BAB 1

PENDAHULUAN

1.1 Latar Belakang

Informasi saat ini merupakan suatu hal yang penting dan harus dijaga, namun dalam hal perlindungan informasi pada saat ini untuk individu maupun organisasi masih dibilang sangat kurang diperhatikan[1]. Padahal informasi sendiri merupakan hal yang sangat penting dan beberapa bersifat rahasia bagi beberapa orang, informasi juga dapat menimbulkan ancaman bagi pemilik informasi apabila informasinya jatuh kepada orang yang salah, bahkan dapat mengakibatkan kerugian yang besar hanya karena informasi nya tidak terjaga dengan baik[10].

Dalam melakukan perlindungan informasi sendiri tidak lepas dari bidang ilmu anti-forensics, yang merupakan metode untuk menyembunyikan suatu informasi atau file yang dianggap sebagai barang bukti digital [13], dalam hal ini berarti lawan atau kebalikan dari ilmu forensic yang bertujuan untuk mencari bukti digital dari sebuah kasus digital yang terjadi. Pada anti-forensics umumnya perlindungan informasi atau data dapat mengacu pada dua hal, yang pertama yaitu melakukan tindakan agar data yang tersimpan pada media penyimpanan tidak dapat dibuka ataupun ditemukan dengan menggunakan berbagai metode dari anti-forensics, kemudian hal yang kedua yaitu mengupayakan agar data atau file bukti yang berhasil ditemukan tidak dapat digunakan ataupun tidak sesuai dengan standar hukum, yang dalam hal ini berarti data atau file bukti tersebut tidak dapat dijadikan barang bukti pada saat proses persidangan[12]. Mengikuti hal pertama tadi yaitu agar data tidak dapat di temukan salah satu nya dengan penghapusan data, metode ini merupakan salah satu metode anti-forensics yang paling sering digunakan oleh para pemilik informasi yang terdapat pada media penyimpanan elektronik. Pada umumnya metode ini dilakukan dengan menekan tombol delete dan mengosongkan recycle bin atau trash pada sistem.

Pemilik informasi beranggapan bahwa proses yang dilakukan telah benar-benar menghapus data, namun proses tersebut hanya menghilangkan pointer pada blok media penyimpanan yang menyimpan data dan kemudian dianggap sebagai ruang kosong untuk dapat diisi kembali dengan data yang baru[3]. Data yang dianggap telah terhapus sangat berpotensi untuk dilakukan proses recovery dengan menggunakan ilmu digital forensik, atau dengan kata lain bahwa data tersebut masih memungkinkan untuk didapatkan. namun proses tersebut hanya menghilangkan pointer pada blok media penyimpanan yang menyimpan data dan kemudian dianggap sebagai ruang kosong untuk dapat diisi kembali dengan data yang baru[16]. Data yang dianggap telah terhapus sangat berpotensi untuk dilakukan proses recovery dengan menggunakan ilmu digital forensik, atau dengan kata lain bahwa data tersebut masih memungkinkan untuk didapatkan. Untuk mengatasi tindakan tersebut perlu dilakukan proses penghapusan data pada media penyimpanan yang benar-benar aman sehingga data tersebut tidak dapat dilakukan proses recovery [1]. Salah satu yang dapat dilakukan untuk menghilangkan bukti yang terdapat pada media penyimpanan dengan menggunakan teknik data wiping [15], namun metode wiping sendiri sangat beragam jenis nya ada yang melakukan overwrite setelah penghapusan data dengan 1 fase, 7 fase sampai 35 fase[15]. Pada penelitian ini yang akan dilakukan mempunyai tujuan untuk melakukan analisis tools yang sudah di tentukan sebelumnya, untuk mencari seberapa besar efesiensi keberhasilan menggunakan data wiping yang ada dan mengetahui perbedaan pada setiap tools dalam menjalankan metode wiping untuk membantu kegiatan forensic terkait penggunaan tools dalam menjalankan metode wiping nantinya. Karena fakta nya tidak semua alat anti forensik bekerja sesempurna yang diiklankan, sehingga meninggalkan bekas dan jejak[12]. Dalam penelitaan ini untuk menguji tools dilakukan metode-metode wiping yang sama yang terdapat pada tools, dan metode yang dipilih menjadi acuan yaitu Zero Overwrite, Random Data Overwrite, U.S. DoD 5220.22-M (E), U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's Algorithm.

