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

Habib Reza Khalifa[1], Fazmah Arif Yulianto, ST.,MT.[2], Erwid M.Jadied, ST., MT.[3]

[1,2,3] Prodi S1 Teknik Informatika, Fakultas Informatika, Universitas Telkom
Jl. Telekomunikasi, Dayeuh Kolot, Bandung 40257 Telp. (62-22) 7564108 ext. 2333

habibreza@students.telkomuniversity.ac.id[1] , fazmaharif@telkomuniversity.ac.id[2], jadied@telkomuniversity.ac.id[3]

ABSTRAK

Keamanan suatu data baik itu milik perorangann ataupun data penting perusahaan perlu dijaga agar tidak sampai jatuh ke tangan yang salah. Dalam menjaga keamanan tersebut, salah satu caranya yaitu dengan melakukan penghapusan data penting tersebut dari media penyimpanan. Namun diperlukan cara penghapusan yang benar-benar aman dalam melakukan penghapusan tersebut, agar data yang telah dihapus tidak dapat dipulihkan kembali. Dari hal tersebut, diperlukan sebuah metode yang dapat membuat penghapusan data tersebut benar-benar aman dan tidak mudah untuk dipulihkan dengan berbagai *tools recovery*.

Dalam pengujian pada tugas akhir ini akan diambil beberapa aplikasi sampel yang telah dipilih sebelumnya untuk dianalisa kekurangannya untuk kemudian diperbaiki beberapa kekurangannya oleh aplikasi yang dibuat, baru kemudian dibandingkan dibandingkan hasil keamanan data antara aplikasi yang dibuat dengan aplikasi sampel. Dari hasil analisa kekurangan aplikasi sampel didapatkan bahwa aplikasi sampel yang diambil saat melakukan penghapusan tidak menggubah ataupun menghapus nama file dari data yang dihapus, untuk itu pada pembuatan aplikasi selain ditujukan untuk melakukan penghapusan data juga ditambahkan fungsi untuk melakukan pengubahan nama file. Aplikasi yang dibuat menggunakan metode DoD 5220.22-M dalam implementasinya dan memiliki beberapa kelebihan dibandingkan dengan aplikasi andro shredder dan juga remo file eraser. Dari segi keamanan data, aplikasi yang dibuat memiliki kelebihan yaitu aplikasi ini mengubah nama file asli kedalam bentuk acak, sehingga nama file asli dari data yang dihapus tidak dapat diketahui. Kemudian dari segi efisiensi waktu, aplikasi yang dibuat juga memiliki waktu penghapusan yang cukup cepat, sehingga cukup baik jika digunakan untuk melakukan penghapusan data. Namun aplikasi yang dibuat belum mampu menghapus file dengan sempurna dan masih ada file yang dapat dipulihkan kembali.
Kata kunci : A*nti-forensics, DoD 5220.22M, SDcard, Recovery*

ABSTRACT

Security of a data that belongs to an individual or company data should be maintained in order not to fall into the wrong hands. In maintaining the security, one way is by doing the deletion of critical data from any storage media. However need a deletion techniques of a truly safe to delete the data, so that deleted data can not be recovered. From this, we need a method that can make deletion of such data is absolutely safe and not easy to be restored with various recovery tools.

In the test will take several sample applications that have been previously to analyze the weakness and then repaired some of its weakness by the application is made, and then compared the findings of safety data between applications made with a sample application. From the analysis of the sample application deficiencies found that application samples taken when doing deletion does not compose or delete the file name of the deleted data, for it is the creation

of applications in addition is intended to perform data deletion also added functionality to make changes to the file name. Applications created using DoD 5220.22-M method in its implementation and has several advantages compared with Andro Shredder and also Remo File Eraser. In terms of data security, application is made has the advantages of this application to modify the original file name into random shapes, so that the original file name of the deleted data can not be known. Then in terms of time efficiency, the application made also have a fast enough time deletion, so it's quite good if used to perform data deletion. But the application is made has not been able to delete files perfectly and still files can be restored.

Keywords : A*nti-forensics, DoD 5220.22M, SDcard,, Recovery*

1. Latar Belakang

Mobile device forensics atau forensik perangkat mobile merupakan cabang dari forensic digital yang berkaitan dengan pemulihan bukti digital atau data dari suatu perangkat mobile. Di dalam suatu perangkat mobile tentunya ada sebuah sistem operasi yang disematkan didalamnya, adanya sistem operasi dalam perangkat mobile ini seperti Adroid, IOS, Windows phone dan berbagai sistem operasi yang lain tentunya membuat para pengguna akan menyimpan informasi-informasi penting yang mereka miliki kedalam perangkat tersebut memanfaatkan fitur dari sistem operasi tersebut. Dengan banyaknya informasi penting yang ada dalam sebuah perangkat mobile, tentunya akan memunculkan resiko yang menjadikan data-data atau informasi yang ada dalam perangkat tersebut akan dimiliki oleh orang yang tidak berhak atas data tersebut.

Sistem operasi Android pada kuartal ke tiga pada tahun 2014 menjadi peringkat pertama pada pemasaran global dan menjadi sistem operasi mobile yang paling banyak digunakan oleh para pengguna perangkat mobile, pada pemasaran global android menjadi peringkat pertama dengan total pengiriman perangkat dengan sistem operasi android yaitu mencapati 84,4%[3]. Hal tersebut menjadi salah satu faktor para penjahat lebih memilih perangkat android ini dalam aksi kejahatan mereka seperti mencuri data-data penting dalam perangkat tersebut.

Perangkat *mobile* merupakan suatu benda yang mudah untuk berpindah tangan dari pemilik satu ke pemilik lainnya. Di zaman teknologi maju seperti sekarang ini jual beli perangkat *mobile* banyak terjadi di kalangan masyarakat, baik itu perangkat baru maupun bekas. Untuk itu bagi mereka yang mempunyai informasi atau data penting dalam perangkat *mobile* tersebut bukan tidak mungkin informasi tersebut dapat diambil oleh pengguna baru dari perangkat tersebut. Kebanyakan orang beranggapan bahwa data yang telah dihapus dalam perangkat tersebut adalah sudah aman dan tidak akan dapat diambil oleh orang lain. Padahal sebenarnya penghapusan secara biasa sangatlah mudah untuk dipulihkan kembali karena tingkat keamananya rendah.

Dalam suatu aplikasi *mobile* ada terdapat berbagai aplikasi penghapusan data pada media penyimpanan mobile. Namun masih banyak aplikasi yang tidak sempurna dalam penghapusan data tersebut, dan masih dapat dipulihkan menggunakan sebuah aplikasi *recovery.* Untuk itu perlu adanya pengembangan dari aplikasi tersebut agar lebih efisien dan sempurna dalam penghapusan data sehingga data-data yang telah kita hapus sulit dipulihkan bahkan tidak bisa dipulihkan secara utuh oleh perangkat-perangkat *recovery.* Dengan semakin efisien dan semakin aman perangkat penghapus data yang kita miliki tentunya akan menambah keamanan kita dalam perangkat *mobile* tersebut sehingga data-data penting yang kita miliki pun tidak akan bisa diambil alih oleh orang lain yang tidak bertanggung jawab.

Dengan demikian perlu adanya pengembangan dari suatu aplikasi penghapusan data tersebut agar data yang telah kita hapus tidak dapat dipulihkan secara sempurna oleh aplikasi *recovery*.

