Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 4 No. 4 (2020) 736 - 744 ISSN Media Elektronik: 2580-0760

Implementasi Anti Forensik pada Harddisk Menggunakan Metode *DoD 5220.22 M* dan *British HMG IS5 E*

Muh Fadli Hasa[1], Anton Yudhana[2], Abdul Fadlil[3]
[1]Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan
[2,3]Program Studi Teknik Elektro, Universitas Ahmad Dahlan
[1]muh1808048038@webmail.ac.id, [2]eyudhana@ee.uad.ac.id, [3]fadlil@mti.uad.ac.id

Abstract

The process of securing data is related to anti-forensic science, one of the anti-forensic techniques that can be used to safeguard data security, namely by deleting data on storage media. This study examines the implementation of data deletion using the DoD 5220.22 M and British HMG IS5 E methods, then compares these methods. The comparison of the two methods includes performance tests, forensic tests, and data recovery tests. The results of the performance test show that the two methods are strongly influenced by the anti-forensic tools used and do not provide a significant difference when applied using one of the tools. The results of the implementation of data deletion using both methods on the hard disk drive are declared safe to delete data, as evidenced by the extraction results in the forensic test using the Autopsy tool found files on the partition :F with the number of 252 files and on the partition :I with the number of 1 file and the extraction results from the test Forensics using the Recover My File tool managed to find files with the number of 102 files on different partitions, but all the files found in the forensic test process cannot be accessed. The results of the recovery test show that the safest method in the process of deleting data is the British HMG IS5 E method using the Active @ Kill Disk tool, as evidenced by all the results of the recovery process using three tools that do not find any files. Meanwhile, the application of the deletion method that is generally carried out by users, namely the shift + delete method, is declared unsafe, as evidenced by the results of the recovery tests conducted showing that the deleted files can be recovered 100% and can be reaccessed using recovery tools.

Keywords: Anti forensics, British HMG IS5 E, DoD 5220.22 M, Data security

Abstrak

Proses pengamanan data memiliki keterkaitan dengan ilmu anti forensik, salah satu teknik anti forensik yang dapat dilakukan dalam menjaga kemanan data yaitu dengan melakukan proses penghapusan data pada media penyimpanan. Penelitian ini mengkaji implementasi penghapusan data menggunakan metode *DoD 5220.22 M* dan *British HMG IS5 E*, kemudian membandingkan metode tersebut. Perbandingan dari kedua metode yaitu meliputi uji kinerja *(performance)*, uji forensik dan uji pemulihan data *(recovery)*. Hasil uji kinerja *(performance)* menunjukkan bahwa kedua metode sangat dipengaruhi oleh *tools* anti forensik yang digunakan dan tidak memberikan perbedaan yang signifikan ketika diterapkan menggunakan salah satu *tools*. Hasil implementasi penghapusan data menggunakan kedua metode pada *hardisk drive* dinyatakan aman untuk menghapus data, terbukti dari hasil ekstraksi pada uji forensik menggunakan *tool Autopsy* ditemukan *file* pada partisi :F dengan jumlah 252 *file* dan pada pertisi :I dengan jumlah 1 *file* serta hasil ekstraksi dari uji forensik menggunakan *tool Recover My File* berhasil menemukan *file* dengan jumlah 102 *file* pada partisi yang berbeda, namun dari semua hasil temuan *file* pada proses uji forensik tersebut tidak dapat diakses. Hasil uji *recovery* menunjukkan bahwa metode yang paling aman dalam proses penghapusan data yaitu metode *British HMG IS5 E* menggunakan *tool Active @ Kill Disk*, terbukti dari semua hasil proses *recovery* menggunakan tiga *tools* tidak menemukan *file* apapun. Sedangkan pada penerapan metode penghapusan yang secara umum dilakukan oleh *user* yaitu metode *shift+delete* dinyatakan tidak aman, terbukti dengan hasil uji *recovery* yang dilakukan menunjukkan bahwa *file* yang telah dihapus dapat dipulihkan 100% serta dapat diakses kembali menggunakan *tools recovery*.

Kata kunci: Anti forensik, *British HMG IS5 E*, *DoD 5220.22 M*, Keamanan data.

1. Pendahuluan

Kemanan informasi merupakan salah satu aspek yang sangat penting bagi suatu individu ataupun organisasi [1]. Namun masalah kerahasiaan informasi tersebut terkadang kurang mendapatkan perhatian yang serius dari para pemilik informasi. Pentingnya nilai dari suatu

Diterima Redaksi : 15-07-2020 | Selesai Revisi : 13-08-2020 | Diterbitkan Online : 20-08-2020

informasi dapat menimbulkan ancaman bagi pemilik informasi dikarenakan terdapat orang-orang tertentu yang ingin mendapatkan informasi tersebut [2]. Apabila informasi tersebut jatuh kepada orang lain, maka akan mengakibatkan kerugian yang sangat besar bagi pemilik informasi [3].

Salah satu dari 3 aspek utama dalam teori keamanan informasi yaitu kerahasiaan *(confidentiality)* dijelaskan bahwa informasi pada sistem komputer harus terjamin kerahasiaannya dan hanya dapat diakses oleh pihak-pihak yang diotorisasi [4]. Menurut UU Nomor 19 Tahun 2016 Tentang Perubahan UU Nomor 11 Tahun 2008 Pasal 26 Tentang Informasi Dan Transaksi Elektonik secara substansi menjelaskan bahwa penggunaan setiap informasi melalui media elektronik yang menyangkut data pribadi seseorang harus dilakukan atas persetujuan orang yang bersangkutan [5].

Menjaga kerahasiaan suatu informasi memiliki keterkaitan dengan ilmu anti forensik [6]. Ilmu anti forensik merupakan metode untuk menyembunyikan suatu informasi atau *file* yang dianggap sebagai barang bukti digital, namun pada dasarnya mempunyai fungsi positif bagi individu maupun suatu organisasi yang ingin melindungi informasi yang dimiliki, agar tidak terjadi pencurian data dari para pihak yang ingin mendapatkan data tersebut. [7]

Anti forensik bertujuan untuk melindungi informasi atau data dari para pihak yang ingin mendapatkan informasi atau data tersebut untuk disalahgunakan. Pada umumnya anti forensik mengacu pada 2 hal, yang pertama yaitu melakukan tindakan agar data yang tersimpan pada media penyimpanan tidak dapat dibuka ataupun ditemukan dengan menggunakan berbagai metode, kemudian hal yang kedua yaitu mengupayakan agar data atau *file* yang berhasil ditemukan tidak dapat digunakan ataupun tidak sesuai dengan standar hukum yang dalam hal ini berarti data atau *file* tersebut tidak dapat dijadikan barang bukti pada saat proses persidangan. [8].

