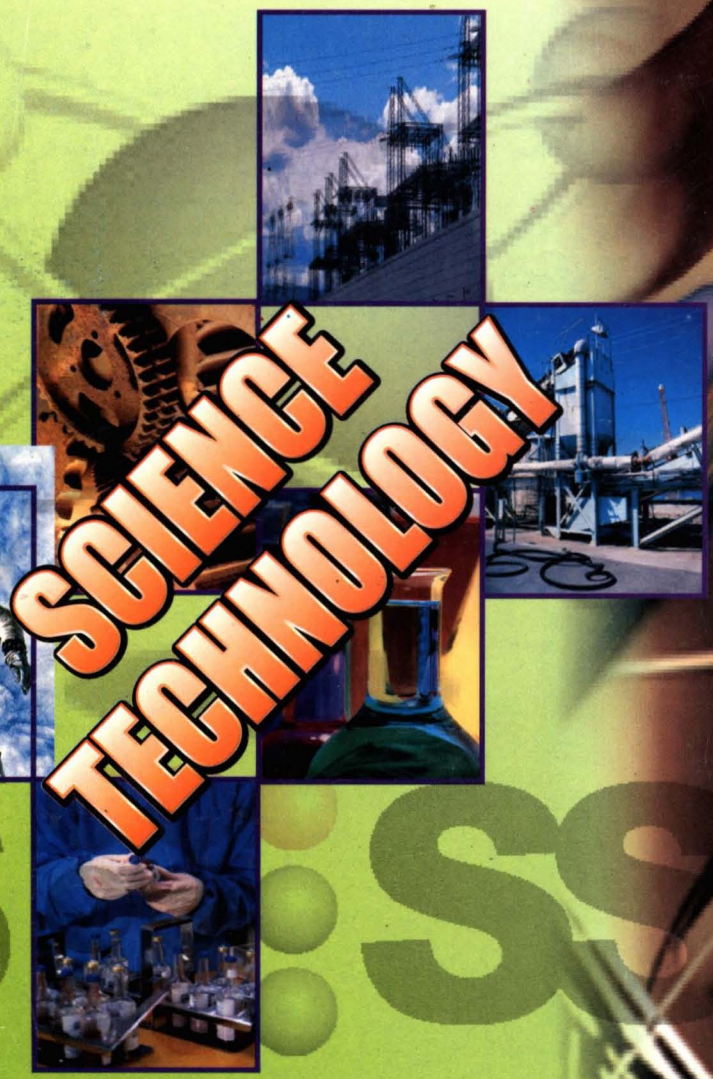
UNIVERSITI TEKNOLOGI MARA

ISO 9001:2000 No Sijil :0500132

Globalising Knowledge and Information



NATIONAL SEMINAR ON SCIENCE TECHNOLOGY & SOCIAL SCIENCES 2006

30-31 May 2006

Swiss Garden Resort & Spa

Kuantan, Pahang

Sistem Pemulihan Data: Alat Forensik Cakera Dalam Mengesan Jenayah Komputer

Abd Hadi Abd Razak

ABSTRAK

Pemulihan data adalah merupakan satu kaedah yang sering digunakan di dalam bidang forensik komputer bagi mendapatkan bukti jenayah yang telah dipadam dari komputer. Proses pemulihan data yang telah dipadam boleh dilakukan kerana apabila fail dipadam dari komputer, ia sebenarnya bukan hilang dari cakera tetapi hanya penunjuk kepada fail tersebut yang dipadam dari Jadual Perletakan Fail (FAT), Jadual Utama Fail (MFT) atau skema lain yang digunakan oleh sistem pengoperasian. Ini membuktikan bahawa sesuatu fail yang telah dipadam dapat dipulihkan kembali dan proses pemulihan yang dilakukan memerlukan pemahaman yang mendalam mengenai kaedah bagaimana hendak memulihkan data tersebut. Sistem pemulihan data ini mempunyai kaedah atau proses yang tersendiri bagi memulihkan data yang dipadam. Di dalam sesuatu penyiasatan forensik, proses pemulihan data perlu jelas kerana ia akan digunakan sebagai salah satu cara pengumpulan bukti untuk dikemukakan kepada mahkamah. Justeru, model proses pemulihan data perlu dijelaskan supaya ianya sah digunakan di dalam perbicaraan. Objektif kertas kerja ini adalah untuk membentangkan satu model yang dibangunkan dan proses-proses terlibat bagi memulihkan data yang telah dipadam. Selain dari itu, kertas kerja ini akan menerangkan secara teknikal bagaimana sesuatu sistem pemulihan data beroperasi.