2. Dasar Teori

2.1 *Data Sanitization*

Data Sanitization yaitu suatu proses dengan sengaja, permanen, dan ireversibel untuk menghapus atau menghancurkan data yang tersimpan pada media penyimpanan agar tidak dapat dipulihkan kembali. Sebuah perangkat yang telah disanitasi tidak akan memiliki data residual yang berfungsi dan bahkan alat-alat forensic canggih pun seharusnya tidak pernah dapat memulihkan data yang telah disanitasi tersebut [3][4]. Sanitasi data ini dilakukan untuk melindungi data-data rahasia yang tidak boleh diketahui oleh orang lain. Misalkan sebuah perangkat *mobile* yang akan berpindah tangan, dengan dilakukannya sanitasi data ini, maka data-data kita yang sebelumnya ada di perangkat tersebut tentunya akan aman karena tidak akan dapat dipulihkan lagi [9].

2.2 *Department Of Defense (DoD) Media Sanitization Guidelines 5220.22M*

DoD 5220.22M menetapkan proses yang menimpa data pada harddisk dengan pola acak dengan 0 dan 1. Dalam DoD 5220.22M ini diperlukan tiga fase *overwriting* jadi akan terlihat lebih aman daripada proses penghapusan biasa, seperti yang dilakukan dalam Departement of Defence [7]. Melakukan penghapusan data menggunakan metode DoD 5220.22M ini akan mencegah aplikasi *recovery* file untuk dapat memulihkan kembali data yang telah dihapus. Ada 3 jenis metode DoD 5220.22M ini, yaitu DoD 5220.22M C, DoD 5220.22M D, dan DoD 5220.22M E atau yang sering disebut metode DoD standar. Dalam penelitian ini, metode yang digunakan yaitu metode DoD standar atau DoD 5220.22M E. Dalam implementasinya, dari ketiga metode DoD 5220.22M ini menggunakan metode yang berbeda dalam melakukan penghapusan datanya.

Metode DoD 5220.22M C menggunakan 1 fase dalam melakukan penghapusan yaitu [11][12].

Fase 1 : Menimpa file dengan byte 0.

Metode DoD 5220.22M D menggunakan 4 fase dalam melakukan penghapusan yaitu:

Fase 1 : Menimpa dengan byte 0
Fase 2 : Menimpa dengan byte 1
Fase 3 : Menimpa dengan byte random
Fase 4 : Melakukan verifikasi pada fase terkahir.

Sedangkan metode DoD 5220.22M E menggunakan 3 fase dalam melakukan penghapusannya, yaitu :

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

DoD 5220.22M ini merupkan salah satu metode terbaik dalam melakukan penghapusan data. Selain cukup aman, waktu yang dibutuhkan dalam penghapusan data pun tidak terlalu lama jadi akan lebih efisien jika digunakan untuk melakukan suatu penghapusan data, terutama pada aplikasi mobile.

3. Pembahasan

3.1 Alur Pengerjaan

3.1.1 Ambil Sample Aplikasi Android

Dalam pengambilan sample aplikasi yang akan digunakan dalam pengujian ini, penulis memilih beberapa aplikasi yang ada di *playstore*. Pemilihan aplikasi dilakukan berdasarkan metode aplikasi yang digunakan untuk menghapus file, berdasarkan rating dan kepopuleran aplikasi di *playstore*, serta berdasarkan banyaknya unduhan di tiap aplikasi tersebut. Setelah dilakukan survey tersebut, diambil 3 aplikasi *file shredder* yang sesuai dengan kriteria tersebut, yaitu :

1. Andro Shredder (rating 4,0 dan 50 ribu unduhan)
2. Remo File Eraser (rating 3,6 dan 10 ribu unduhan)
3. Protect Star iShredder Enterprise Edition (rating 4,4 dan 500 unduhan)

3.1.2 Pengujian Keamanan Data Aplikasi Sampel

Di pengujian ini, kemudian akan dilakukan pengujian penghapusan file menggunakan aplikasi yang telah dipilih tadi. Dalam melakukan pengujiannya, akan diberikan beberapa file untuk kemudian dihapus menggunakan aplikasi penghapusan tersebut. Hal yang akan diamati dalam pengujian ini yaitu dari segi keamanan penghapusannya. Seperti ada tidaknya nama file dan ukuran file dan juga jumlah file yang dapat di pulihkan, semakin sedikit file yang bisa dipulihkan, maka semakin bagus aplikasi tersebut. Untuk melakukan pengujian keamanan data, digunakan 3 buah perangkat lunak untuk pemulihan data yaitu

1. Recuva
2. FTK Imager
3. Easeus Data Recovery

Aplikasi pemulihan data dipilih berdasarkan kepopuleran aplikasi tersebut, serta fungsionalitas aplikasi tersebut yang mampu memulihkan data yang telah terhapus.

3.1.3 Pengujian Performansi Aplikasi Sampel

Setelah dilakukan pengujian keamanan data aplikasi sampel, dilakukan pengujian dari segi performansi penghapusan aplikasi tersebut. Yaitu dengan melakukan pengukuran waktu yang dibutuhkan oleh aplikasi sampel untuk melakukan penghapusan suatu data. Pengukuran dilakukan secara manual menggunakan *stopwatch*, dan dihitung dalam satuan detik.

3.1.4 Analisis Kelemahan dan Kelebihan Aplikasi Sampel

Pada proses analisis kelemahan dan kelebihan ini, kita menggambil data dari waktu yang dibutuhkan aplikasi penghapusan untuk menghapus suatu data, serta jumlah data yang masih bisa dipulihkan oleh aplikasi pemulihan data tersebut. Pada analisis ini, dilihat dari segi waktu yang dibutuhkan untuk menghapus data, jumlah data yang masih bisa dipulihkan baik yang bisa dijalnkan kembali atau tidak, kemudian adanya file slack, keutuhan ukuran file setelah dilakukan pemulihan data, dan masih ada atau tidaknya nama file yang sesungguhnya setelah dilakukan proses pemulihan data.

3.1.5 Develop Aplikasi

Setelah kita mengetahui beberapa kelemahan dari aplikasi-aplikasi penghapusan tersebut, kemudian penulis melakukan pembuatan aplikasi. Aplikasi yang dibuat bisa melihat dari berbagai sumber yang ada di internet. Aplikasi yang dibuat yaitu aplikasi untuk menghapus data yang diharapkan dapat menutupi beberapa kelemahan dari aplikasi yang diambil sebagai sample. Aplikasi dibuat merupakan aplikasi yang berjalan di sistem operasi android.

3.1.6 Pengujian Keamanan Data Aplikasi yang Dibuat

Pengujian kali ini ditujukan untuk mengetahui hasil dari aplikasi yang telah dibuat dari segi keamanannya. Untuk kemudian akan dibandingkan dengan aplikasi yang telah diambil sebagai sampel.

3.1.7 Pengujian Performansi Aplikasi yang Dibuat

Pengujian kali ini ditujukan untuk mengetahui hasil dari aplikasi yang telah dibuat dari segi performansi aplikasi dalam melakukan penghapusan. Yaitu dengan melakukan pengukuran waktu yang dibutuhkan oleh aplikasi yang dibuat untuk melakukan penghapusan data. Kemudian akan dibandingkan dengan aplikasi yang telah diambil sebagai sampel.

3.1.8 Perbandingan Aplikasi yang Dibuat dengan Aplikasi Sampel

Setelah dilakukan pengujian aplikasi yang telah dibuat, maka akan dilakukan perbandingan dengan aplikasi sampel yang diambil. Akan dilakukan perbandingan baik dari segi keamanan data dan juga dari segi efisiensi waktu penghapusan yang dilakukan aplikasi tersebut.