Penghapusan data merupakan salah satu metode anti forensik yang paling sering digunakan oleh pengguna komputer *(user)*. Pada umumnya metode ini dilakukan dengan menekan tombol *delete* dan mengosongkan *recycle bin* atau *trash* pada sistem. *User* beranggapan bahwa proses yang dilakukan telah benar-benar menghapus data, namun proses tersebut tombol *delete* hanya menghilangkan *pointer* pada blok media penyimpanan *(storage)* yang menyimpan data dan kemudian dianggap sebagai ruang kosong untuk dapat diisi kembali dengan data yang baru [9].

Data yang dianggap telah terhapus sangat berpotensi untuk dilakukan proses *recovery* (dipulihkan) dengan menggunakan ilmu digital forensik, atau dengan kata lain bahwa data tersebut masih memungkinkan untuk didapatkan [10]. Untuk mengatasi tindakan tersebut perlu dilakukan proses penghapusan data pada media penyimpanan *(storage)* yang benar-benar aman sehingga data tersebut tidak dapat dilakukan proses *recovery* [11].

Penelitian pertama dengan tema sejenis yang berjudul Analisis Perbandingan Keamanan Teknik Penghapusan Data pada Hardisk dengan Metode DoD 5220 . 22 dan Gutmann [9]. Penelitian ini membahas tentang pengujian teknik penghapusan pada media penyimpanan secara normal dan menggunakan dua metode penghapusan data yaitu *DoD 5220.22 M* dan *Gutmann*. Hasil dari penelitian ini menjelaskan bahwa penghapusan dengan metode *DoD 5220.22 M* maupun *Gutmann* lebih baik dibandingkan dengan penghapusan yang dilakukan secara normal, sedangkan antara metode *DoD 5220.22 M* dan *Gutmann* akan menghasilkan performansi yang lebih baik pada metode *Gutmann*, dengan perbedaan yang relatif kecil. Adapun kekurangan dari penelitian tersebut terletak pada proses pengujian metode penghapusan serta *tools* yang digunakan cukup terbatas. Perbedaan dengan penelitian yang dilakukan dengan penelitian tersebut terletak pada proses pengujian serta *tools recovery* data pada saat proses percobaan mendapatkan data yang telah dihapus.

Penelitian kedua dengan tema sejenis yang berjudul Implementasi Teknik Penghapusan Data Dengan Metode *DoD 5220 . 22 M* Pada Sistem Operasi Android [12]. Penelitian ini menjelaskan bahwa sebagian besar aplikasi penghapusan dengan menggunakan metode *DoD 5220.22 M* yang berjalan di sistem operasi android belum mampu menghapus *file* dengan benar-benar sempurna. Masih terdapat beberapa *file* yang masih bisa dipulihkan dan dijalankan kembali. Serta masih ada celah keamanan lain yang ditemukan dan memungkinkan informasi dari *file* tersebut dapat bisa digali kembali melalui proses forensik yang lebih dalam. Perbedaan antara penelitian tersebut dengan penelitian yang dilakukan yaitu pada objek penelitian.

Penelitian ketiga dengan tema sejenis yang berjudul *Data security issues relating to end of life equipment* [13]. Penelitian ini menerangkan bahwa metode *DoD 5220.22 M* merupakan salah satu metode yang cukup baik untuk diterapkan dalam proses penghancuran data. Tujuan dari penelitian tersebut yaitu untuk mengamankan data pribadi yang berada pada media penyimpanan yang akan dipindah tangankan. Perbedaan antara penelitian tersebut dengan penelitian yang dilakukan yaitu pada *tools* penerapan metodenya.

Untuk mengatasi keterbatasan penelitian sebagaimana sudah diungkapkan dalam beberapa penelitian sebelumnya, penelitian ini mengkaji penghapusan data menggunakan metode *DoD 5220.22 M* dan *British HMG IS5 E*. Metode ini diaplikasikan untuk menghapus data pada media penyimpanan *harddisk* (HDD). Kedua metode kemudian dianalisa dan membandingkan kinerja metode tersebut.

2. Metode Penelitian

Proses penelitian yang dilakukan yaitu menerapkan penghapusan data menggunakan metode *DoD 5220.22 M* dan *British HMG IS5 E*. Metode DoD 5220.22 M merupakan metode standar penghapusan data yang digunakan oleh pemerintah Amerika Serikat. Proses penghapusan data dengan metode *DoD 5220.22 M* diuraikan seperti berikut ini.

Fase 1 : Menimpa dengan bit 0
Fase 2 : Menimpa dengan bit 1
Fase 3 : Menimpa dengan bit random.

Metode *DoD 5220.22 M* menetapkan proses yang menimpa data pada harddisk dengan pola acak dengan 0 dan 1. Dalam metode tersebut diperlukan tiga *fase overwriting* dimana proses tersebut lebih aman daripada proses penghapusan biasa, seperti yang dilakukan dalam *Departement of Defence*. Melakukan penghapusan data menggunakan metode DoD 5220.22 M ini akan mencegah aplikasi *recovery* file untuk dapat memulihkan kembali data yang telah dihapus [14].

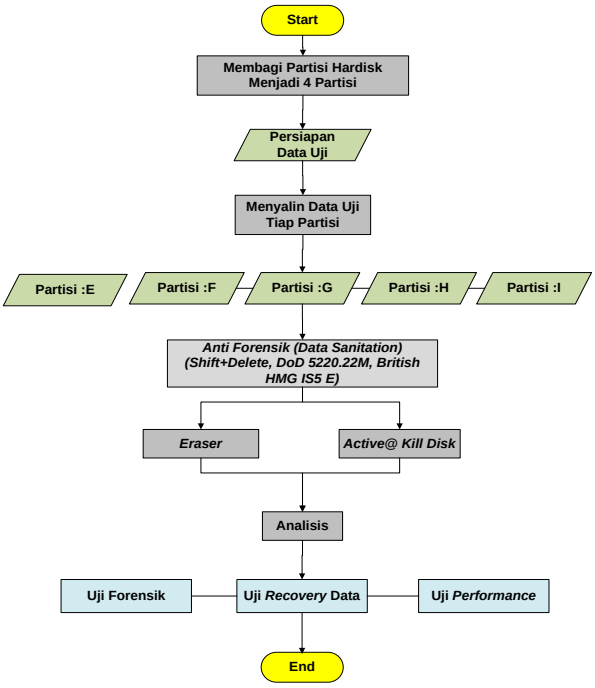
Metode *British HM Goverrntmen Infosec Standard 5 Enhanced (British HMG IS5 E)* merupakan metode yang digunakan oleh pemerintah Kerajaan Inggris sebagai standart *sanization media* (penghapusan data) [15]. Metode tersebut juga melakukan 3 fase penulisan ulang pada media penyimpanan sehingga data yang ada didalamnya tertimpa oleh proses tersebut. Proses yang 3 fase yang digunakan pada metode *British HMG IS5 E* diuraikan seperti berikut ini.