Kata kunci: *Sistem pemulihan data, forensik komputer, jenayah*

Pengenalan

Sejak kebelakangan ini, jenayah komputer semakin berkembang kesan dari perkembangan ICT yang menyeluruh di seluruh dunia. Selain itu jenayah komputer semakin berkembang kerana komputer amat mudah untuk didapati dan harganya adalah amat murah berbanding 20 tahun dahulu. Bagi mengatasi masalah yang semakin meruncing ini, organisasi bukan kerajaan di seluruh dunia telah menubuhkan organisasi-organisasi yang memantau isu keselamatan komputer seperti NISER di Malaysia, CFI di Amerika Syarikat dan lain-lain lagi di serata dunia. Penubuhan organisasi ini adalah bertujuan bagi mengenal pasti kaedah-kaedah yang boleh diguna pakai bagi mengatasi dan membanteras jenayah komputer. Di samping itu, pihak kerajaan juga telah memainkan peranan yang penting dalam isu ini dengan mewujudkan akta berkaitan jenayah komputer bagi menghadapinya. Malah di negara kita Malaysia, akta jenayah komputer telah digubal pada tahun 1998 sebagai garis panduan dan undang-undang bagi membawa penjenayah komputer ke muka pengadilan. Kebiasaannya, bukti-bukti jenayah komputer diperolehi daripada komputer melalui kaedah forensik komputer dan boleh dikesan dari cakera, pelayan rangkaian dan peralatan rangkaian.

Kes-kes jenayah komputer dapat diselesaikan dengan menggunakan kaedah komputer forensik dengan pengumpulan maklumat di mana maklumat ini akan dianalisis dan dikemukakan ke mahkamah bagi pembuktian fakta kes. Ia adalah penting apabila menjalankan komputer forensik, bukti-bukti tersebut hendaklah bebas dari pengubahsuaian, virus dan kerosakan. Bagi melakukan analisis dengan baik, perkara yang pertama untuk dilakukan adalah pemuliharaan bukti yang dikumpulkan dari komputer. Pemuliharaan bukti ini adalah penting bagi memastikan ketelusan dan keselamatan maklumat tersebut. Kaedah yang terbaik untuk proses ini adalah dengan menggunakan alatan analisis data. Contoh alatan analisis yang terdapat di pasaran pada masa sekarang adalah seperti EnCase, TCT, Slueth Kit, Undeleete, Search and Recover dan pelbagai lagi.

Latar Belakang

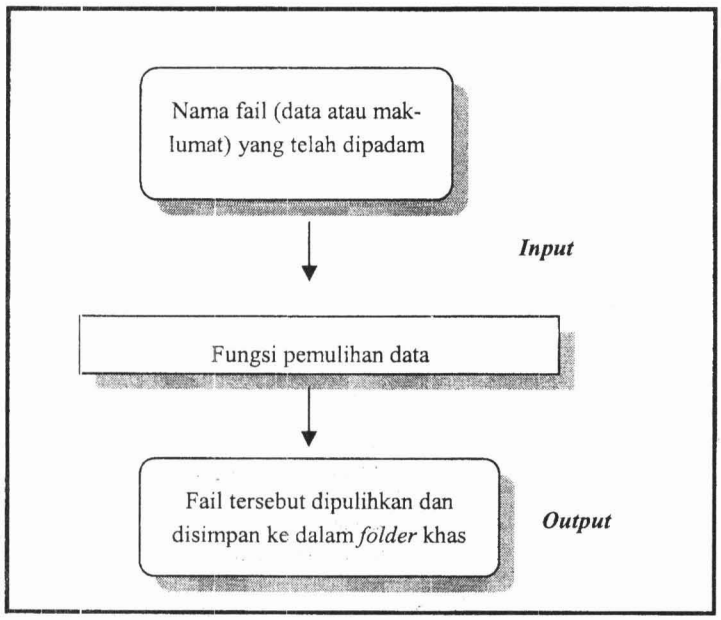
Jika kita melayari Internet, kita sering terbaca artikel yang berkaitan dengan keselamatan komputer. Artikel-artikel ini membincangkan konsep-konsep dan kaedah-kaedah yang terkandung di dalam bidang keselamatan komputer. Antara isu semasa yang sedang hangat diperbincangkan adalah berkaitan dengan forensik komputer. Forensik komputer adalah merupakan satu kaedah yang digunakan oleh penyiasat atau penganalisis keselamatan komputer bagi mendapatkan bukti-bukti jenayah yang boleh diperolehi daripada komputer. Bukti-bukti jenayah boleh diperolehi daripada pelbagai komponen dan media komputer seperti cakera, pita magnetik, peralatan rangkaian, email dan pelbagai komponen lagi.