3.2 Skenario Pengujian

3.2.1 Skenario Umum Pengujian

Pada skenario umum pengujian dilakukan untuk mengimplementasikan metode penghapusan yang diajukan pada Tugas Akhir ini dengan hasilnya adalah sebuah aplikasi *mobile* yang dibuat dengan mengimplementasikan metode penghapusan data secara aman yaitu menggunakan metode DoD 5220.22M.

Skenario pertama yang dilakukan yaitu ditujukan untuk mengukur Keamanan data terhadap sebuah aplikasi yang digunakan dalam penghapusan. Apakah aplikasi tersebut sudah melakukan penghapusan secara aman ataukah belum. Untuk itu akan dilakukan proses pemulihan data menggunakan 3 buah software *recovery* yang secara bebas dapat didapatkan dari internet. Hal yang diamati adalah banyaknya file yang dapat dipulihkan dan file yang masih dapat digunakan dari penghapusan sebelumnya, adanya nama file, adanya ukuran file serta ditemukannya *file slack*.

Skenario yang kedua yaitu dengan menguji efisiensi waktu penghapusan menggunakan metode DoD 5220.22M ini. Penghapusan dilakukan pada sebuah *SDCard* pada perangkat *android*. Hal-hal yang diamati yaitu waktu yang dibutuhkan untuk melakukan penghapusan data.

Secara garis besar, skenario pengujian yang akan dilakukan dalam tugas akhir ini yaitu :

1. Menyalin data yang akan diuji kedalam sebuah SD Card berkapasitas 2GB. Data dikopi dari PC ke dalam SD Card menggunakan USB yang dihubungkan langsung antara PC dan Smartphone yang sudah ada SD Card tersebut didalamnya.
2. Setelah data tersebut tersalin kedalam SD Card, maka cabut SD card dari sambungan PC untuk kemudian tersambung dengan smartphone.
3. Melakukan penghapusan data tersebut menggunakan aplikasi pertama, yaitu remo file eraser dan catat waktu penghapusannya.
4. Ukur waktu penghapusan file yang dilakukan oleh aplikasi tersebut.
5. Mengaktifkan USB write blocker pada PC untuk memastikan tidak adanya data tambahan yang dilakukan oleh PC ke dalam SD Card.
6. Memindahkan sambungan SD Card dari smartphone ke PC. Setelah tersambung maka dilakukan proses pemulihan data menggunakan aplikasi *recovery* yang sudah ditentukan tadi, yaitu recuva, FTK imager, dan easeus data recovery wizard. Kemudian analisis hasil *recovery* file tersebut.
7. Ulangi kelima langkah diatas dengan SD Card baru, serta lakukan proses penghapusan menggunakan aplikasi yang berbeda yaitu ulangi menggunakan aplikasi andro shredder, protect star ishredder, dan aplikasi yang kita bangun.

3.2.2 Protokol Pengujian

Dalam protokol pengujian yang akan diujikan dalam Tugas Akhir ini, akan dilakukan pengujian dengan melibatkan beberapa file dengan, ukuran, *filetype,* dan jumlah yang berbeda. Tabel 3.1 adalah tabel tipe file dan juga ekstensi sebagai data set dalam pengujian penghapusan dan pemulihan data :

Tabel 1.1 Tipe File dan Ekstensi yang Diuji

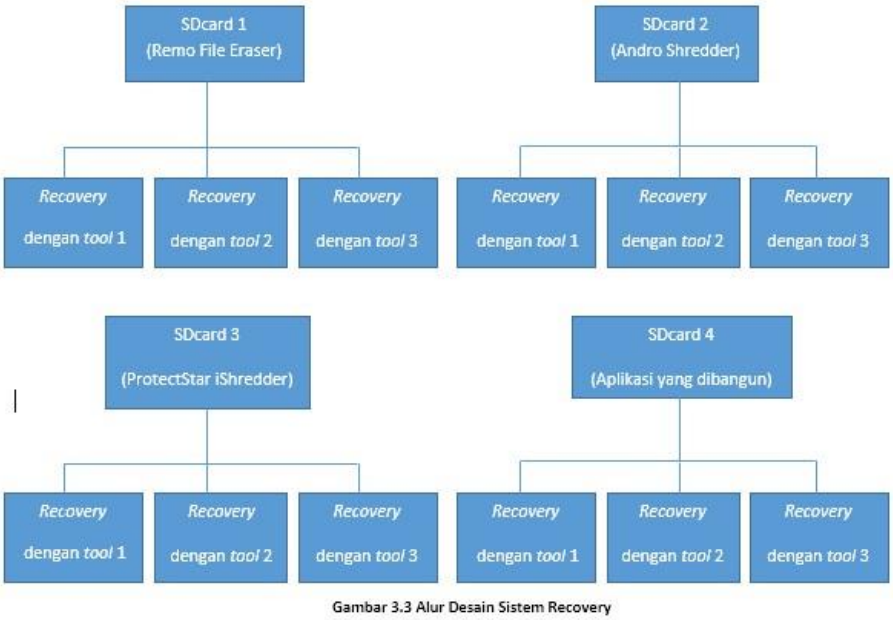
No	Tipe file	Ekstensi	Ukuran file (Total)	Jumlah file
1	Compressed File	.rar	1,4 MB	3
		.zip	73,9 MB	3
2	Text file	.txt	12,6 KB	3
3	Image file	.jpg	3,6 MB	3
		.png	1,6 MB	3
		.bmp	1 MB	3
4	Video file	.mp4	66 MB	1
		.flv	74 MB	1
		.avi	31,7 MB	1
5	Audio File	.mp3	12,6 MB	3
		.wav	13,8 MB	3
6	Document Files	.docx	159 KB	3
		.pptx	7,2 MB	3
		.xlsx	38 KB	3
		.pdf	10,6 MB	3

3.3 Skenario Pengujian Keamanan Data

Pada skenario ini, data yang diuji yaitu dari analisa file yang dapat dipulihkan kembali, ada atau tidaknya nama file, ada atau tidaknya ukuran file setelah dilakukan penghapusan data serta adanya *file slack* dari data yang telah dihapus oleh aplikasi penghapusan yang telah dijabarkan sebelumnya. Dimana *File slack* yaitu sebuah ruang di antara akhir sebuah berkas dan akhir dari gugus terakhir yang digunakan oleh berkas yang bersangkutan. Ruang tersebut merupakan area yang tidak akan digunakan lagi untuk menyimpan informasi di sana, sehingga ruang tersebut "terbuang" percuma. slack sering terdiri dari kumpulan teks-teks sampah, tetapi banyak kesempatan yang ditemukan dari file slack dan yang berkaitan dengan investigasi [15] [16]. Jadi adanya *file slack* ini dapat ditelusuri lebih lanjut oleh para pakar forensik karena dapat dianalisa kembali dan banyak kesempatan tentang informasi data yang dapat diketahui jika dianalisa lebih lanjut.

Untuk mendapatkan hasil pada skenario pengujian ini, akan dicatat banyaknya file yang masih bisa terbaca nama file nya dan juga mencatat masih ada atau tidaknya ukuran file pada masing-masing file yang telah dihapus. Semakin sedikit nama file yang masih terbaca maka semakin bagus aplikasi penghapusan tersebut. Dan aplikasi penghapusan tersebut akan dikatakan lebih aman jika tidak meninggalkan ukuran file setelah dilakukan penghapusan. Karena akan lebih sedikit juga kemungkinan untuk file tersebut dapat dipulihkan secara utuh.

