disk drive has been reviewed by experts and proved that this framework is comprehensive and secure to protect the deleted contents. In conclusion, content of the hard disk drive can be completely wiped through logical data disposal methods. This technique is carried out through reading and writing techniques using the special data sanitization equipment used in this study. Through this study, it also proves that the proposed data sanitization process is able to completely remove logical data with single pass overwrite. Thus, it may no longer be recovered through data recovery activities.

Therefore, individual and agencies should acknowledge and use this proposed data sanitization framework before discarding the hard disk drive, or before recycling the hard disk drive, or before disposing of the hard disk physically. This is important to protect the confidentiality of sensitive content and information belonging to the individual or agencies from being accessed by the third party.

However, this research was focusing on the hard disk drive from the normal PCs or servers. For future work, the research will look into data sanitization from mobile devices such as tablet PC and handphones for asset disposal process.

ACKNOWLEDGMENT

Special thanks to Universiti Kebangsaan Malaysia for the grant support PP-FTSM-2019 and UKM-AP-2017-005/2. Furthermore, special gratitude to all friends and colleagues who give the comments and support for this work as well as CSM for the used tools and laboratory, and to Center of Information Technology, Universiti Kebangsaan Malaysia (UKM), and two agencies representing government sector and educational institution for providing hard disk drives samples.

REFERENCES

[1] Akbar Khanan, Salwani Abdullah, Abdul Hakim H. M. Mohamed, Amjad Mehmood, and Khairul Akram Zainol Ariffin, "Big Data Security and Privacy Concerns: A Review," in Proceedings of the 1st American University in the Emirates International Research Conference, 2017, pp. 55–62.

[2] Samar Kamil, Masri Ayob, Siti Norul Huda Sheikh Abdullah, and Zulkifli Ahmad, "Challenges in Multi-Layer Data Security for Video Steganography Revisited," Asia-Pacific J. Inf. Technol. Multimed., vol. 7, no. 2–2, pp. 53–62, 2018.

[3] Kenan Kalajdzic and Ahmed Patel, “A Fast Practical Method for Recovery of Lost Files in Digital Forensics,” J. Internet Technol., vol. 10, no. 5, 2009.

[4] K. Kalajdzic and A. Patel, “A Fast Scheme for Recovery of Deleted Files with Evidential Recording for Digital Forensics,” in Proceedings of the Fourth International Workshop on Digital Forensics & Incident Analysis, 2009, no. WDFIA, pp. 9–19.

[5] Razana Md Salleh, Masnizah Mohd, and Kamarul Baharin Khalid, “Validation of Digital Forensics Tools for Android Tablet,” J. Inf. Assur. Secur., vol. 9, pp. 19–26, 2014.

[6] A. Al Anhar, M. Gandeva Bayu Satrya ST., and F. A. Yulianto, “Analisis perbandingan keamanan teknik penghapusan data pada hardisk dengan metode DoD 5220.22 dan Gutmann,” in eProceedings of Engineering, 2014, vol. 1, no. 1, pp. 607–613.

[7] S. L.Garfinkel and A. Shelat, “Remembrance of data passed: A study of disk sanitization practices,” IEEE Secur. Priv., pp. 17–27, 2003.

[8] G. F. Hughes, D. M. Commins, and T. Coughlin, “Disposal of disk and tape data by secure sanitization,” IEEE Secur. Priv., pp. 29–34, 2009.

[9] R. Raman and D. Pramod, “A study on data privacy, protection & sanitization practices during disk disposal by Indian educational institutes,” Int. J. Comput. Sci. Issues, vol. 10, no. 2, pp. 1–6, 2013.

[10] K. Sansurooah, H. Hope, H. Almutairi, F. Alnazawi, and Y. Jiang, “An investigation into the efficiency of forensic data erasure tools for removable USB flash memory storage devices,” in Australian Digital Forensics Conference, 2013.

[11] R. Kissel, A. Regenscheid, M. Scholl, and K. Stine, “NIST Special Publication 800-88 (Revision 1) Guidelines for Media Sanitization,” 2014.

[12] R. Stiennon, “Everything You Need to Know About the DoD 5220.22-M Wiping Standard & Its Applications Today,” blancco, 2017. [Online]. Available: https://www.blancco.com/blog-dod-5220-22-m-wiping-standard-method/. [Accessed: 30-Jan-2018].

[13] C. Liu, P. Han, Y. Dong, H. Pan, S. Duan and B. Fang, "CloudDLP: Transparent and Automatic Data Sanitization for Browser-Based Cloud Storage," 2019 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 2019, pp. 1-8.

[14] Y. Zhu, S. Yang, W. C. Chu and R. Feng, "FlashGhost: Data Sanitization with Privacy Protection Based on Frequent Colliding Hash Table," 2019 IEEE International Conference on Services Computing (SCC), Milan, Italy, 2019, pp. 90-99.

[15] J. C. Lin, J. M. Wu, P. Fournier-Viger, Y. Djenouri, C. Chen and Y. Zhang, "A Sanitization Approach to Secure Shared Data in an IoT Environment," in IEEE Access, vol. 7, pp. 25359-25368, 2019.

[16] M. Geiger, “Evaluating Commercial Counter-Forensic Tools,” Digit. Forensic Res. Work., vol. 1, pp. 1–12, 2005.

[17] R. Kissel, M. Scholl, S. Skolochenko, and X. Li, “Guidelines for Media Sanitization Reports on Computer Systems Technology,” 2006.

[18] P. Gutmann, “Secure deletion of data from magnetic and solid-state memory,” in Sixth USENIX Security Symposium, 1996, pp. 77–90.

[19] C. Valli and P. Patak, “An Investigation into the efficiency of forensic erasure tools for hard disk mechanisms,” in Proceeding of 3rd Australian Computer, Network & Information Forensics Conference, 2005, pp. 79–83.