Bukti yang diperolehi daripada kaedah forensik komputer ini amat berguna kepada pihak pendakwa jenayah, institut kewangan, syarikat insurans, syarikat korporat, penguat kuasa undang-undang dan individu yang boleh

menggunakan bukti jenayah yang dapat dikemukakan oleh penganalisis komputer forensik. Terdapat banyak pecahan bidang di dalam komputer forensik. Antara bidang yang sering menjadi tumpuan untuk penyelidikan adalah di dalam bidang forensik cakera. Forensik cakera digunakan bagi mendapatkan bukti-bukti yang boleh diperolehi daripada cakera. Bagi memperoleh bukti-bukti yang diperolehi daripada cakera, penganalisis forensik komputer akan menggunakan satu perisian forensik yang boleh mencari maklumat dan mendapatkan kembali data daripada komputer tanpa mengubahsuai data di dalam fail tersebut.

Konsep untuk tidak mengubah data asal yang diperolehi daripada komputer adalah merupakan prinsip utama di dalam penganalisisan komputer forensik dan perisian yang digunakan hendaklah mempunyai fungsi ini bagi menjamin ketelusan bukti yang diperolehi. Salah satu konsep utama di dalam forensik cakera adalah mengenai data yang telah dipadam daripada komputer secara teorinya boleh diperolehi kembali melalui kaedah forensik. Secara realitinya apabila data telah dipadam daripada komputer, ia tidak dipadam secara fizikal seperti kita memadam tulisan yang ditulis dengan pensel. Sebenarnya apa yang berlaku adalah hanya rujukan kepada lokasi data (dalam cakera atau media lain) telah dibuang. Oleh yang demikian, data tersebut masih berada di dalam cakera tetapi sistem pengoperasian kepada komputer tersebut tidak "mengetahui" mengenai data tersebut. Dengan menggunakan kaedah pengimbasan dan penganalisisan data terhadap cakera tersebut adalah tidak mustahil untuk mendapatkan data yang telah dipadam secara sengaja atau tidak sengaja daripada cakera tersebut.

Proses Sistem Pemulihan Data



Rajah 1: Proses Sistem Pemulihan Data

Nama Fail Yang Hendak Dipulihkan

Proses pertama yang diperlukan di dalam rekabentuk sistem pemulihan data adalah keperluan nama fail bagi data yang ingin dipulihkan. Nama fail diperlukan sebagai input kerana ia memainkan peranan yang penting dalam proses pemulihan prototaip sistem ini. Pengguna perlu mengenal pasti nama fail yang hendak dipulihkan dan perlu dimasukkan ke dalam kotak dialog yang disediakan pada antaramuka prototaip sistem yang dibangunkan.

Fungsi Pemulihan Data

Bahagian yang terpenting di dalam rekabentuk sistem pemulihan data adalah fungsi pemulihan data. Segala proses dan aktiviti pemulihan data terkandung di dalam bahagian ini. Ia dihasilkan melalui pengaturcaraan yang berinteraksi dengan sistem pengoperasian secara langsung.

Fail Yang Dipulihkan

Output yang dihasilkan oleh sistem ini adalah fail yang telah dipadamkan dari komputer telah dipulihkan. Fail yang

telah dipulihkan akan disimpan ke dalam folder tertentu yang telah ditetapkan oleh pengguna. Fail ini seterusnya akan dianalisis bagi mengetahui jenis sambungan fail tersebut dan selanjutnya kandungan kepada fail tersebut.

