# Analisis Perbandingan Keamanan Teknik Penghapusan Data pada *Hardisk* dengan Metode DoD 5220.22 dan Gutmann

# Comparative Analysis of Data Deletion Technique Security on Hard disk with DoD 5220.22 and Gutmann Method

**Azwar Al Anhar[1], Gandeva Bayu Satrya ST.,MT.[2], Fazmah Arif Yulianto[3]**

[1,2,3]Prodi S1 Teknik Informatika, Fakultas Informatika, Universitas Telkom
[1]from.rein@gmail.com, [2]gandeva.bayu.s@gmail.com, [3]fazmaharif@telkomuniversity.ac.id

**Abstrak**

**Kerahasiaan informasi sebuah data perorangan maupun dalam skala besar seperti perusahaan adalah hal yang perlu dijaga agar tidak dapat diketahui secara bebas oleh orang lain. Salah satu cara untuk menjaga kerahasian itu adalah dengan melakukan penghapusan data pada media penyimpanan. Namun penghapusan data yang dilakukan secara normal akan lebih mudah untuk dapat dilakukan pemulihan data kembali dengan menggunakan perangkat lunak yang banyak tersebar luas di dunia maya. Oleh karena itu diperlukan teknik khusus untuk melakukan penghapusan data agar tidak mudah dilakukan pemulihan kembali oleh orang yang tidak berhak.**

**Pada tugas akhir ini diadakan uji teknik penghapusan pada media penyimpanan secara normal dan menggunakan dua metode penghapusan data yaitu DoD 5220.22 dan Gutmann. Parameter pengujian tersebut akan dilihat data yang dapat dipulihkan, integritas data, serta waktu pemulihan yang diperlukan. Pada akhir pengujian didapat hasil bahwa penghapusan dengan metode DoD 5220.22 maupun Gutmann lebih baik dibandingkan dengan penghapusan yang dilakukan secara normal, sedangkan antara metode DoD 5220.22 dan Gutmann akan menghasilkan performansi yang lebih baik pada metode Gutmann, dengan perbedaan yang relatif kecil.**

**Metode DoD 5220.22 maupun Gutmaan sudah cukup untuk melakukan penghapusan data secara aman dan sulit untuk dapat dilakukan recovery secara normal, namun tidak menutup kemungkinan pemulihan dapat dilakukan dengan alat atau teknik yang lebih maju**.

**Kata kunci :** ***anti-forensic, file-recovery, wiping, secure delete***

**Abstract**

**Confidentiality of personal data as well as big scale such as company is a things that need to be guarded so cannot be known by others freely. One way to keep the confidentiality is to perform data deletion on media storage. However, data deletion that performed normally will be easier to do data recovery using software that scattered freely on the internet. Therefore required special technique to do data deletion so that can't be easily recovered by unauthorized people.**

**In this final task will be held data deletion technique test on media storage normally and using two data deletion method which is DoD 5220.22 and Gutmann. The test parameters will be seen recovered data, data integrity, and time to do data recovery In the end of the test obtained result that data deletion using DoD 5220.22 as well as Gutmann method better than deletion that do normally, while between DoD 5220.22 and Gutmann methods will produce performance that better in Gutmann method, with a relatively small difference.**

**DoD 5220.22 as well as Gutmann method is enough to do data deletion safely and hard to do recovery using a normal way. However it's still possible that recovery could do with a tools or technique that more advance**.