Fase 1 : penulisan bit 0
Fase 2 : penulisan bit 1
Fase 3 : menulis karakter acak dan memferifikasi Penulisan

Penerapan metode *British HMG IS5 E* akan mencegah semua metode pemulihan data yang berbasis perangkat lunak dan juga cenderung mencegah sebagian besar metode pemulihan data berbasis perangkat keras dalam mengekstraksi data dalam suatu *harddrive*.

Perbadaan dari kedua metode tersebut terletak pada proses penimpaan data pada *hardisk*. Metode *DoD 5220.22 M* menetapkan proses yang menimpa data pada harddisk dengan pola acak dengan 0 dan 1, sedangkan pada metode *British HMG IS5 E* proses penghapusan dilakukan dengan penulisan data ulang menggunakan bit 0, bit 1 dan karakter acak.

Kedua metode tersebut kemudian di implementasikan dengan cara melakukan perancangan alur tahapan penelitian. Perancangan alur penelitian merupakan proses atau tahapan yang dilakukan dalam penelitian ini atau langkah-langkah operasi dalam proses pengolahan data. Untuk lebih jelasnya, perancangan alur penelitian dapat dilihat pada Gambar 1.



Gambar 1. Perancangan alur

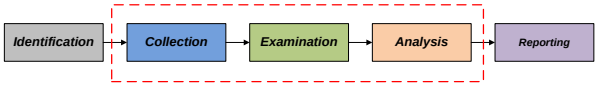
Berdasarkan Gambar 1, proses yang dilakukan pada penelitian ini dimulai dari tahap persiapan yaitu dengan membagi HDD menjadi 5 partisi dengan ukuran 21 *GB* dari *harddisk* dan kemudian diisi dengan data uji. Tahap selanjutnya yaitu melakukan proses penghapusan terhadap masing-masing partisi dengan menerapkan proses penghapusan *shift+delete*, menerapkan metode penghapusan *DoD 5220.22 M* dan menerepkan metode *British HMG IS5 E* menggunakan *tool eraser* dan *active@ kill disk.*

Tahapan berikutnya yaitu tahap analisis, tahapan ini dilakukan proses analisa terhadap partisi yang telah dilakukan proses penghapusan. Tahap analisis dilakukan dengan menggunakan 3 bentuk pengujian, yaitu uji kinerja metode penghapusan, uji forensik, dan uji *recovery*.

Proses analisa yang pertama yaitu melakukan uji kinerja metode penghapusan merupakan proses pengukuran kinerja metode penghapusan berdasarkan *tools* yang digunakan. Uji kinerja *(performance)* bertujuan untuk mengetahui tingkat kecepatan serta penggunaan sumber daya dari metode penghapusan dalam melakukan proses menghapus data. Proses uji *performance* dilakukan dengan cara mengukur rata-rata penggunaan *CPU, Running Time*, dan *Memory* pada saat proses implementasi metode penghapusan. Proses ini menggunakan *tools* yang ada sistem operasi windows 10 yaitu *Task Manager.*

Proses analisa yang kedua yaitu uji forensik yang dilakukan dengan tujuan untuk mengetahui tingkat keamanan dari proses penghapusan data dengan menerapkan metode anti forensik yang dilakukan dalam penelitian ini. Proses uji forensik dilakukan dengan

menggunakan standart *National Institute of Justice (NIJ)* yang terbagi menjadi 5 tahapan yaitu *Identification, Collection, Examination, Analysis,* dan *Reporting.* Namun pada penelitian ini hanya menggunakan 3 tahapan yaitu *Collection, Examination,* dan *Analysis.* Untuk lebih jelasnya tahapan NIJ dapat dilihat pada Gambar 2.



Gambar 2. Tahapan NIJ

Tahap *Collection* merupakan proses duplikasi dari barang bukti fisik yang otentik ke bukti digital untuk menjaga integritas barang bukti dari perubahan. Penjagaan barang bukti fisik dan membuat duplikasi menjadi *image* proses ini dinamakan akuisisi. Tahap *Examination* atau disebut tahap pemeriksaan, hasil *image* diekstrak sehingga data digital yang ada didalamnya sama dengan barang bukti fisik. tahapan ini memastikan data yang didapat asli dan akan dicek validasinya menggunakan *hashing*. Tahap *analysis* dilakukan setelah mendapatkan data digital yang diinginkan dari proses pemeriksaan sebelumnya, kemudian data tersebut dianalisa secara detail dengan metode yang dibenarkan secara teknik dan hukum untuk dapat membuktikan data tersebut.

Proses analisa yang ketiga yaitu uji *recovery*, uji *recovery* dilakukan dengan tujuan untuk mengetahui seberapa besar tingkat keberhasilan metode dalam melakukan proses penghapusan data. Proses uji *recovery* dilakukan dengan menghubungkan HDD secara langsung dan menggunakan *tool recovery* yang telah disiapkan. Proses uji *recovery* dibagi menjadi 3 sesi sesuai dengan jumlah *tools recovery* yang digunakan dan metode penghapusan yang diterapkan proses uji *recovery* dilakukan dengan menggunakan beberapa *tools*. Penjelasan *tools recovery* dan spesifikasinya dapat dilihat pada Tabel 1.

Tabel 1. Spesifikasi *tools data recovery*

No.	Nama	Versi
1	*MiniTool Power Data Recovery*	8.0.6
2	*EaseUS Data Recovery*	5.2.1
3	*Recuva*	1.53

2.1 Objek Penelitian

Objek penelitian yang digunakan pada penelitian ini adalah *hard disk drive* merk *HITACHI* dengan kapasitas 120 GB yang digabagi menjadi 4 partisi, dengan tambahan alat pendukung lainnya seperti *case* eksternal *merk Orico* agar HDD dapat dijadikan storage eksternal. Data uji yang digunakan dalam penelitian ini merupakan kumpulan berbagai jenis *file* yang memiliki ekstensi yang berbeda yang digunakan sebagai sample bukti digital dalam penelitian ini. Daftar sampel data uji yang digunakan dalam penelitian ini dapat dilihat pada Tabel 2.

Tabel 2. Sampel data uji

Jenis File	Ekstensi	Jumlah
Dokumen Ms Word	.docx	10
Dokumen Ms Excel	.xlxs	10
Dokumen Ms Power Point	.pptx	10
Dokumen Adobe	.pdf	10
Gambar	.jpg	10
Gambar	.png	10
Video	.Mp4	10
Audio	.Mp3	10
File Aplikasi *(executable)*	.exe	10
File Kompresi	.zip	10
	Total	100

2.2 Persiapan Alat dan Bahan

Alat dan bahan yang digunakan dalam penelitian ini dapat dilihat pada Tabel 3.