Rekabentuk Sistem Pemulihan Data

Secara ringkasnya rekabentuk sistem pemulihan data adalah seperti di dalam Rajah 2. Rekabentuk adalah berdasarkan kepada dua modul yang telah dikenal pasti iaitu Modul Imbasan dan Modul Pemulihan Data.

Setiap sub modul ini mempunyai fungsi-fungsi yang tersendiri dan berperanan dalam menjayakan perlaksanaan sistem pemulihan data bagi data yang telah dipadam. Penerangan mengenai fungsi dan perlaksanaan setiap modul ini akan dihuraikan dengan lebih lanjut di dalam bahagian seterusnya.

Modul Imbasan Fail

Modul ini berperanan untuk mengimbas fail-fail yang telah dipadam daripada sistem pengoperasian komputer. Pengimbasan perlu dilakukan untuk mengetahui nama fail-fail yang telah dipadam bagi dijadikan input untuk Modul Pemulihan Data. Proses yang dilakukan oleh modul ini akan digambarkan di dalam kod pseudo di dalam Rajah 3.

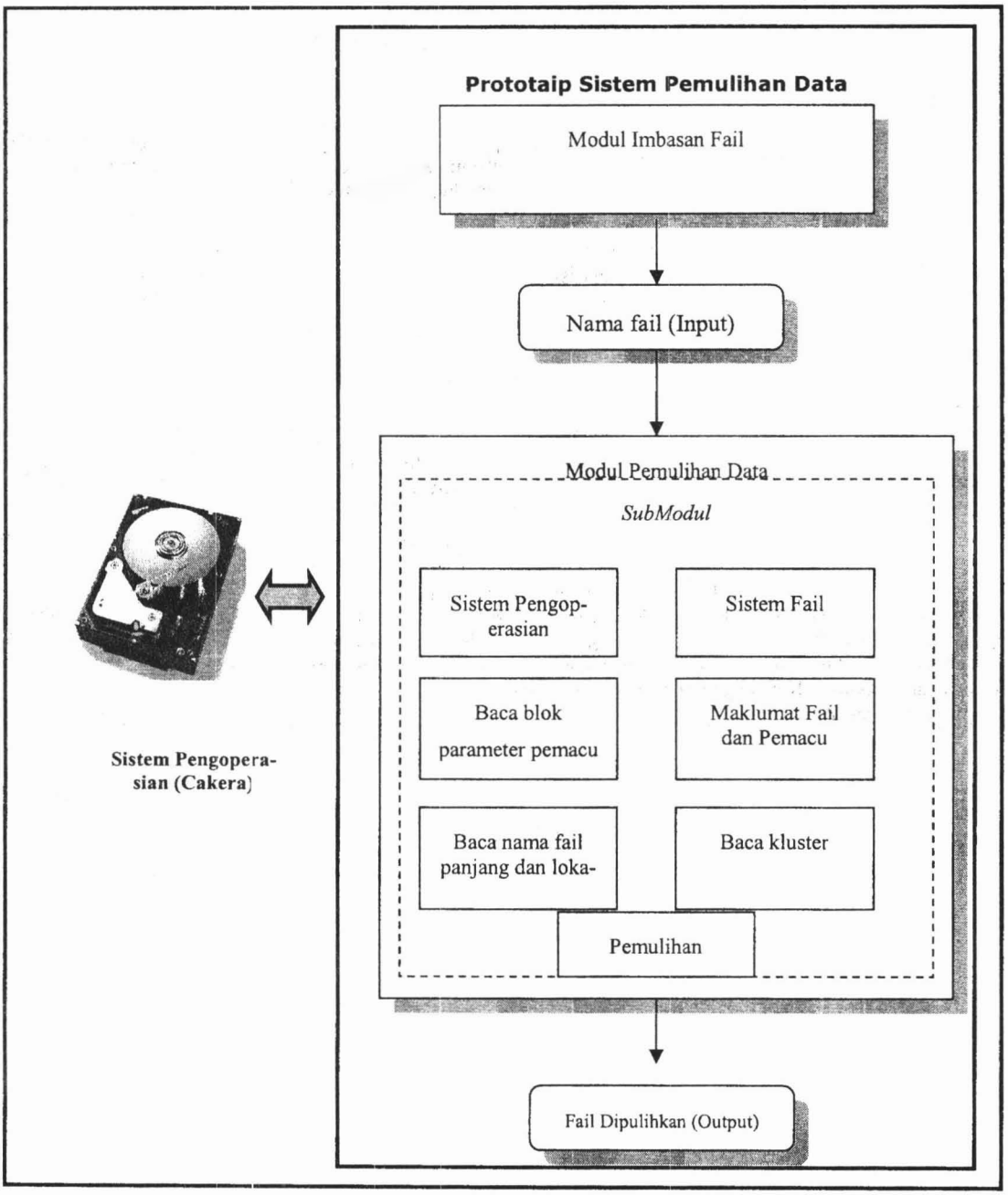
Modul ini berinteraksi dengan sistem pengoperasian Windows di mana segala arahan "Delete" yang berlaku akan direkodkan ke dalam satu fail log bagi merekodkan semua operasi "Delete" yang dilakukan. Semua maklumat mengenai fail yang telah dipadam tersebut akan disimpan seperti nama fail, direktori dan pemacunya. Ini bagi memudahkan proses pemulihan yang akan dilakukan sekiranya fail tersebut ingin dipulihkan kembali. Fail log tersebut akan diimbas bagi mendapatkan input yang diperlukan di dalam Modul Pemulihan Data.