**Keywords:** ***anti-forensic, file-recovery, wiping, secure delete***

## 1. Pendahuluan

Metode penghapusan data atau dikenal sebagai *Data Sanitization Method* adalah metode yang digunakan oleh perangkat lunak dalam melakukan penghancuran data agar sulit bahkan tidak dapat dipulihkan kembali secara utuh pada media penyimpanan. Secara umum metode penghapusan data melakukan penulisan ulang pada memori dimana data tersebut disimpan dengan data sampah atau data yang tidak bermakna apapun agar dapat menghilangkan jejak data sebelumnya. Pada riset yang dilakukan sebelumnya telah diketahui bagaimana data dihapus menggunakan beberapa metode seperti *random write* data dengan menggunakan perangkat lunak wipe, *zero* write, dan DoD 5220.22-M pada media penyimpanan SSD (*Solid State Drives*). Efesiensi dan hasil integritas dari metode dan perangkat lunak yang digunakan diuji dengan menggunakan perangkat lunak scalpel untuk dapat melakukan pemulihan data. Pada tugas akhir ini akan diuji metode Gutmann dibandingkan dengan standar *US Department of Defence* yaitu DoD 5220.22-M pada media penyimpanan hardisk dan dilakukan analisis terhadap efesiensi dan integritasnya dengan menggunakan perangkat lunak EnCase, FTK sebagai perangkat lunak yang banyak digunakan praktisi digital forensik dan Recuva, R-Studio, serta Stellar Phoenix sebagai perangkat lunak untuk pemulihan data yang beredar bebas di Internet menurut kepopulerannya. Berbeda dengan penelitian sebelumnya yang hanya menggunakan perangkat lunak scalpel untuk melakukan pemulihan data. Tugas akhir ini menggunakan perangkat lunak pemulihan data yang juga sebelumnya telah dilakukan riset yang telah diuji performansinya untuk melakukan pemulihan data.

Agar dapat mengetahui metode penghapusan data yang memiliki efesiensi dan efektifitas yang lebih baik akan dilakukan percobaan penghapusan data yang terdapat pada sebuah hardisk secara normal untuk menunjukan ketidakamanan cara tersebut dan dengan dua buah metode sanitasi data yaitu DoD 5220.22 dan Gutmann. Sehingga nantinya akan didapat hasil yang menunjukan metode mempunyai hasil yang lebih optimal.

## 2. Dasar Teori

Metode yang biasanya digunakan oleh para user dalam melakukan penghapusan data ialah dengan menekan tombol detele dan mengosongkan folder *recycle bin* atau *trash* pada sistem. User mempunyai anggapan yang mengenai hal ini, user akan mengira data yang dihapus telah benar-benar dihapus. Namun tombol delete hanya menghilangkan *pointer* pada blok media penyimpanan yang menyimpan data dan dianggap sebagai ruang kosong untuk dapat diisi kembali dengan data yang baru [3].

Beberapa metode untuk melakukan sanitasi data ialah [2][3]:

- Melakukan penghancuran media penyimpanan secara fisik
- Menggunakan enkripsi data pada media penyimpanan
- *Degaussing* atau melakukan pengacakan data dengan menggunakan magnet yang kuat pada media *magnetic drive*
- *Overwriting* atau penulisan ulang data pada media penyimpanan agar tidak dapat dilakukan pemulihan

Keamanan penyimpanan data juga dapat dibagi menjadi beberapa tingkatan dan lokasi data tersebut [3] :

- *Data at rest*
  - Melakukan penghapusan dengan penulisan ulang pada data blok pada drive
  - Penghapusan file satuan secara aman
  - Penghancuran fisik media penyimpanan
- *Data in motion*
  - Memberikan perlindungan data dan kunci kriptografi pada perpindahan data
  - Transparansi ke user (enkripsi otomatis)
- *Drive internal encryption* (enkripsi pada media penyimpanan)

### *Pysical Drive Destruction*

Untuk dapat mencegah data dari *recovery*, piringan hardisk dapat dilepas dan dihancurkan agar tidak dapat dilakukan proses *recovery*. Pada standar DoD 5220.22M diperlukan penghacuran secara fisik pada media penyimpanan data untuk data yang bersifat sangat rahasia [4]. Beberapa media penyimpanan data digital mudah dihancurkan dibandingkan hardisk seperti *usb drives, compact disk, magnetic tape*. Penghacuran secara fisik dapat dilakukan dengan berbagai cara seperti dilelehkan, diamplas, dipotong menjadi beberapa bagian, atau dihancurkan dengan bahan kimia [5].

### *Disk Drive Degaussing*

*Degausser* ialah alat untuk menciptakan medan magnet berkekuatan besar untuk dapat menghapus semua rekaman magnetic yang terdapat pada hardisk termasuk posisi *disk head*. Selain itu, *track* dan *motor magnet* juga dihapus oleh medan magnet. Cara ini sama dengan penghancuran secara fisik yang mana setelah dilakukan *degaussing*, hardisk tidak akan dapat digunakan kembali [4].