Pada tahapan ini, juga dilakukan proses penghapusan, dan juga tahapan pemulihan data. Data yang ada dalam sebuah SD card yang berkapasitas 2GB yang sudah berisikan data yang akan diuji. Kemudian akan dilakukan penghapusan data menggunakan aplikasi penghapusan. Setelah dilakukan penghapusan, maka dilakukan tahapan pemulihan data untuk menguji keefektifitasan suatu aplikasi yang diambil sebagai sampel dan dibandingkan dengan aplikasi yang telah dibuat dengan mengimplementasikan metode DoD 5220.22M. Serta dilakukan pengukuran waktu penghapusan file oleh aplikasi tersebut untuk mengukur tingkat efisiensi dari segi waktu penghapusan yang dibutuhkan aplikasi untuk menghapus suatu data. Untuk itu dibuat alur desain pemulihan data pada Gambar 3.3



Gambar 3.3 Alur Desain Sistem Recovery

SDcard tersebut berisi data-data yang akan dihapus menggunakan aplikasi penghapusan yang telah disebutkan diatas. Sedangkan *Tools recovery* yang digunakan yaitu :

1. *Tool* 1 yaitu menggunakan FTK Imager
2. *Tool* 1 yaitu menggunakan Recuva
3. *Tool* 1 yaitu menggunakan EaseUS Data Recovery Wizard

3.3.1 Penghapusan Data

Penghapusan data dilakukan menggunakan beberapa aplikasi penghapusan yang berjalan di system operasi mobile android yang dapat diunduh di *playstore*. Dan juga menggunakan aplikasi yang telah dibangun sebelumnya menggunakan metode baru dalam penghapusannya. Dimana aplikasi-aplikasi ini mengklaim menggunakan metode DoD 5220.22-M dalam melakukan penghapusan data. Aplikasi yang digunakan yaitu menggunakan

1. Remo File Eraser
2. Andro Shredder
3. ProtectStar iShredder
4. Aplikasi yang dibangun

1. Remo File Eraser

Penghapusan menggunakan aplikasi *Remo File Eraser* dilakukan dengan menggunakan metode penghapusan DoD standard yaitu DoD 5220.22-M yang menggunakan 3 fase dalam melakukan penghapusan file. Langkah-langkah yang dilakukan dalam melakukan penghapusan menggunakan aplikasi *Remo File Eraser* .

1. Pada tampilan awal, pilih menu *options* pada bagian kanan atas kemudian pilih *settings.*
2. Ubah metode penghapusan menjadi High Level (DoD Standard)
3. Pilih folder atau file yang akan dihapus dan klik “erase” untuk memulai penghapusan.

2. Andro Shredder

Penghapusan menggunakan aplikasi *Andro Shredder* dilakukan dengan menggunakan DoD 5220.22-M. Dalam melakukan penghapusan, langkah-langkah yang dilakukan dalam menggunakan aplikasi Andro Shredder

1. Setelah membuka aplikasi, pilih “Shred”.
2. Pilih add pada tab select file and folders.
3. Pilih file maupun folder yang akan dihapus.
4. Tentukan metode penghapusan yang akan digunakan, yaitu menggunakan DoD 5220.22-M (E).
5. Memulai penghapusan “Start Shredder” dengan metode DoD 5220.22-M (E).

3. ProtectStar iShredder

Aplikasi *ProtectStar iShredder* digunakan untuk melakukan penghapusan data yang menggunakan metode DoD 5220.22-M (E) dalam melakukan penghapusan data nya. Aplikasi *ProtectStar iShredder* yang digunakan yaitu merupakan aplikasi *enterprise editon* yaitu aplikasi berbayar yang dapat didapatkan di *android play store.* Langkah-langkah yang dilakukan untuk melakukan penghapusan file menggunakan aplikasi *ProtecStar iShredder*

1. Buka aplikasi kemudian pilih “Start”
2. Pilih menu “files” kemudian tentukan file yang akan dihapus
3. Pilih metode penghapusan yaitu “3 cycles: DoD 5220-22-M E”
4. Mulai penghapusan dengan menekan tombol “Shred”

3.3.2 Pemulihan data

Pemulihan data dilakukan menggunakan tiga buah perangkat lunak yaitu menggunakan FTK Imager, Recuva, dan EaseUS Data Recovery Wizard untuk pemulihan data pada *SDcard* yang telah dilakukan proses penghapusan menggunakan beberapa aplikasi yang telah dijelaskan sebelumnya.

1. Access Data FTK Imager

Access data FTK Imager merupakan suatu perangkat lunak yang sering digunakan untuk melakukan analisa pemulihan data secara forensic. Pemulihan data menggunakan FTK ini dilakukan dengan melakukan mounting pada SDCard yang digunakan untuk melakukan penghapusan file untuk kemudian akan dianalisa.Pada Gambar 3.7 ditunjukkan tampilan pada perangkat FTK Imager. Langkah-langkah yang dilakukan untuk melakukan pemulihan data yaitu sebagai berikut.

1. Tambah image disk yang akan dilakukan analisa pada menu File > Add Evidence Item
2. Pilih opsi image file
3. Tentukan lokasi image file yang akan dilakukan *mounting*, kemudian klik *finish*
4. Cari file yang akan dipulihkan kemudian lakukan *export file*
5. Tentukan tempat dimana file tersebut akan dipulihkan kembali.

2. Recuva

Recuva adalah suatu perangkat lunak berikutnya yang digunakan untuk melakukan pemulihan data di pengujian ini. Recuva merupakan perangkat lunak gratis yang dapat didapatkan secara bebas dan bisa diunduh di Internet. Recuva juga merupakan perangkat lunak yang cukup baik dalam melakukan pemulihan data yang telah terhapus. Langkah-langkah yang dilakukan dalam pemulihan data melalui perangkat lunak recuva yaitu sebagai berikut

1. Setelah aplikasi dibuka, close wizard menu untuk pertama kali aplikasi dibuka
2. Pilih “All Files” agar recuva dapat menemukan semua jenis file yang akan dipulihkan, kemudian klik “next”
3. Pilih “In a specific location” kemudian pilih destinasi folder dari data yang ingin dipulihkan kembali, klik “next”
4. Ceklist pada “Enable Deep Scan” agar recuva dapat menggali data lebih dalam dan data yang didapatkan bisa lebih banyak
5. Lakukan scan dengan klik “start”

3. EaseUS Data Recovery Wizard

EaseUS Data Recovery Wizard merupakan salah satu aplikasi pemulihan data yang tergolong cukup mudah digunakan untuk orang awam. Perangkat lunak ini juga bisa didapatkan dengan gratis dan tersebar bebas di internet. Langkah-langkah yang dilakukan untuk melakukan pemulihan data yaitu

1. Setelah aplikasi dibuka, pilih pada “All File Types” agar aplikasi dapat menemukan semua jenis tipe file yang akan dipulihkan. Klik “next”
2. Tentukan tempat destinasi *drive* yang akan dilakukan pemulihan data
3. Untuk memulai klik “Scan”.