Modul Pemulihan Data

Modul ini berperanan untuk memulihkan fail yang telah dipadam dari komputer dan memulihkannya kembali. Ia berperanan sebagai fungsi pemulihan data untuk sistem tersebut.

Input yang telah dimasukkan akan digunakan oleh fungsi ini untuk mengenal pasti dan mencari fail atau data yang telah dipadam. Hasil yang akan dikeluarkan adalah fail atau data yang telah dipadam akan dipulihkan kembali ke dalam bentuk yang asal dengan nama fail yang mengikut spesifikasi pengguna (Rujuk Rajah 4).

Modul ini berinteraksi secara langsung dengan sistem pengoperasian di mana ia akan mencapai maklumat di dalam jadual perletakan fail bagi mengenal pasti lokasi sektor di atas cakera di mana fail yang telah dipadam tadi disimpan. Apabila lokasi di mana fail yang telah dipadam tadi dikenal pasti, proses pemulihan akan dilaksanakan bagi memulihkan fail atau data yang telah dipadam. Modul ini merangkumi 7 proses utama yang dikategorikan sebagai sub modul. Keterangan mengenai sub modul-sub modul ini dan juga perangkaan kod pseudo akan diterangkan di bawah.



Rajah 2: Rekabentuk Prototaip Sistem Pemulihan

```
Fungsi Imbasan Fail
        Isytihar fail log
        Baca arahan Delete dari sistem pengoperasian Windows
        Jika arahan delete diaktifkan
                Rekod maklumat pemacu, direktori dan nama fail di dalam fail log
        Jika tidak
                Tiada
        Arahan imbas diaktifkan
        Papar maklumat di dalam fail log
Tamat Fungsi
```

```
Modul Pemulihan Data
        Aplikasi pemulihan data diaktifkan
        Input dimasukkan ke dalam kotak input
        Panggil Fungsi Periksa Sistem Pengoperasian
        Jika benar
                Panggil Fungsi Periksa Sistem Fail
                Jika benar
                        Panggil Fungsi Baca Blok Parameter Pemacu
                        Jika benar
                                Panggil Fungsi Maklumat Fail dan Pemacu
                                Panggil Fungsi Baca Nama Fail Panjang dan Lokasi Fail
                                Pendek
                                Panggil Fungsi Baca Kluster
                        Jika salah
                                Keluar
                Jika salah
                        Keluar
                Panggil Fungsi Pemulihan
                Proses pemulihan dilakukan
        Jika salah
                Keluar
Tamat Modul
```