***Nondestructive Data Erasure***

Penghapusan data pada hardisk secara normal hanya akan menghilangkan nama pada struktur direktori. Data masih terdapat pada hardisk dimana akan dapat dipulihkan sampai dengan lokasi data itu disimpan dilakukan proses *overwriting*. Hanya yang sama berlaku untuk kasus hardisk yang diformat [4]. Penghancuran secara fisik maupun melakukan magnetisasi pada hardisk akan menjamin penghapusan data, namun akan sangat disayangkan karena hardisk tersebut tidak dapat digunakan kembali. Proses *overwriting* merupakan salah satu pilihan untuk dapat melakukan penghapusan data tanpa merusak hardisk agar dapat digunakan kembali.

### 2.1 Block Overwrite Method

Salah satu metode yang yang digunakan untuk melakukan sanitasi data ialah melakukan penulisan ulang pada blok yang berisi data agar data tersebut tidak dapat dilakukan proses pemulihan kembali. Dua buah metode *block overwriting* untuk melakukan penghapusan ialah DoD 5220.22M dan Gutmann.

DoD 5220.22M merupakan standar Departemen of Defense yang melakukan *overwriting* sebanyak 3 *passes* yaitu *bit* 0, *bit* 1 , dan *random bit*. Sedangkan Gutmann melakukan proses *overwriting* sebanyak 35 *passes* [3].

*Tabel 1: Pola bit untuk overwriting pada DoD 5220.22*

| Data Destruction Algorithm | Overwriting Pass | Verification Pass |
|---|---|---|
| US Standard DoD 5220.22 | Pass 1: 0x00<br>Pass 2: 0x01<br>Pass 3: *Random* | 3 |

*Tabel 2: Pola bit untuk overwriting pada Gutmann*

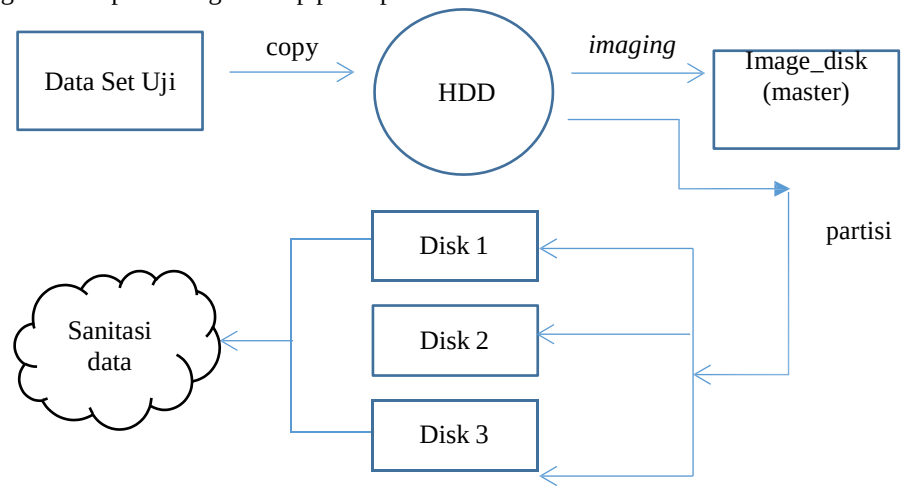
| *Pass* | *Overwritten bit pattern* | |
|---|---|---|
| | *Binary notation* | *Hex notation* |
| 1-4 | Random | Random |
| 5 | 010101010101010101010101 | 55 55 55 |
| 6 | 101010101010101010101010 | AA AA AA |
| 7-9 | 100100100100100100100100<br>010010010010010010010010<br>001001001001001001001001 | 92 49 24<br>49 24 92<br>24 92 49 |
| 10 | 000000000000000000000000 | 00 00 00 |
| 11 | 000100010001000100010001 | 11 11 11 |
| 12 | 001000100010001000100010 | 22 22 22 |
| 13-25 | *Bitpattern from 10 to 25 increase by 0x01 (00 00 00 – FF FF FF)* | 33 33 33 – FF FF FF |
| 26-28 | *same as 7-9* | 92 49 24<br>49 24 92<br>24 92 49 |
| 29-31 | 011011011011011011011011<br>101101101101101101101101<br>110110110110110110110110 | 6D B6 DB<br>B6 DB 6D<br>DB 6D B6 |
| 32-35 | Random | Random |

Perangkat lunak yang melakukan proses *overwriting* secara umum berkerja dengan beberapa mode [6],

1. Perangkat lunak melakukan *overwriting* pada seluruh media
2. Perangkat lunak melakukan overwriting pada tiap-tiap file. Mode ini bergantung pada sistem berkas yang digunakan, file itu sendiri mungkin sudah dilakukan proses *overwriting* namun masih bersisa pada sistem berkas.
3. Perangkat lunak melakukan *overwriting* pada file yang sebelumnya sudah dihapus dengan membuat file baru dan melakukan penulisan pada file tersebut sampai tidak tersisa ruang kosong.