Tabel 3. Alat dan bahan

No	Alat dan Bahan	Deskripsi/Spesifikasi	Keterangan
1.	Laptop	*Merk Asus A455L Series*	*Hardware*
2.	Sistem Operasi	*Windows 10 Pro 64 Bit*	*Software*
3.	*Hard Disk Drive*	Hard Disk dengan kapasitas 120GB	*Hardware*
4.	*Hardisk Case*	*Case* yang digunakan untuk menghubungkan HDD ke lapto	*Hardware*
4.	*Eraser*	Tools anti forensik yang digunakan untuk melakukan penghapusan data	*Software*
5.	*Active@ Kill Disk*	Tools anti forensik yang digunakan untuk melakukan penghapusan data	*Software*
6.	*FTK Imager*	Tools forensik yang digunakan untuk melakukan imaging dan analisis	*Software*
7.	*MiniTool Power Data Recovery*	Tools yang digunakan untuk proses *Recovery*	*Software*
8.	*Recuva*	Tools yang digunakan untuk proses *Recovery*	*Software*
9.	*Recover My File*	Tools yang digunakan untuk proses *Examination*	*Software*
10.	*EaseUS Data Recovery*	Tools yang digunakan untuk proses *Recovery*	*Software*

3. Hasil dan Pembahasan

3.1 Proses Implementasi Anti Forensik

Proses implementasi yang pertama yaitu proses penghapusan dengan cara s*hift+delete* yang dilakukan berdasarkan pada kebiasaan *user* dalam menghapus suatu *file.* Pada proses ini dilakukan penghapusan *file* pada partisi :E yang telah diisi dengan data uji. Penerapan metode penghapusan S*hift+Delete* menunjukkan proses yang tergolong sangat cepat. Waktu yang diperlukan dalam proses penghapusan dengan menggunakan metode S*hift+Delete* yaitu hanya 3 detik. Pada pengamatan yang dilakukan dalam proses penghapusan tidak dapat dilakukan proses pengukuran presentase penggunaan CPU dan memori.

Proses implementasi yag kedua yaitu proses penghapusan data dengan menerapkan metode *DoD 5220.22 M* pada partisi :F dan :G dilakukan dengan menggunakan 2 *tools* penghapusan data, yaitu *Eraser Tool* dan *Active@ Kill Disk* yang telah disiapkan sebelumnya. Proses penghapusan data dengan menerapkan metode *DoD 5220.22 M* menggunakan *Eraser Tool* dilakukan pada partisi: F. Pengamatan yang dilakukan pada proses penerapan Metode *DoD 5220.22 M* dengan menggunakan *Eraser Tool* memerlukan waktu 8 menit 24 detik. Dalam proses ini, *Eraser Tool* menggunakan CPU sebesar 4,5% dan rata-rata penggunaan memori sebesar 2,8%. Kemudian proses penghapusan data dengan menerapkan metode *DoD 5220.22 M* menggunakan *Active@ Kill Disk* dilakukan pada *disk* 3. Pengamatan dilakukan pada saat proses berlangsung dengan menggunakan *Task Manager*. Hasil yang didapatkan pada saat pengamatan yaitu waktu yang dibutuhkan dalam proses penghapusan tergolong cukup lama yaitu 1 jam 20 menit 11 detik. Proses ini menggunakan rata-rata CPU sebesar 2,3% dan rata-rata penggunaan memori sebesar 3,2%. Hasil tersebut menunjukkan perbedaan terhadapat proses penerapan yang dilakukan dengan Metode *DoD 5220.22 M* dan menggunakan *Eraser Tool.* Perbedaan yang sangat signifikan terletak pada waktu yang diperlukan dalam proses penghapusan.

Proses implementasi yang ketiga yaitu proses penghapusan data dengan penerapan metode *British HMG IS5 E* dengan menggunakan *Eraser Tool Active@ Kill Disk.* Hasil dari pengamatan yang dilakukan saat proses penghapusan menggunakan *Eraser Tool*, waktu yang diperlukan dalam proses penghapusan yaitu 8 menit 31 detik. Adapun penggunaan rata-rata CPU sebesar 4,1% dan penggunaan rata-rata memori sebesar 2,9%. Kemudian proses penghapusan data dengan menerapakan metode *British HMG IS5 E* dan menggunakan *Active@ Kill Disk Tool*, Pengamatan dilakukan pada saat proses berlangsung dengan menggunakan *Task Manager.* Hasil yang didapatkan pada saat pengamatan yaitu waktu yang dibutuhkan dalam proses penghapusan tergolong cukup lama yaitu 1 jam 15 menit 48 detik. Proses ini menggunakan rata-rata CPU sebesar 2,3% dan rata-rata penggunaan memori sebesar 3,4%.

3.2 Proses Analisis

Berdasarkan pada perancangan sistem yang terdapat pada Gambar 3, proses analisa pertama yang dilakukan yaitu uji kinerja dari metode penghapusan berdasarkan *tools* yang digunakan.

Hasil pengamatan yang dilakukan pada saat proses penerapan metode penghapusan, menghasilkan data dari tiap proses. Data yang didapatkan tersebut kemudian dilakukan uji *performance* metode penghapusan data yang dapat dilihat pada Tabel 4 menunjukkan perbedaan performa dari masing-masing metode.

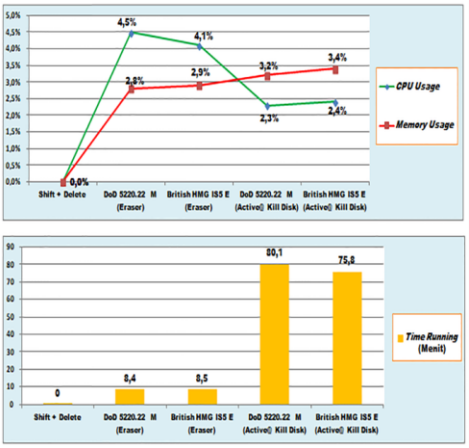
Tabel 4. Perbedaan performa dari masing-masing metode

Metode	*Tools (Type)*	*CPU Usage*	*Running Time*	*Memory Usage*
Shift + Delete	*SO Deletion (*dokumen*)*	-	3 detik	-
DoD 5220.22 M	*Eraser (File)*	4,5%	8 menit 24 detik	2,8%
British HMG IS5 (Enhanced)	*Eraser (File)*	4,1%	8 menit 31 detik	2,9%
DoD 5220.22 M	*Active@ Kill Disk (Disk)*	2,3%	1 jam 20 menit 11 detik	3,2%
British HMG IS5 (Enhanced)	*Active@ Kill Disk (Disk)*	2,4%	1 jam 15 menit 48 detik	3,4%

Berdasarkan Tabel 4 menunjukkan bahwa proses penghapusan dengan menerapkan metode penghapusan perintah sistem operasi *(shift+delete)* pada HDD yang berisi data uji tergolong sangat cepat yaitu hanya membutuhkan waktu 3 detik dalam prosesnya. Proses tersebut tidak dapat dilakukan pengamatan rata-rata penggunaan CPU dan memori dikarenakan proses yang sangat cepat.