3.3.3 Parameter Pembanding Keamanan Data

Parameter yang digunakan untuk melakukan perbandingan hasil analisis keaman data yaitu menggunakan sistem status. Dimana akan dibagi menjadi tiga status yaitu Awas, siaga , dan waspada. Dimana hal-hal yang akan dibandingkan yaitu

1. File yang dapat dipulihkan dan dapat dijalankan kembali
2. File yang dapat dipulihkan sebagian (*partial recovered)*
3. Adanya nama file, ukuran file, dan adanya file slack

Tabel 3.2 Poin Parameter Pengujian Keamanan Data

No	Jenis	Status
1	File dapat dipulihkan dan dijalankan kembali	Awas

2	File dapat dipulihkan sebagian	Siaga
3	Adanya nama file, ukuran file, dan file slack	Waspada

Seperti pada tabel 3.2, parameter perbandingan ini dilakukan untuk mengukur tingkat kekurangan suatu aplikasi dalam segi keamanan datanya. Dalam parameter pengujian ini, Status awas memiliki nilai tertinggi diikuti oleh status siaga kemudian waspada. Aplikasi dengan status Awas paling banyak, berarti memiliki tingkat kelemahan yang paling tinggi, tidak peduli jumlah status siaga dan waspada yg didapat, layaknya sistem olimpiade.

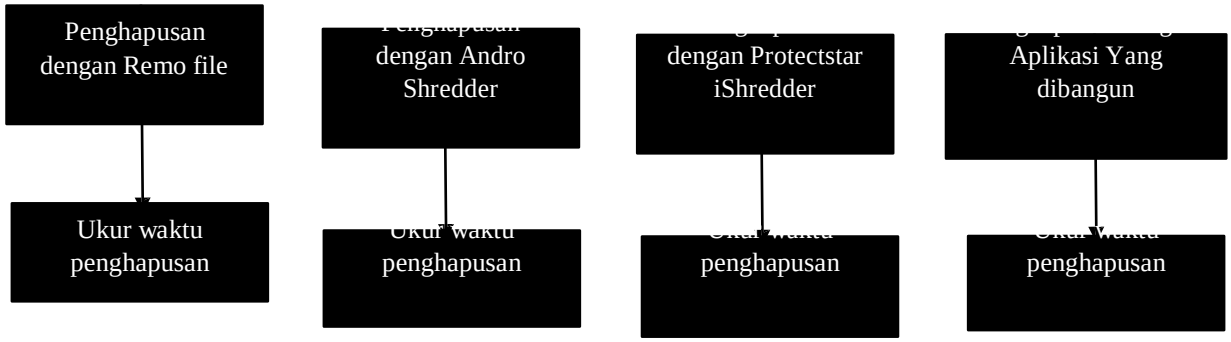
File dapat dipulihkan dan dijalankan kembali mempunyai nilai status yg paling besar yaitu status awas, dikarenakan jika ada file yang masih bisa dipulihkan berarti aplikasi tersebut belum sempurna dalam melakukan penghapusan file. Kemudian diikuti status siaga sebagai nilai dari file yang bisa dipulihkan sebagian, atau *partial recovery*, karena file tersebut dapat dipulihkan meskipun tidak bisa dijalankan kembali ataupun file tersebut rusak, dan dari hal itu masih ada celah untuk dilakukan analisa forensic digital.

Sedangkan adanya nama file, ukuran file, serta adanya file slack memiliki status waspada karena dalam keadaan tersebut sangat memungkinkan oleh para pakar forensic untuk dapat dianalisa, baik dari nama file yang terlihat maupun file slack yang ditemukan yang dapat dianalisis lebih lanjut oleh para ahli forensic digital.

Pemeringkatan tingkat kekurangan aplikasi dinilai berdasarkan jumlah status yang didapat, aplikasi dengan jumlah status paling banyak memiliki peringkat keamanan yang paling rendah. Tentunya didasarkan pada parameter yang sudah dijelaskan pada tabel 3.2 .

3.4 Skenario Pengujian Performansi Sistem

Pada tahap uji performansi ini, akan dilakukan pengujian berdasarkan waktu yang dibutuhkan oleh aplikasi dalam menghapus suatu data yang diberikan. Semakin cepat waktu yang dibutuhkan untuk melakukan penghapusan, maka semakin baik juga aplikasi tersebut dari segi efisiensinya. Pengukuran akan dilakukan secara manual menggunakan *timer* saat aplikasi melakukan penghapusan data. Dalam melakukan skenario uji efisiensi ini akan dicatat waktu yang dibutuhkan oleh aplikasi penghapusan dalam melakukan penghapusan 40 file sebesar 298 MB pada lima *SDCard* yang telah disiapkan, yang mana masing-masing *SDCard* mempunyai kapasitas 2 GB. Penghapusan dilakukan sebanyak lima kali menggunakan aplikasi yang berbeda.Pencatatan waktu penghapusan dilakukan menggunakan *stopwatch* pada *smartphone.* Dan akan dilaporkan dalam bentuk *screenshot* dari tiap waktu yang dibutuhkan oleh aplikasi dalam melakukan penghapusan data. Pengujian performansi melalui waktu penghapusan ini digunakan sebagai parameter pembanding antar aplikasi penghapusan. Dimana penilaian performansi sistem ini dilakukan sebagai pembanding jika saat dilakukan pengujian keamanan data terdapat nilai yang sama. Sehingga perlu dilakukan pengujian performansi sistem ini untuk menentukan aplikasi yang lebih baik. Pemeringkatan dilakukan berdasarkan kecepatan waktu penghapusan, aplikasi dengan waktu penghapusan tercepat akan memiliki peringkat tertinggi. Gambar 3.10 menunjukkan rancangan pengukuran waktu penghapusan data.



Gambar 1.2 Uji Waktu Penghapusan

3.5. Pengujian Keamanan Data Aplikasi Sampel

Pada skenario uji keamanan data ini akan dilakukan proses *recovery* dari data yang telah dihapus sebelumnya untuk mendapatkan kembali data yang telah dihapus oleh masing-masing aplikasi penghapusan yang telah diujikan sebelumnya. Dalam skenario ini menggunakan tiga buah perangkat lunak untuk melakukan proses *recovery* data.

3.5.1 Remo File Eraser

Aplikasi pertama yang dilakukan uji pemulihan data yaitu Remo File Eraser. Proses pemulihan data dilakukan menggunakan tiga buah aplikasi yaitu Acces Data FTK Imager, recuva, dan EaseUS Data Recovery Wizard.

1. Access Data FTK Imager

Dalam pengujian pemulihan data menggunakan Access Data FTK Imager, ditemukan total 65 file dari total 40 file. Hal ini dikarenakan ditemukan juga *file slack* saat dilakukan proses pemulihan data. Setelah dilakukan proses *recovery* hanya ada lima file yang masih bisa dibuka dan dijalankan kembali. Yaitu file

1) ksm.oxps
2) 03. Michelle Branch - All You Wanted.mp3
3) 3 Door Down - Here Without You.mp3
4) !taf.rar (staf.rar)
5) IBMRSA_v8_Activation_Kit.z

2. Recuva

Dalam pengujian pemulihan data menggunakan aplikasi Recuva, ditemukan 30 file dari total 40 file yang dihapus. Dan 30 file tersebut memiliki status "*excellent"* yang berarti file tersebut memiliki kesempatan yang tinggi untuk dilakukan proses *recovery*. Setelah dilakukan proses *recovery* didapatkan tiga file yang masih bisa dibuka dan dijalankan kembali yaitu

1) ksm.oxps
2) 3 Door Down - Here Without You.mp3
3) _faf.rar (staf.rar)

3. Easeus Data Recovery Wizard

Dalam pengujian pemulihan data menggunakan aplikasi ini, ditemukan 29 file dari total 40 file yang dihapus. Gambar 4.3 menunjukkan tampilan pemulihan data menggunakan aplikasi ini. Hanya ditemukan lima file yang masih bisa dibuka dan dijalankan kembali, yaitu

1) ksm.oxps
2) 03. Michelle Branch - All You Wanted.mp3
3) 3 Door Down - Here Without You.mp3
4) #taf.rar (staf.rar)
5) IBMRSA_v8_Activation_Kit.z

3.5.2 Andro Shredder

Aplikasi ke dua yang akan dilakukan uji pemulihan data yaitu Andro Shredder. Akan dilakukan proses *recovery* menggunakan 3 buah aplikasi pemulihan data yang sudah dijabarkan sebelumnya.