**2.2 Desain Sistem**

Pada tahapan desain sistem, akan dibagi menjadi satu tahapan persiapan dan dua tahapan sistem sanitasi dan pemulihan data, untuk tahapan persiapan akan dibuat *image disk* utama dengan ukuran 20 GB dari USB Hard Disk yang sudah diisi dengan data uji. Dan akan di duplikasi sebanyak dua buah untuk dilakukan percobaan sanitasi data, berikut adalah gambaran perancangan tahap persiapan awal




*Gambar 1: Alur tahapan persiapan sistem*

Pada tahapan selanjutnya, dari tiga buah image disk yang telah diduplikasi sebelumnya akan dilakukan penghapusan dengan menggunakan perintah *delete* pada sistem operasi dan dengan dua buah metode penghapusan DoD 5220.22M dan Gutmann

**2.3 Penghapusan Data**

Penghapusan data dilakukan dengan tiga buah cara yaitu menggunakan cara penghapusan yang dilakukan oleh sistem operasi secara normal, menggunakan metode Gutmann, dan menggunakan DoD 5220.22. Berikut ini adalah tabel penghapusan data pada masing-masing partisi pada hardisk

*Tabel 3 :Partisi dan metode penghapusan yang digunakan*

| No | *Disk Partition* | *Deletion Method* |
|---|---|---|
| 1 | I | OS Deletion |
| 2 | II | DoD 5220.22 |
| 3 | III | Gutmann Method |

**3. Pembahasan**

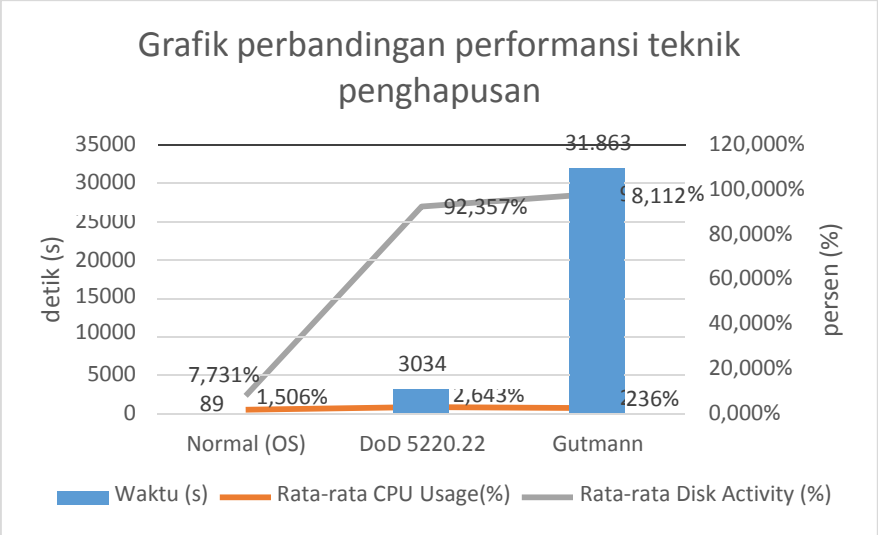
**3.1 Uji performansi teknik penghapusan**

Data yang diujikan untuk melakukan penghapusan data adalah sebanyak 4280 buah file dengan berbagai macam kategori file yaitu terkompresi, dokumen, gambar, music, *pdf*, teks, video. Total ukuran data yang akan dihapus adalah 20 GB dengan jumlah partisi ≥ 20 GB. Berikut adalah perbandingan dari masing-masing teknik penghapusan

*Tabel 4: Perbandingan performansi teknik penghapusan*

| No | Deletion Technique | Waktu | Rata-rata *CPU Usage* | Rata-rata *Disk I/O* |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 1 | Normal (OS) | 1 menit 29 detik | 1,506 % | 7,731 % |
| 2 | DoD 5220.22 | 50 menit 34 detik | 2,643 % | 92,357 % |
| 3 | Gutmann | 8 jam 51m 3 detik | 2,236 % | 98,112 % |