Rajah 3: Kod Pseudo untuk Modul Imbasan Fail

Sub Modul Sistem Pengoperasian

Langkah pertama yang dilakukan oleh sistem pemulihan data apabila dilaksanakan adalah untuk mengenal pasti sistem pengoperasian yang digunakan oleh komputer. Tujuannya adalah untuk mengenal pasti sistem pengoperasian kerana sistem pemulihan data ini hanya dibangunkan khusus untuk sistem pengoperasian Windows ME ke bawah. Kod pseudo untuk fungsi sub modul ini seperti tertera di dalam Rajah 5. Sub modul ini memerlukan pengisytiharaan pembolehubah versi sistem pengoperasian yang digunakan.

```
Modul Pemulihan Data
        Aplikasi pemulihan data diaktifkan
        Input dimasukkan ke dalam kotak input
        Panggil Fungsi Periksa Sistem Pengoperasian
        Jika benar
                Panggil Fungsi Periksa Sistem Fail
                Jika benar
                        Panggil Fungsi Baca Blok Parameter Pemacu
                        Jika benar
                                Panggil Fungsi Maklumat Fail dan Pemacu
                                Panggil Fungsi Baca Nama Fail Panjang dan Lokasi Fail
                                Pendek
                                Panggil Fungsi Baca Kluster
                        Jika salah
                                Keluar
                Jika salah
                        Keluar
                Panggil Fungsi Pemulihan
                Proses pemulihan dilakukan
        Jika salah
                Keluar
```

Rajah 4: Kod Pseudo Untuk Modul Pemulihan Data

```
Fungsi Periksa Sistem Pengoperasian
        Isytihar pembolehubah versi sistem pengoperasian
        Jika versi sistem pengoperasian sama dengan versi Windows 32
                Pulangkan Benar
        Jika tidak
                Pulangkan Salah
Tamat Fungsi
```

Rajah 5: Kod Pseudo Untuk Sub Modul Sistem Pengoperasian

Sub Modul Sistem Fail

Di dalam sub modul ini, sistem fail bagi sesuatu sistem pengoperasian akan diperiksa untuk memastikan bahawa ia menggunakan sistem fail FAT32. Perkara yang diperlukan di dalam sub modul ini adalah blok parameter pemacu. Jika blok parameter pemacu ini memberikan nilai yang kosong maka ia bukan menggunakan sistem fail FAT32. Kod psuedo untuk fungsi sub modul ini seperti tertera di dalam Rajah 6.

```
Fungsi Periksa Sistem Fail
        Tetapkan blok parameter pemacu = dapatkan blok parameter pemacu
        Jika blok parameter pemacu mempunyai nilai 0
                Pulangkan Salah
        Set byte buffer = saiz byte
        Panggil fungsi baca blok parameter pemacu
        Setkan buffer = 0
        Jika pemacu c sama dengan 0
                Pulangkan benar
        Jika tidak
                Pulangkan Salah
Tamat Fungsi
```

Rajah 6: Kod Pseudo Untuk Sub Modul Sistem Fail

Sub Modul Baca Blok Parameter Pemacu

Sub modul ini berfungsi untuk membaca blok parameter blok bagi pemacu yang digunakan untuk perlaksanaan sistem pemulihan data ini. Blok parameter ini perlu dibaca bagi mendapatkan maklumat yang akan digunakan di dalam fungsi sistem fail. Maklumat yang diperolehi daripada sub modul ini menentukan sama ada sistem fail tersebut adalah sistem fail FAT32 ataupun tidak. Kod psuedo untuk fungsi sub modul ini seperti tertera di dalam Rajah 7.

```
Fungsi Baca Blok Parameter Pemacu
        Isytihar register
        Isytihar struktur format blok parameter pemacu
        Isytihar keputusan
        Isytihar urus peranti
        Isytihar direktori perkataan
        Isytihar blok parameter pemacu
        Isytihar memori kosong
        Urus peranti = wujudkan fail vwin32
        Keputusan = kawalan input output peranti
        Tamat urus
                Pulangkan parameter pemacu
Tamat Fungsi
```

Rajah 7: Kod Pseudo Untuk Sub Modul Baca Blok Parameter Pemacu

Sub Modul Maklumat Fail dan Pemacu

Sub modul ini berfungsi untuk membaca maklumat fail dan pemacu yang digunakan untuk perlaksanaan sistem pemulihan data ini. Ia dilaksanakan untuk membaca direktori kepada jujukan fail yang pendek. Selain itu ia akan mencari maklumat untuk fail yang telah dipadam dengan karakter pertama telah dipadam. Operasi yang berlaku di dalam fungsi ini berdasarkan pengujian yang dilakukan terhadap bilangan kemasukan. Bilangan kemasukan ini diisytiharkan pada fungsi di mana:

```
((Blok parameter pemacu kluster mask + 1) * saiz blok parameter pemacu) / 32
```