Sedangkan penerapan metode *Dod 5220.22 M* dan *British HMG IS5 E* menunjukkan bahwa *performance* dari kedua metode tersebut tergantung pada *tools* yang digunakan. Ketika proses penghapusan dengan metode *Dod 5220.22 M* dan menggunakan *tools Eraser*, *performance* yang didapatkan tidak jauh berbeda dengan penerapan metode *British HMG IS5 E* dengan menggunakan *tools* yang sama.

Adapun penerapan metode *Dod 5220.22 M* dan *British HMG IS5 E* dengan menggunakan tools *Active@ Kill Disk* memakan waktu yang cukup lama dibandingkan dengan *tools Eraser*. Akan tetapi penerapan dari kedua metode penghapusan menunjukkan bahwa *performace* dari kedua metode tersebut tidak jauh berbeda. Untuk lebih jelasnya, perbandingan *performance* dari penerapan metode berdasarkan *tools* yang digunakan dapat dilihat pada Gambar 3.



Gambar 3. Perbandingan *performance* dari penerapan metode berdasarkan *tools*

Berdasarkan Gambar 3 menunjukkan bahwa kinerja *(performance)* dari setiap metode penghapusan sangat dipengaruhi oleh *tools* yang digunakan. *Performance*

dari kedua metode tersebut tidak memberikan perbedaan yang signifikan ketika diterapkan menggunakan salah satu *tools.*

Proses analisa yang kedua yaitu uji forensik, proses uji forensik dilakukan menggunakan tahapan standar NIJ yang telah dibahas pada bab sebelumnya, yaitu hanya menggunakan 3 tahapan forensik dari 5 tahapan yang ada pada standar NIJ.

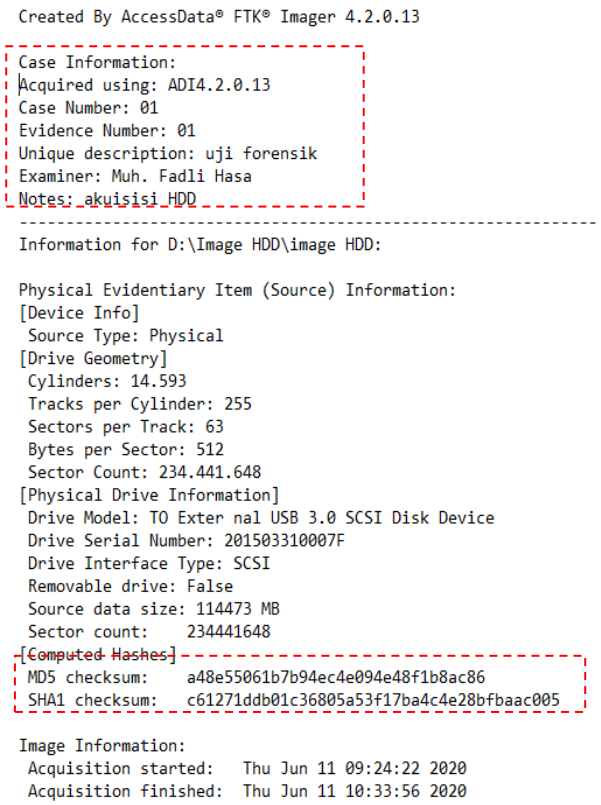
Tahap pertama dari 3 tahapan forensik yaitu tahap *collection.* Proses yang dilakukan pada tahapan ini yaitu membuat salinan *(cloning)* secara utuh menjadi *file image* dari objek penelitian yang digunakan yaitu HDD. Proses *image* ini menggunakan *tools FTK Imager*. Proses *image* dilakukan pada HDD secara utuh dimana HDD tersebut telah dilakukan penerapan metode penghapusan yang terbagi menjadi 4 sesi penghapusan. Jumlah proses pembuatan *image* yang dilakukan hanya 1 proses yaitu 1 HDD secara utuh.

Proses *image* dimulai dengan mencolokkan HDD ke laptop dan kemudian pada *tool FTK Imager* akan mengidentifikasi perangkat HDD sebagai *Phisical Drive 1*. Tahapan selanjutnya memilih opsi *physical drive* untuk proses *full* akuisisi, setelah itu memiliih *source drive* HDD dengan nama *"TO External USB 3.0 SCSI Disk Device"* dan memilih tujuan *drive* penyimpanan. Ekstensi yang digunakan adalah RAW (dd), fungsi "*Verify image after created*" untuk mengecek ulang nilai *hash* yang dihasilkan oleh aplikasi *FTK Imager*. Setelah proses persiapan selesai, tahap selanjutnya yaitu menjalankan proses *image* dengan cara mengklik *button start* pada *form* terakhir pada proses persiapan. Proses pembuatan *image* HDD ini memerlukan waktu 1 jam 9 menit 35 detik.

Hasil yang didapakan pada proses *collection* ini berupa *file image* yang berekstensi RAW dengan ukuran 111 Gb sesuai dengan ukuran asli objek penelitian yaitu HDD. Proses akuisisi ini juga menghasilkan nilai *hash* dari *file image*, nilai *hash* yang didapat yaitu *Message-Direst Algorithm* 5 (MD5) dan *Secure Hash Algorithm* 1 (SHA1) yang digunakan untuk memverifikasi keaslian *file* duplikasi *image*. Nilai *hash* mempunyai nilai unik dan berbeda-beda antara *file*, informasi yang didapat saat akusisi berupa nomor studi kasus forensik, nomor bukti digital, nama *examiner* yang bertanggung jawab akusisi bukti digital dan keterangan kapasitas dan *serial number* media penyimpanan yang diakuisisi, berikut Gambar 4 hasil *log* dan nilai *hash* akuisisi pada HDD menggunakan *tool FTK Imager*.

Gambar 4 menunjukkan hasil dari proses pembuatan *image* HDD yang memuat seluruh informasi tentang *file image* yang telah selesai diproses. Data tersebut dijadikan sebagai validasi dari proses *collection* yang menunjukkan integritas dari barang bukit.