*Gambar 2: Perbandingan performansi teknik penghapusan*

Tabel 4 dan Gambar 2 memperlihatkan bahwa penghapusan secara normal mempunyai waktu yang singkat yaitu sebesar 89 detik atau 1 menit 29 detik dibandingkan dengan DoD 5220.22 dan Gutmann. Sedangkan diantara kedua metode penghapusan digunakan, metode DoD 5220.22 lebih unggul dari segi waktu dan *Disk Activity* yang lebih kecil dibandingkan Gutmann. Parameter *CPU Usage* tidak mempunyai pengaruh yang signifikan terhadap teknik penghapusa

### 3.1 Uji *recovery data*

Pada skenario uji pemulihan data akan dilakukan proses *recovery* untuk mendapatkan kembali data yang telah dihapus dengan masing-masing teknik penghapusan yang telah diujikan sebelumnya. Skenario ini melibatkan lima buah perangkat lunak untuk pemulihan data. Berikut ini adalah banyaknya jumlah file berhasil dipulihkan kembali :

*Tabel 5: Jumlah file yang dapat dipulihkan dan total ukurannya*

| No | Recovery Tools | Disk 1 | | Disk 2 | | Disk 3 | |
|---|---|---|---|---|---|---|---|
| | | *Loadable* | *Size* | *Loadable* | *Size* | *Loadable* | *Size* |
| 1 | FTK | 4282 | 19,9 GB | 0 | 20,3 GB | 0 | 20,3 GB |
| 2 | EnCase | 4255 | 19,9 GB | 0 | 19,9 GB | 0 | 60,6 GB |
| 3 | Recuva | 4263 | 19,9 GB | 0 | 20 MB | 0 | 89 MB |
| 4 | Stellar Phoenix | 4280 | 19,9 GB | 0 | 89,1 MB | 0 | 89,1 MB |
| 5 | R-Studio | 4280 | 19,9 GB | 0 | 40,2 GB | 0 | 40,2 GB |

Table 5 menggambarkan bahwa semua file pada Disk 1 dapat dibaca setelah dipulihkan kembali, sedangkan pada Disk 2 dan Disk 3 tidak terdapat satupun file yang dapat dibuka dan dibaca kembali. Hal ini dikarenakan file yang dapat dipulihkan pada Disk 2 dan Disk 3 adalah file *metadata* dari sistem berkas NTFS dan file sampah yang tidak mempunyai tipe file. Dari hasil diatas menunjukan penghapusan dengan DoD 5220.22 dan Gutmann sudah cukup aman untuk menghilangkan data residu pada hardisk.

### 3.1 Uji data sensitif

Pada skenario ini akan diuji pencarian *string* pada data sensitif yang sisipkan pada data uji. Skenario ini merupakan lanjutan dari skenario sebelumnya yang mana untuk menguji keamanan suatu data yang telah dihapus.

Tiga buah image disk yang telah dihapus sebelumnya diuji menggunakan program *srch_string* dengan filter menggunakan *string* yang dicari maupun dengan *regular expression*. Berikut adalah hasil cari pencarian string yang terdapat pada 7 buah file data sensitif :

*Tabel 6: Checklist string pada data sensitif*

| No | Partisi | *String* ditemukan pada file- | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Disk 2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2 | Disk 3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Keterangan :
File-1 : Kartu Kredit (Master Card).txt
File-2 : Kartu Kredit (Visa).txt
File-3 : Password.txt
File-4 : PIN ATM BCA.txt
File-5 : PIN ATM BNI.txt
File-6 : PIN ATM BRI.txt
File-7 : PIN ATM Mandiri.txt

Table 6 menunjukan bahwa penghapusan yang dilakukan pada Disk 2 (DoD 5220.22) maupun Disk 3 (Gutmann) belum cukup aman untuk dapat melakukan penghapusan data khususnya *string* yang masih menjadi residu pada hardisk tersebut. Hal ini dimungkinkan keterbatasan perangkat lunak dalam melakukan penghapusan secara aman untuk file-file yang ukurannya kecil.