1. Access Data FTK Imager

Dalam pemulihan data mengguanakan aplikasi Access Data FTK Imager ini, ditemukan 53 file dari 40 file yang dihapus dapat dilihat pada Gambar 4.4. Hal tersebut dikarenakan penulis juga menemukan

adanya *file slack* dari data yang telah dihapus. Setelah dilakukan proses *recovery* hanya ada 1 file yang masih bisa dibuka yaitu file "Indieground_freebies_newyear.zip".

2. Recuva

Dalam pemulihan data menggunakan aplikasi recuva seperti Gambar 4.5, ditemukan tiga file dari total 40 file yang telah dilakukan penghapusan sebelumnya menggunakan aplikasi Andro Shredder. Dan setelah dilakukan proses *recovery*, hanya tiga file yang dapat dibuka dan dijalankan kembali yaitu

1) Kesalahan Yang Sama_Kerispatih000.MP3
2) FILE001.MP3 dengan nama file aslinya adalah "3 Door Down - Here Without You.mp3"
3) indieground_freebies_newyear.zip

3. EaseUS Data Recovery Wizard

Setelah dilakukan proses pemulihan data menggunakan aplikasi ini, ditemukan enam file dari total 40 file yang telah dihapus menggunakan aplikasi Andro Shredder. Dapat dilihat di Gambar 4.6 ,Setelah dilakukan proses *recovery,* ada tiga file yang masih bisa dibuka dan dijalankan kembali yaitu

1) Kesalahan Yang Sama_Kerispatih000.MP3
2) FILE001.MP3 dengan nama file aslinya adalah "3 Door Down - Here Without You.mp3"
3) indieground_freebies_newyear.zip

3.5.3 ProtectStar iShredder Enterprise Edition

Aplikasi berikutnya yang digunakan untuk melakukan uji pemulihan data yaitu ProtectStar iShredder Enterprise Edition. Dilakukan proses pemulihan data menggunakan 3 buah aplikasi *recovery data.*

1. Access Data FTK Imager
   Setelah proses pemulihan data dilakukan menggunakan FTK Imager, tidak ditemukan file yang bisa dipulihkan kembali

2. Recuva
   Menunjukkan pemulihan data menggunakan aplikasi recuva juga tidak menemukan satu file pun setalah dilakukan proses recovery.

3. EaseUS Data Recovery Wizzard
   Dilakukan pemulihan data menggunakan aplikasi ini juga tidak menemukan file yang sebelumnya telah dihapus. Jadi tidak ada file yang dapat dipulihkan serta dijalankan kembali.

Setelah dilakukan pengujian aplikasi, didapatkan kesimpulan dari segi keamanan data seperti pada tabel 4.1.

Tabel 2.1 Data Hasil Uji Keamanan Data Aplikasi Sampel

no	Nama Aplikasi	File bisa dipulihkan (Awas)	File di*recovery* Sebagian (Siaga)	Ukuran file, nama file dan file Slack (Waspada)			Peringkat
				Ukuran File	Nama file	File Slack	
1	Remo file	5	30	ada	ada	ada	3

2	Andro Shredder	3	6	tidak	ada	ada	2
3	iShredder	0	0	tidak	tidak	tidak	1

3.6 Pengujian Performansi Aplikasi Sampel

Pengujian performansi ini dilakukan untuk melakukan penilaian terhadap aplikasi jika ditemukan nilai yang sama pada aplikasi yang dibandingkan dari segi keamanan data. Data yang diujikan untuk dilakukan penghapusan data yaitu sebanyak 40 file dengan berbagai tipe file yaitu audio, *compressed file*, dokumen, gambar, teks, dan video. Total keseluruhan data yang akan dihapus yaitu sebesar 298 MB. Perhitungan waktu dilakukan secara manual menggunakan *stopwatch* dalam satuan detik.

Hasil pengujian

3.6.1 Remo File Eraser

Dilakukan perhitungan waktu yang dibutuhkan oleh aplikasi remo file eraser untuk melakukan penghapusan menggunakan metode DoD 5220.22 M. Tercatat waktu yang diperlukan untuk menghapus file sebanyak 40 file sebesar total 298 MB yaitu selama kurang lebih 4 detik.

3.6.2 Andro Shredder

Dilakukan pengujian untuk mengukur jumlah waktu yang diperlukan oleh aplikasi Andro Shredder untuk melakukan penghapusan file sebanyak 40 file dan sebesar 298 MB. Metode yang digunakan yaitu menggunakan metode DoD 5220.22 M. Tercatat waktu yang dibutuhkan yaitu selama 45 detik.

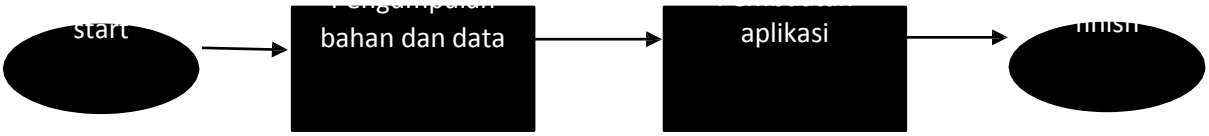
3.6.3 ProtectStar iShredder Enterprise Edition

Dilakukan pengujian untuk mengukur waktu yang dibutuhkan aplikasi ProtectStar iShredder dalam melakukan penghapusan file sebesar 298 MB dan sebanyak 40 buah file. Metode yang digunakan untuk melakukan penghapusan yaitu mengguanakan metode DoD 5220.22 M. Tercatat aplikasi ini dapat melakukan penghapusan file selama 11 menit 5,38 detik.

Tabel 3.2 Tabel Perbandingan Performansi Waktu

No	Nama Aplikasi	Waktu Penghapusan	Peringkat
1	Remo File Eraser	4 detik	1
2	Andro Shredder	45 detik	2
3	ProtectStar iShredder Enterprise	11 menit 5 detik	3

3.7 Develop Aplikasi



Gambar 3.32 Flowchart Pembuatan Aplikasi

3.7.1 Pengumpulan Source dan Data

Dalam pembuatan aplikasi penghapusan ini, mengambil dari beberapa source yang berasal dari internet dan dipublikasikan secara bebas. Source yang didapat berupa sebuah file manager yang berjalan di aplikasi android, aplikasi tersebut bernama "open manager" merupakan aplikasi yang berfungsi sebagai file

manager yang bisa untuk menjelajah file, menghapus file, rename file, *copy* file, dan beberapa fungsi lain [17].

Sedangkan untuk menjalankan fungsi shredder atau fungsi penghapusannya, penulis menggunakan source yang didapatkan dari internet juga, dimana dalam source tersebut terdapat beberapa metode shredder atau metode penghapusan, termasuk DoD 5220.22M E berada di dalam source tersebut. Source yang didapat merupakan sebuah aplikasi yang berjalan di sistem java. File tersebut bernama Ataraxis [18].