Tahap uji forensik selanjutnya yaitu tahap *examination* yang merupakan tahap lanjutan setelah proses akuisisi. Pada tahap ini dilakukan proses pencarian bukti digital pada HDD yang telah dilakukan proses penghapusan dengan cara mengekstrak *file image* yang telah didapatkan pada saat proses akuisisi. Perangkat lunak yang digunakan pada proses ekstraksi ini yaitu *Autopsy* dan *Recover My File.* Proses eksaminasi dilakukan dengan cara *logical extraction* yaitu tidak langsung terhubung dengan perangkat fisik melainkan menggunakan hasil salinan *image* yang telah disiapkan pada proses akuisisi.

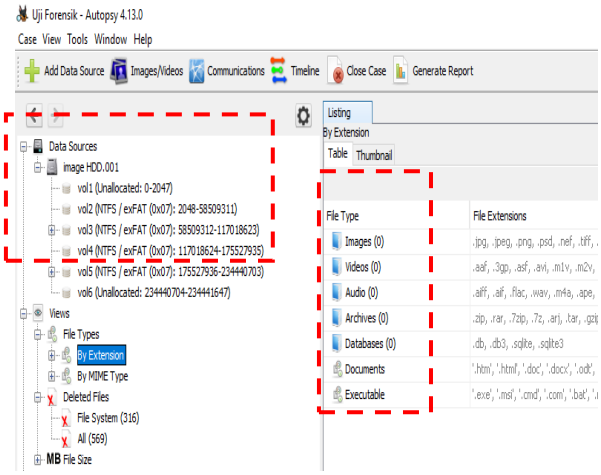


Gambar 4. Hasil *log* dan nilai *hash* akuisisi pada HDD menggunakan *tool FTK Imager*

Proses *examination* yang pertama yaitu proses analisa image menggunakan *Autopsy* ini memerlukan waktu sekitar 5 sampai 6 jam, waktu tersebut tergantung pada besar *file image* yang dianalisa serta spesifikasi perangkat komputer yang digunakan. Setelah proses analisa *image* selesai, *tool autopsy* akan menunjukkan isi dari HDD yang telah dilakukan proses penghapusan. Pada proses ini hasil yang didapatkan hanya berupa partisi HDD yang berjumlah 4 partisi, *file directory*, serta *file slack.* Proses eksaminasi menggunakan *Autopsy* ini sama sekali tidak mendapatkan file yang telah dihapus pada proses sebelumnya. Hasil dari proses analisa *image* menggunakan *tool autopsy* dapat dilihat pada Gambar 5.

Berdasarkan pada Gambar 5 tersebut menunjukkan bahwa proses eksaminasi menggunakan *tool Autopsy* ditemukan berupa partisi yang berjumlah 4 partisi dan *file* yang berjumlah 252 file, namun file tersebut tidak dapat diidentifikasi. Hal ini menunjukkan bahwa penerapan metode penghapusan berhasil dan tidak dapat

dilakukan proses forensic menggunakan *tool Autopsy*. Hasil proses eksaminasi *file image* menggunakan *tool Autopsy* dapat dilihat pada Tabel 5.



Gambar 5. Hasil proses analisa *image* menggunakan *tool Autopsy*

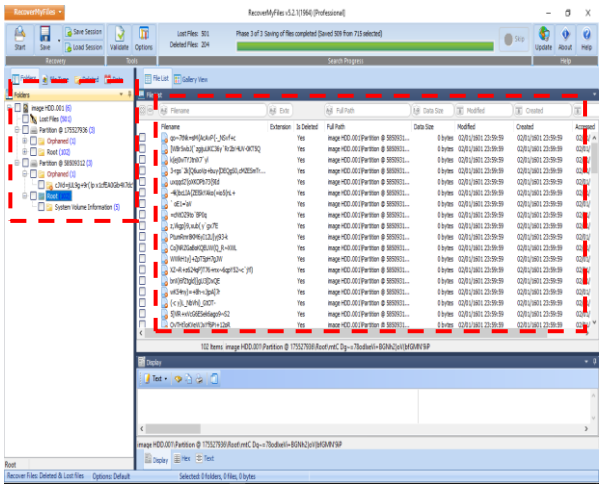
Tabel 5. Hasil eksaminasi *file image* menggunakan *tool Autopsy*

Partisi	Jumlah File	Letak file	Keterangan
Vol 2(NTFS/exFAT)	252	*Carved File*	Tidak teridentifikasi
Vol 3(NTFS/exFAT)	0	-	-
Vol 4(NTFS/exFAT)	1	*Carved File*	Tidak teridentifikasi
Vol 5(NTFS/exFAT)	0	-	-

Berdasarkan Tabel 5 diketahui bahwa *file* yang berhasil ditemukan yaitu terletak pada partisi Vol 2(NTFS/exFAT) dan partisi Vol 4(NTFS/exFAT) dan berada di *folder carved file*. *File* yang ditemukan tersebut tidak dapat diidentifikasi.

Proses *examination* yang kedua yaitu proses analisa image menggunakan *tool Recover My File*. Proses eksaminasi *image* tersebut memerlukan sekitar 3 sampai 4 jam, hal ini tergantung pada kapasitas media penyimpanan yang dilakukan proses eksaminasi serta juga tergantung pada kecepatan perangkat komputer yang digunakan untuk proses ekstraksi. Setelah proses eksaminasi selesai, maka *tool* tersebut akan memunculkan berbagai informasi mengenai HDD yang digunakan dalam penelitian. Informasi yang didapatkan yaitu berupa partisi HDD yang berjumlah 4 serta *file slack*. Proses pencarian file yang dilakukan tidak dapat menemukan *file* pada HDD yang telah dilakukan proses penghapusan. Hasil dari proses eksaminasi *file image* dapat dilihat pada Gambar 6.

Berdasarkan hasil dari proses eksaminasi *file image* menggunakan *tool Revover My File* yang terdapat pada Gambar 6 ditemukan partisi HDD berjumlah 2 partisi. *File* yang ditemukan berjumlah 102 *file* yang terletak pada sub direktori root pada masing-masing partisi, akan tetapi jenis *file* tersebut tidak dapat diidentifikasi. Hasil dari proses eksaminasi *file image* menggunakan *tool Revover My File* dapat dilihat pada Tabel 6.



Gambar 6. Hasil proses eksaminasi *file image* menggunakan *tool Revover My File*

Tabel 6. Hasil proses eksaminasi *file image* menggunakan *tool Revover My File*

Partisi	Jumlah File	Letak file	Keterangan
@ 175527936	102	*Root*	Tidak teridentifikasi
@ 58509312	102	*Root*	Tidak teridentifikasi

Tabel 6 menunjukkan bahwa *file* yang berhasil ditemukan yaitu terletak pada partisi @ 175527936 dan partisi @ 58509312. Namun *file* yang ditemukan tersebut tidak dapat diidentifikasi.