**4. Kesimpulan**

Dari pengujian yang dilakukan dapat diambil beberapa kesimpulan untuk teknik penghapusan normal, DoD 5220.22, dan Gutmann

1. Pada pengujian performansi penghapusan, penghapusan normal mempunyai waktu yang lebih cepat dibandingkan DoD 5220.22 dan Gutmann. Sedangkan Gutmann mempunyai waktu terlama. CPU Usage tidak mempunyai pengaruh yang signifikan terhadap proses penghapusan sedangkan *Disk I/O* mempunyai pengaruh kuat dalam melakukan penghapusan. *Disk I/O* pada penghapusan menggunakan Gutmann mempunyai nilai paling besar dibandingkan DoD 5220.22 dan penghapusan secara normal.
2. Tingkat keamanan dari penghapusan yang dilakukan secara normal sangatlah tidak aman dikarenakan hampir semua perangkat lunak untuk pemulihan dapat mengembalikannya. Sedangkan DoD 5220.22 dan Gutmann sudah cukup aman dengan membuat nama file tidak terbaca dan tidak dapat dibuka. Namun DoD 5220.22 dan Gutmann masih menyisakan residu berupa data *string* yang dapat digali lebih lanjut dan dapat membahayakan apabila ditemukan.

**Daftar Pustaka**

[1] N. Joukov dan E. Zadok, "Adding Secure Deletion to Your Favorite File System," dalam Third IEEE International Security in Storage Workshop (SISW'05), San Francisco, 2005.
[2] L. S. Garfinkel dan A. Shelat, "Remembrance of Data Passed : A Study of Disk Sanitization Practices," IEEE Computer Society, Cambridge, 2003.
[3] V. Bahl, D. Leong , G. Jiayan, J. Siang dan T. M. Lan, "Secure Data Shredder," dalam Proceedings of the Global Engineering, Science and Technology Conference, Dhaka, 2012.
[4] G. Huges dan T. Coughlin, "Tutorial on Disk Drive Data Sanitization," Center for Magnetic Recording Research (CMRR), SanDiego, 2006.
[5] P. Bennison dan Lasher, P.J, "Data security issues relating to end of life equipment," dalam Electronics and the Environment, 2004.
[6] S. Garfinkel, "Anti-Forensic: Techniques, Detection and Countermeasures," dalam 2nd International Conference on i-Wareface and Security, Indiana, 2007.
[7] L. C. Martel, Data Recovery Service Providers, DriverSaver Data Recovery, Inc., 2013.

S. A. Moulton, Scott Moulton's Speech Research Material and Notes on Data Recovery, Forensic Strategy Services, 2007.

[8] M. Freeman dan A. Woodward, "Secure State Deletion : Testing the efficacy and integrity of secure deletion tools on Solid State Drives," dalam Australian Digital Forensics Conference, Perth, 2009.

[9] B. D. Carrier dan E. H. Spafford, "An Event-Based Digital Forensic Investigation Framework," dalam Digital Forensic Research Workshop (DFRWS 2004), Baltimore, 2004.

[10] A. Ariffin, J. Slay dan K.-K. Choo, "Data Recovery from Proprietary Formatted CCTV Hard Disks," Advances in Digital Forensics, vol. IX, pp. 213-223, 2013.

[11] D. Allen, "Digital Investigation Workforce," Carnegie Mellon, CERT, United States, 2012.

H. Al-Hajri dan P. Williams, "The effectiveness of investigative tools for Secure Digital (SD) Memory Card forensics," dalam Australian Digital Forensics Conference, Perth, 2007.

[12] C. Hargreaves dan J. Patterson, "An automated timeline reconstruction approach for digital forensic investigations," Digital Investigation, vol. IX, pp. S69-S79, 2012.

[13] M. C. Johannes Stuttgen, "Anti-forensic resilient memory acquisition," Digital Investigation, vol. X, pp. S105-S115, 2013.

[14] G. F. Hughes, D. M. Commins dan T. Coughlin, "Disposal of Disk and Tape Data by Secure Sanitization," IEEE Computer and Reliability Societies, California, 2009.

[15] J. R. Mallery, "Secure File Deletion: Fact or Fiction," SANS Institute, 2007.

B. Lee, K. Son, D. Won dan S. Kim, "Secure Data Deletion for USB Flash Memory," Journal of Information Science and Engineering, vol. 27, pp. 933-952, 2011.

[16] M. Wei, L. M. Grupp, F. E. Spada dan S. Swanson, "Reliably Erasing Data From Flash-Based Solid State Drives," dalam USENIX Conference on File and Storage Technologies, California, 2011.