3.7.2 Pembuatan Aplikasi

Pembuatan aplikasi penghapusan ini menggunakan aplikasi android studio. Langkah pertama yang dilakukan dalam pembuatan aplikasi yaitu :

1. Meng *import* source yang didapat tadi kedalam android studio
2. Setelah berhasil meng *import* file manager, kemudian tambahkan juga file dari Ataraxis yang dibutuhkan untuk melakukan penghapusan atau *Shredder* file seperti pada Gambar 4.12. Dalam pembuatan aplikasi ini, file yang dibutuhkan dari project Ataraxis untuk melakukan penghapusan yaitu AtaraxisShredder.java, FileList.java, dan folder ataraxis.crypt. File tersebut kemudian ditambahkan ke dalam project di android studio. Dalam class AtaraxisShredder.java terdapat metode DoD 5220.22M standar yang akan digunakan sebagai metode penghapusan dalam aplikasi ini.

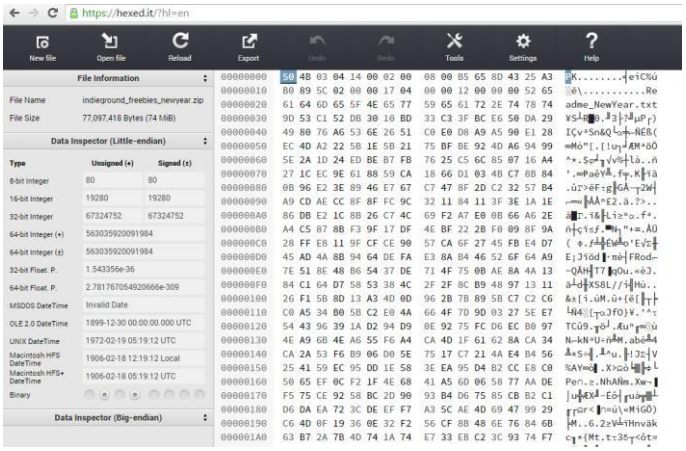
   Dalam metode tersebut yaitu menggunakan 3 pass dalam pengimplementasiannya. Yaitu menimpa dengan byte random, byte_FF, dan byte_00. Dimana byte_00 yaitu Byte 0x00 = 00000000 . Byte 0x00 diletakkan di fase terakhir ditujukan agar lebih mudah dalam proses verifikasi. Setelah dilakukan proses *overwrite* tersebut, barulah dilakukan penghapusan data, namun sebelum data tersebut dihapus, data tersebut dihapus terlebih dahulu nama file nya secara acak, agar saat dilakukan proses *recovery* nama asli dari file yang dihapus tidak akan terbaca.
3. Dalam pembuatan aplikasi ini, perlu beberapa perubahan agar class dari project ataraxis bisa tersambung dengan project pada file open manager ini tanpa adanya *error*. Karena pada file manager ini belum mempunyai menu untuk melakukan penghapusan menggunakan metode DoD 5220.22M, ditambahkan beberapa *syntax* pada *class* Main, dan *class* EventHandler.

   Pada *class* Main, ditambahkan konteks menu, agar saat melakukan penghapusan muncul pilihan untuk melakukan penghapusan menggunakan metode DoD 5220.22M ini. Seperti tambahan menu untuk mendelete dengan DoD, dan juga tampilan peringatan untuk melanjutkan penghapusan atau tidak.
4. Build project

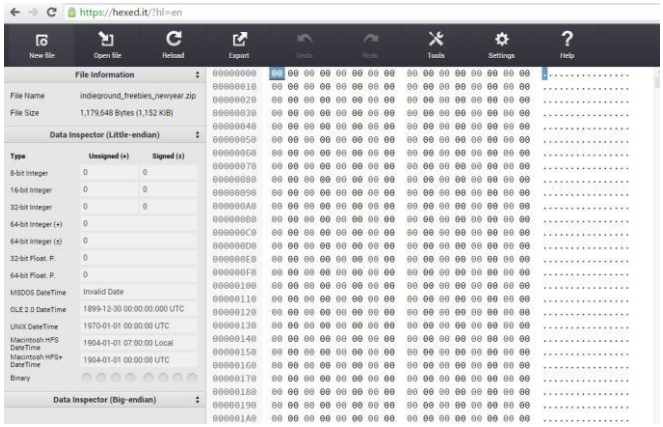
   Setelah semua terhubung dan tidak ada *error* yang muncul, maka tahap akhir yang dilakukan yaitu pembangunan atau *build project* untuk kemudian dijalankan. Tampilan aplikasi yang dibuat, sebelum adanya metode DoD untuk melakukan penghapusan, dibandingkan dengan aplikasi yang sudah ditambahkan metode DoD untuk melakukan penghapusan data.

3.7.3 Pengujian Verifikasi Aplikasi yang Dibuat

Pengujian aplikasi ini bertujuan untuk mengetahua atau memverifikasi bahwa aplikasi telah menjalankan fungsi penghapusan dengan benar, yaitu dengan melakukan *overwrite* file dengan byte random, byte 1, dan kemudian dengan byte 0. Untuk itu akan dilakukan penghapusan sebuah file untuk kemudian dilihat hex dari file tersebut untuk kemudian dilihat perbedaan hex sebelum dan sesudah dilakukan penghapusan file tersebut. Gambar 4.19 menunjukkan hex dari file sebelum dilakukan penghapusan menggunakan metode DoD 5220.22M ini, sedangkan gambar 4.20 menunjukkan hex dari file setelah dilakukan penghapusan. Pengecekan hex file ini menggunakan fasilitas hex editor online yang dapat diakses di situs https://hexed.it.



Gambar 4.19



Gambar 4.20

3.8 Pengujian Keamanan Data Aplikasi yang Dibuat

Aplikasi ke empat yang digunakan untuk melakukan proses pemulihan data yaitu aplikasi yang dibangun dan didevelop oleh penulis. Yang kemudian akan dilakukan proses pemulihan data menggunakan tiga buah aplikasi *recovery.*

Tabel 3.3 Hasil Uji Keamanan Data Aplikasi yang Dibuat

no	Nama Aplikasi	File bisa dipulihkan (Awas)	File di*recovery* Sebagian (siaga)	Ukuran file, nama file dan file Slack (waspada)		
				Ukuran File	Nama file	File Slack
1	Aplikasi yang dibuat	5	5	ada	tidak	ada

3.9 Pengujian Performansi Aplikasi yang Dibuat

Dalam pengujian performansi aplikasi yang dibuat ini, diukur waktu yang dibutuhkan oleh aplikasi yang dibuat untuk menghapus sejumlah data dan diukur secara manual mengguanak stopwatch dalam satuan detik, dan didapatkan hasil seperti pada tabel

Tabel 3.4

No	Nama Aplikasi	Waktu Penghapusan
1	Aplikasi yang dibuat	3 menit 7 detik

Dalam Tabel 3.4 menunjukkan waktu yang diperlukan oleh aplikasi yang dibuat untuk menghapus sebanyak 40 file sebesar total 298 MB, dan menggunakan metode DoD 5220.22 M dalam melakukan penghapusannya. Tercatat aplikasi yang dibuat ini membutuhkan waktu 3 Menit 7 detik untuk melakukan penghapusan data.