Tahap selanjutnya dalam proses uji forensik yaitu *analysis*. Pada tahapan ini, proses yang dilakukan yaitu pencarian secara detail artefak yang didapatkan dari proses eksaminasi dan proses ekstraksi. Hasil analisa yang didapatkan dapat dilihat pada Tabel 7.

Tabel 7. Hasil proses *analysis*

Tool	Partisi	Jumlah File	Letak file	Keterangan
Autopsy	Vol 2 (NTFS/exFAT)	252	*Carved File*	Tidak teridentifikasi
	Vol 3 (NTFS/exFAT)	0	-	-
	Vol 4 (NTFS/exFAT)	1	*Carved File*	Tidak teridentifikasi
	Vol 5 (NTFS/exFAT)	0	-	-
Recover My File	@ 175527936	102	*Root*	Tidak teridentifikasi
	@ 58509312	102	*Root*	Tidak teridentifikasi

Berdasarkan Tabel 7 diketahui bahwa proses eksaminasi menggunakan *tool Autopsy* ditemukan berupa partisi yang berjumlah 4 partisi dan file yang berjumlah 253 file, namun file tersebut tidak dapat diidentifikasi. Hal ini menunjukkan bahwa penerapan metode penghapusan berhasil dan tidak dapat dilakukan proses forensic menggunakan *tool Autopsy*.

Sedangkan proses eksaminasi menggunakan *tool Recover My File* ditemukan partisi HDD berjumlah 2 partisi. *File* yang ditemukan berjumlah 102 *file* yang

terletak pada sub direktori root pada masing-masing partisi, akan tetapi jenis *file* yang ditemukan tersebut juga tidak dapat diidentifikasi. Hal ini menunjukkan bahwa penerapan metode penghapusan berhasil dan tidak dapat dilakukan proses forensik menggunakan *tool Recover My File*

Setelah uji forensik, tahap pengujian yang ketiga yaitu tahap uji *recovery*. Tahap ini berbeda dengan dengan proses eksaminasi yang dilakukan pada proses uji forensik, perbedaannya terletak pada proses ekstraksi yang dilakukan. Pada proses uji forensik, proses ekstraksi dilakukan menggunakan *image file* yang dihasilkan dari proses akuisisi dan tidak melalui HDD secara langsung. Sedangkan pada proses uji *recovery* proses dilakukan dengan menghubungkan HDD secara langsung dan menggunakan *tool recovery* yang telah disiapkan. Proses uji *recovery* dibagi menjadi 3 sesi sesuai dengan jumlah *tools recovery* yang digunakan dan metode penghapusan yang diterapkan

Sesi pertama yang dilakukan yaitu uji *recovery* menggunakan *Mini Tool Power Data Recovery*. Proses ini dilakukan pada masing-masing partisi yang telah dilakukan proses penerapan metode penghapusan. Hasil yang didapatkan pada proses *recovery* menggunakan *Mini Tool Power Data Recovery* dapat dilihat pada Tabel 8.

Tabel 8. Hasil *recovery* menggunakan *Mini Tool Power Data Recovery*

Metode	Tools	Jml. File	Keterangan
Shift + Delete	OS	100	Dapat diakses
British HMG IS5 E	Eraser	0	-
DoD 5220.22 M	Eraser	95	Tidak dapat diakses
DoD 5220.22 M	Active @ Kill Disk	0	-
British HMG IS5 E	Active @ Kill Disk	0	-

Berdasarkan Tabel 8 menunjukkan bahwa proses *recovery* menggunakan *Mini Tool Power Data Recovery* berhasil memulihkan data pada partisi HDD yang diterapkan metode penghapusan *Shift + Delete*, data dapat dipulihkan secara utuh sesuai dengan kondisi file sebelum dihapus serta file yang didapat masih dapat di akses.

Sedangkan proses *recovery* pada partisi HDD yang diterapkan metode penghapusan *British HMG IS5 E* dan *DoD 5220.22 M* serta menggunakan *Active @ Kill Disk* dan *Eraser*. Hasil yang didapatkan yaitu file yang berhasil di *recovery* hanya pada partisi HDD yang dihapus dengan metode *DoD 5220.22 M* menggunakan *tool Eraser* dengan jumlah 95 file, namun file yang berhasil didapatkan tersebut tidak dapat diakses.

Sesi kedua yang dilakukan yaitu uji *recovery* menggunakan Proses *recovery* menggunakan *EaseUS Data Recovery*. Proses ini dilakukan pada masing-masing partisi yang berjumlah 5 partisi dan telah dilakukan proses penerapan metode penghapusan. Hasil yang didapatkan pada proses *recovery* menggunakan *EaseUS Data Recovery* dapat dilihat pada Tabel 9.

Tabel 9. Hasil proses *recovery* menggunakan *EaseUS Data Recovery*

Metode	*Tools*	Jml. File	Keterangan
Shift + Delete	*OS*	100	Teridentifikasi
British HMG IS5 E	*Eraser*	116	Tidak Teridentifikasi
DoD 5220.22 M	*Eraser*	105	Tidak Teridentifikasi
DoD 5220.22 M	*Active @ Kill Disk*	0	Tidak Teridentifikasi
British HMG IS5 E	*Active @ Kill Disk*	0	Tidak Teridentifikasi

Berdasarkan Tabel 9 menunjukkan bahwa proses *recovery* menggunakan *EaseUS Data Recovery* berhasil memulihkan data pada partisi HDD yang diterapkan metode penghapusan *Shift + Delete*, data dapat dipulihkan secara utuh sesuai dengan kondisi file sebelum dihapus. File yang didapat berjumlah 100 file dan masih dapat di akses.

Sedangkan proses *recovery* pada partisi HDD yang diterapkan metode penghapusan *British HMG IS5 E* dan *DoD 5220.22 M* serta menggunakan *Active @ Kill Disk* dan *Eraser*, hasil yang didapatkan yaitu hanya berupa file metadata yang tidak dapat di akses sama sekali serta tidak teridentifikasi.

Sesi pertama yang dilakukan yaitu uji *recovery* menggunakan *Recuva*. Proses *recovery* menggunakan *Recuva* ini dilakukan pada masing-masing partisi yang berjumlah 5 partisi dan telah dilakukan proses penerapan metode penghapusan. Hasil yang didapatkan pada proses *recovery* menggunakan *Recuva* dapat dilihat pada Tabel 10.