Adapun alasan pada penelitian ini mengapa menggunakan metode-metode wiping data seperti yang di sebutkan di atas adalah. Pertama pada metode yang

paling simple yaitu zero overwrite dipilih karena ingin membuktikan apakah ada kesalahan pada setiap tools yang dipilih untuk melakukan penghapusan dengan satu fase yang data nya hanya ditimpa dengan nol[15], jika ada maka tools tersebut tidak terbilang berhasil melakukan wiping data. Lalu pada metode random data overwrite yang persis sama dengan metode sebelumnya tapi mempunyai perbedaan ada pada data yang ditimpa dengan aliran byte yang dihasilkan secara acak, pada algoritma ini dilakukan observasi apakah setiap tools menghasilkan random yang berpola sama atau berbeda total[16]. Dan metode sisanya dipilih karena merupakan metode yang popular digunakan untuk melakukan wiping data, yang mempunyai fase overwrite setelah penghapusannya lebih dari satu. Dari yang melakukan wiping data dengan 3 fase overwrite setelah penghapusan yaitu U.S. DoD 5220.22-M (E)[13]. dan ada yang menggunakan 7 fase overwrite yaitu U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's Algorithm setelah penghapusan[13].

1.2 Rumusan Masalah

Berikut rumusan masalah dalam penelitian ini:

1. Apakah setiap tools berhasil mengamankan data setelah dilakukan wiping data?
2. Apakah ada tools yang paling optimal melakukan wiping data dengan metode wiping data yang sama?
3. Apakah ada metode yang paling unggul pada setiap tools dalam menjalankan data wiping dengan menggunakan setiap metode yang ditentukan?

1.3 Batasan Masalah

Berikut batasan masalah dalam penelitian ini:

1. Penghapusan wipping data menggunakan tools berdasarkan file yang sudah disiapkan.
2. Penghapusan wipping data menggunakan tools pada device penyimpanan yang disiapkan.
3. Penghapusan wipping data menggunakan tools dengan menerapkan metode wiping data yaitu Zero Overwrite, Random Data Overwrite, U.S. DoD 5220.22-M (E), U.S. DoD 5220.22-M (ECE), dan Bruce Schneier's Algorithm.
4. Pengecekan performance tools tidak dari sisi data wipping, menambahkan aspek aplikasi lainnya seperti running time, CPU usage, memory usage, dan recovery data.

1.4 Tujuan Penelitian

Berikut adalah tujuan yang ingin dicapai dalam penelitian ini:

1. Mengidentifikasi seberapa akurat metode yang di tentukan sebelumnya dalam melakukan data wiping pada setiap tools.
2. Mengidentifikasi kelebihan setiap tools dalam menjalankan data wiping dengan menggunakan metode yang sama dalam data wiping.
3. Mengidentifikasi kekurangan setiap tools dalam menjalankan data wiping dengan menggunakan metode yang sama dalam data wiping.
4. Mengidentifikasi tools terbaik untuk setiap metode dan metode terbaik untuk setiap tools menjalankan wiping data berdasarkan variabel running time, CPU usage, memory usage, dan recovery data.

1.5 Hipotesis

Berikut Hipotesis dalam penelitian ini:

Table 1 Hipotesis Penelitian

Pertanyaan Penelitian	Hipotesis	Hipotesis nol
Apakah setiap tools berhasil merusak data setelah dilakukan wiping data?	setiap tools berhasil merusak data setelah dilakukan wiping data	setiap tools tidak berhasil merusak data setelah dilakukan wiping data?
Apakah ada tools yang paling optimal melakukan wiping data dengan metode wiping data yang sama?	Terdapat tools yang paling optimal melakukan wiping data dengan metode wiping data yang sama	Tidak terdapat tools yang paling optimal melakukan wiping data dengan metode wiping data yang sama
Apakah ada metode yang paling unggul pada setiap tools dalam menjalankan data wiping dengan menggunakan setiap metode yang ditentukan?	Setiap tools mempunyai keunggulan nya tersendiri dalam menjalankan data wiping dengan metode yang sama	Setiap tools tidak mempunyai keunggulan nya tersendiri dalam menjalankan data wiping dengan metode yang sama

1.6 Rencana Kegiatan

Table 2 Rencana Kegiatan

No	Nama Kegiatan	Bulan					
		1	2	3	4	5	6
1	Studi Literatur						
2	Pengajuan Judul						
3	Penulisan Laporan						
4	Pengajjuan Proposal						
5	Penelitian Proposal						
6	Sidang						
7	Revisi						
8	Pembuatan Buku Laporan / Jurnal TA						