3.10 Perbandingan Aplikasi Yang Dibuat Dengan Aplikasi Sampel

Tabel 3.5

no	Nama Aplikasi	File bisa dipulihkan (Awas)	File di*recovery* Sebagian (Siaga)	Ukuran file, nama file dan file Slack (Waspada)			Waktu Penghapusan	Peringkat
				Ukuran File	Nama file	File Slack		
1	Remo file	6	30	ada	ada	ada	4 detik	4
2	Andro Shredder	5	6	tidak	ada	ada	45 detik	3
3	iShredder	0	0	tidak	tidak	tidak	11 menit 5 detik	1
4	Aplikasi yang dibuat	5	5	ada	tidak	ada	3 menit 7 detik	2

Dari tabel 3.5 menunjukkan perbandingan aplikasi dan dapat dilihat bahwa aplikasi remo file memiliki status Awas yang paling banyak yaitu dengan 6 status, diikuti oleh aplikasi andro shredder dan aplikasi yang dibuat dengan 5 status awas. Dengan demikian, aplikasi remo file eraser memiliki tingkat keamanan data yang paling rendah merujuk dari parameter pembanding keamanan data. Sedangkan aplikasi yang dibuat memiliki tingkat keamanan yang lebih baik dibanding remo file dan andro shredder. Walaupun aplikasi yang dibangun dan andro shredder memiliki status awas yang sama yaitu lima, namun dalam banyaknya status siaga yang didapat, andro shredder memiliki status siaga yang lebih banyak dibandingkan dengan aplikasi yang dibuat. Untuk itu tingkat keamanan data dari aplikasi yang dibuat lebih baik dibanding Andro Shredder dan Remo File Eraser. Karena waktu penghapusan data dimasukkan kedalam penilaian jika ada nilai poin yang sama, maka waktu penghapusan data tidak berpengaruh pada peringkat yang didapat oleh aplikasi diatas.

Hal yang mempengaruhi segi keamanan data dan juga performansi aplikasi yaitu dari segi pengimplementasian metode DoD 5220.22M kedalam aplikasi. Kebanyakan aplikasi yang dibuat tidak hanya langsung menerapkan metode ini kedalam aplikasi, namun juga menambah beberapa teknik tambahan untuk menambah keamanan data yang telah dihapus agar tidak bisa dipulihkan kembali. Teknik tambahan tersebut seperti adanya fase verifikasi yang dilakukan dalam pengimplementasiannya, dimana verifikasi ini ditujukan untuk melakukan pengecekan apakah tahapan penghapusan data sudah dilakukan secara benar atau tidak. Tentunya proses ini akan memakan waktu yang lebih lama jika dibandingkan dengan aplikasi yang tidak melakukan proses verifikasi dalam pengimplementasiannya. Selain itu, setiap aplikasi juga memiliki cara yang berbeda dalam mengimplementasikan metode DoD 5220.22M ini, ada yang melakukan penghapusan *free space* dahulu setelah melakukan *overwrite* pada data yang dihapus.

4 Kesimpulan.

Dari hasil analisis serta perbandingan aplikasi penghapusan yang diujikan dalam penelitian ini, maka dapat ditarik kesimpulan sebagai berikut:

a) Sebagian besar aplikasi penghapusan dengan menggunakan metode DoD 5220.22M 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. Seperti adanya nama file yang masih bisa dilihat setelah dilakukan proses pemulihan data.

b) Dari segi keamanan data penghapusan dari aplikasi yang dibuat, sudah memiliki tingkat kemanan data yang cukup baik dibanding dengan Remo File Eraser dan juga Andro Shredder. Serta memiliki waktu penghapusan yang tidak terlalu lama sehingga memiliki tingkat performansi yang cukup baik. Namun masih memiliki kekurangan dalam hal keamanan data, yaitu masih ada file yang bisa dipulihkan kembali.

c) Aplikasi yang dibuat sudah dengan benar menerapkan metode penghapusan menggunakan DoD 5220.22M pada aplikasi tersebut, yaitu menimpa file dengan byte random, byte 1, dan byte 0.

DAFTAR PUSTAKA

[1] Bahl, Vikram., Leong, David., Jiayan ,Guo., Siang, Jonathan., and Lan, Tay Mei., "Secure Data Shredder," in *Proceedings* of the *Global Engineering*, *science* and *technology Conference*, Dhaka, 2012

[2] "ERASER: Appendix A : Erasure Methods, "www.eraser.heidi.ie. [Online]. Available: http://eraser.heidi.ie/documentation/appendix-a-erasure-methods/ [Accessed 10-Mar-2015]

[3] "UCRiverside: Data Sanitization, "www. cnc.ucr.edu. [Online]. Available : http://cnc.ucr.edu/security/datasan.html. [Accesed: 10-mar-2015].

[4] "Standford University: Disk and data Sanitization Policy and Guidelines," web.stanford.edu. [Online]. Available : http://web.stanford.edu/group/security/securecomputing/data_destruction_guidelines.html. [Accessed: 10-Mar-2015].

[5] Hughes, Gordon and Coughlin, Tom. (2006) Tutorial on Disk Drive Data Sanitization.

[6] "GuruHDD: Data Recovery, "www.guruhdd.com. [Online]. Available: http://www.guruhdd.com/recovery.php. [Accesed: 11-mar-2015].

[7] "DestruckData: Departement of Defence (DoD) Media Sanitization Guidelines 5220.22M, www.destructdata.com. [Online]. Available: http://www.destructdata.com/dod-standard/. [Accessed: 11-mar-2015].

[8] Al Anhar, Azwar. "Analisis Perbandingan Kemanan Teknik Penghapusan Data Pada *Hardisk* dengan Metode DoD 5220.22 dan Gutmann, Bandung, 2014.

[9] D. Edgar, "Data sanitization Techniques," White Pap,. 2004

[10] "HGST: Instant Secure Erase, "www.hgst.com. [Online]. Available: http://www.hgst.com/tech/techlib.nsf/techdocs/066FD0FE010564C788257D8F0008851A/$file/Instant-Secure-Erase-Overview-TB01.pdf. [Accessed: 11-mar-2015].

[11] Eraser.heidi: American Department of Defense 5220.22-M standard wipe, **www.eraser.heidi.ie**. [Online]. Available : http://eraser.heidi.ie/forum/threads/american-department-of-defense-5220-22-m-standard-wipe.530/

[12] Wikipedia: National Industrial security program .wikipedia.org. [Online]. Available : https://en.wikipedia.org/wiki/National_Industrial_Security_Program [Accessed: Dec-2015].

[13] Wikipedia: Data Shredder. wikipedia.org. [Online]. Available : https://en.wikipedia.org/wiki/Data_Shredder. [Accessed:Dec-2015].

[14] D-Artchitext's, Fungsi perbedaan delete dan Shred. Blog.finderonly.net.[Online[Available : http://blog.finderonly.net/2014/fungsi-perbedaan-delete-dan-shred-scrub.html

[15] Wikipedia: Ruang Renggang. wikipedia.org. [Online]. Available : https://id.wikipedia.org/wiki/Ruang_renggang. [Accessed:Dec-2015].

[16] Forensics.Computer: what is file slack. www.computer-forensics.net. [Online]. Available: http://www.computer-forensics.net/FAQs/what-is-file-slack.html

[17] Github: Android file Manager, www.github.com. [Online]. Available: https://github.com/nexes/Android-File-Manager [Accessed: Jan-2015].

[18] Github: Ataraxis, www.github.com. [Online]. Available: https://github.com/jgraber/ataraxis [Accessed: Jan-2015].