Tabel 10. Hasil proses *recovery* menggunakan *Recuva*

Metode	*Tools*	Jumlah FIle	Keterangan
Shift + Delete	*OS*	100	Teridentifikasi
British HMG IS5 E	*Eraser*	127	Tidak Teridentifikasi
DoD 5220.22 M	*Eraser*	158	Tidak Teridentifikasi
DoD 5220.22 M	*Active @ Kill Disk*	-	*Scan* Gagal
British HMG IS5 E	*Active @ Kill Disk*	-	*Scan* Gagal

Berdasarkan Tabel 10 menunjukkan bahwa hasil dari *recovery* menggunakan *Recuva* berhasil memulihkan data pada partisi HDD yang diterapkan metode penghapusan *Shift + Delete*, data dapat dipulihkan secara utuh sesuai dengan kondisi file sebelum dihapus. File yang didapat berjumlah 100 file dan masih dapat di akses.

Proses *recovery* pada partisi HDD yang diterapkan metode penghapusan *British HMG IS5 E* dan *DoD 5220.22 M* dan menggunakan *tool Eraser*, hasil yang

didapatkan yaitu hanya berupa file metadata yang tidak dapat di akses sama sekali serta tidak teridentifikasi.

Sedangkan proses *recovery* pada partisi HDD yang diterapkan metode penghapusan *British HMG IS5 E* dan *DoD 5220.22 M* serta menggunakan *tool Active @ Kill Disk*, hasil yang didapatkan berdasarkan pengamatan yang dilakukan yaitu *tool recuva* tidak dapat melakukan proses *scan* pada 2 partisi HDD tersebut.

4. Kesimpulan

Berdasarkan hasil pengamatan yang dilakukan pada saat proses penerapan metode anti forensik *(data sanitation)* menggunakan metode *British HMG IS5 E* dan *DoD 5220.22 M* secara signifikan menunjukkan bahwa kinerja *(performance)* dari kedua metode tersebut sangat dipengaruhi oleh *tools* anti forensik yang digunakan. kinerja *(performance)* dari kedua metode tersebut tidak memberikan perbedaan yang signifikan ketika diterapkan menggunakan salah satu *tools.*

Berdasarkan dari hasil analisa yang dilakukan, metode penghapusan *file* yang biasa digunakan oleh *user* yaitu dengan cara *shift + delete* dapat dinyatakan tidak aman, terbukti dengan hasil uji *recovery* yang dilakukan menunjukkan bahwa *file* yang telah dihapus dapat dipulihkan 100% serta dapat diakses kembali menggunakan 3 *tool recovery*. Sedangkan penerapan metode anti forensik *(data sanitization)* menggunakan metode *British HMG IS5 E* dan *DoD 5220.22 M* dapat diimplementasikan pada proses penghapusan *file* yang berada di dalam *hardisk drive* secara aman. Hal tersebut berdasarkan hasil ekstraksi dari uji forensik menggunakan *tool Autopsy* ditemukan *file* pada partisi :F dengan jumlah 252 *file* dan pada pertisi :I dengan jumlah 1 *file*. Sedangkan hasil ekstraksi dari uji forensik menggunakan *tool Recover My File* berhasil menemukan *file* dengan jumlah 102 *file* pada partisi yang berbeda, namun dari semua hasil temuan *file* pada proses uji forensik tersebut tidak dapat diakses.

Hasil uji *recovery* yang dilakukan menunjukkan bahwa metode yang paling aman dalam melakukan penghapusan data yaitu metode *British HMG IS5 E* menggunakan *tool Active @ Kill Disk*, terbukti dari semua hasil proses *recovery* menggunakan tiga *tools* tidak menemukan *file* apapun.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Program Studi Magister Teknik Informatika Universitas Ahmad Dahlan yang telah mengizinkan untuk menggunakan fasilitas sebagai penunjang dalam penelitian ini.

Daftar Rujukan

[1] Hermansa, R. Umar, and A. Yudhana, "Pangamanan Pesan Menggunakan Kriptografi Caesar Cipher dan Steganografi EOF pada Citra," *J. Sains Komput. Inform.*, vol. 4, pp. 157–169, 2020.

[2] Jessica, "Sistem informasi manajemen," *Sist. Inf. Manaj.*, p. 109, 2018.

[3] S. M. Diesburg and A. I. A. Wang, "A survey of confidential data storage and deletion methods," *ACM Comput. Surv.*, vol. 43, no. 1, 2010.

[4] Y. W, I. Riadi, and A. Yudhana, "Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing (PENTEST)," *Annu. Res. Semin.*, vol. 2, no. 1, pp. 300–304, 2016.

[5] R. Indonesia, "Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik," *UU No. 19 tahun 2016*, no. 1, pp. 1–31, 2016.

[6] M. F. Hasa, A. Yudhana, and A. Fadlil, "Analisis Bukti Digital Pada Storage Secure Digital Card Menggunakan Metode Static Forensic," *J. Mob. Forensics*, vol. 1, no. 2, pp. 22–30, 2019.

[7] E. Wahyudi, "Definisi dan Teknik Anti forensik," 2016.

[8] Fathoni Mahardika; Yulian Sani, "Anti Forensik Tools Dalam Meningkatkan Keamanan Data," pp. 37–39, 2012.

[9] A. Al Anhar, G. B. Satrya, and F. A. Yulianto, "Analisis Perbandingan Keamanan Teknik Penghapusan Data pada Hardisk dengan Metode DoD 5220 . 22 dan GutmannzComparative Analysis of Data Deletion Technique Security on Hard disk with DoD 5220 . 22 and Gutmann Method," vol. 1, no. 1, pp. 607–613, 2014.

[10] G. Hughes and T. Coughlin, "Tutorial on Disk Drive Data Sanitization Data Loss is Rampant," *Nist Spec. Publ.*, vol. Volume|, no. September, pp. 1–15, 2006.

[11] S. M. Beloussov, "(12) United States Patent Sty for Partial Erasing Run Wipe Procedure as," vol. 1, no. 12, 2010.

[12] H. R. Khalifa, F. A. Yulianto, and E. M. Jadied, "Implementasi Teknik Penghapusan Data Dengan Metode DoD 5220 . 22M Pada Sistem Operasi Android Implementation Of Data Deletion Using DoD 5220 . 22M method On Android Operating System," vol. 3, no. 1, pp. 897–913, 2016.

[13] P. F. Bennison and P. J. Lasher, "Data security issues relating to end of life equipment," *IEEE Int. Symp. Electron. Environ.*, pp. 317–320, 2004.

[14] T. Martin and A. Jones, "An evaluation of data erasing tools," *Proc. 9th Aust. Digit. Forensics Conf.*, no. December, pp. 84–92, 2011.

[15] F. P. Document, "Force Policy Document," pp. 1–11, 2012.