Kod psuedo untuk fungsi sub modul ini seperti tertera di dalam rajah 8.

```
Fungsi Maklumat Fail dan Pemacu
        Jika fail kosong
                Pulangkan Salah
        Isytihar pembilang = bilangan kemasukan
        Isytihar pembolehubah i dan flag = 0
        Sementara benar
                Panggil fungsi baca kluster
                Untuk i = 1
                        Dapatkan id untuk fail yang hendak dipulihkan
                        Dapatkan maklumat fail yang karektor pertamanya telah dipadam dan
                        digantikan dengan tanda "_"
Tamat fungsi
```

Rajah 8: Kod Pseudo Untuk Sub Modul Maklumat Fail dan Pemacu

Sub Modul Baca Nama Fail Panjang dan Lokasi Fail Pendek

Sub modul ini berfungsi untuk membaca nama fail panjang dan lokasi untuk fail yang pendek. Kod psuedo untuk fungsi sub modul ini seperti tertera di dalam Rajah 9.

```
Fungsi Baca Nama Fail Panjang dan Lokasi Fail Pendek
        Isytihar C ("")
        Isytihar pembolehubah b jenis char bersaiz 256
        Isytihar pembolehubah j = direktori kemasukan(a-1)
        Jika direktori kemasukan  tidak sama dengan 0
        Pulangkan C
Tamat fungsi
```

Rajah 9: Kod Pseudo Untuk Sub Modul Baca Nama Fail Panjang dan Lokasi Fail Pendek

Sub Modul Baca Kluster

Sub modul ini berfungsi untuk membaca kluster bagi mencari lokasi fizikal data atau fail yang telah dipadam di dalam cakera. Fungsi baca kluster ini berfungsi untuk mencari sektor permulaan dan sektor seterusnya. Maklumat ini adalah penting kerana ia akan menentukan kedudukan fizikal data atau fail tersebut di atas cakera. Kod psuedo untuk fungsi sub modul ini seperti tertera di dalam Rajah 10.

```
Fungsi Baca Kluster
        Isytihar register
        Isytihar struktur format blok parameter pemacu
        Isytihar input output cakera
                Isytihar blok parameter pemacu
        Isytihar sektor mula = kluster mula * (blok parameter pemacu +1)
        Isytihar sektor seterusnya = kluster seterusnya * (blok parameter pemacu + 1)
        Isytihar bilangan kluster = blok parameter pemacu kluster mask + 1
        Urus peranti = wujudkan fail vwin32
Tamat Fungsi
```

Rajah 10: Kod Pseudo Untuk Sub Modul Baca Kluster

Sub Modul Pemulihan

Sub modul ini berfungsi untuk memulihkan fail yang telah dipadam. Apabila fail tersebut telah dapat dicari menggunakan sub modul-sub modul sebelumnya, maka fungsi pemulihan ini akan memulihkan fail tersebut agar dapat dikenal pasti oleh sistem pengoperasian. Fungsi pemulihan ini akan mendapatkan nama fail dan kedudukan sektor. Kemudian fail tersebut akan dicipta sebagai fail yang baru dan dipindahkan mengikut spesifikasi pengguna. Kod psuedo untuk fungsi sub modul ini seperti tertera di dalam Rajah 11.

```
Fungsi Pemulihan
        Isytihar fail
        Isytihar pembolehubah j jenis long untuk saiz
        Isytihar saiz kluster =(blok parameter pemacu kluster mask + 1)* saiz
                blok parameter pemacu
        Cuba
                Panggil perpustakaan buka fail
        Perolehi
                Padam buffer cluster
                Pulangkan kosong
        Untuk proses pemulihan
                Jika lokasi dikenal pasti
                        Teruskan
                Pembolehubah j- = kluster
                Baca kluster
                Jika j kurang atau sama dengan 0
                        Panggil perpustakaan baca fail
                        Padam buffer cluster
                        Pulangkan nilai 1
                Jika tidak
                        Panggil perpustakaan baca fail
Tamat Fungsi
```

Rajah 11: Kod Pseudo Untuk Sub Modul Pemulihan

Perbincangan

Secara keseluruhannya apabila prototaip ini selesai dibangunkan, ia telah memenuhi keperluan di dalam objektif yang pertama di mana teknik-teknik yang dikaji di dalam kajian awalan telah memberikan satu pengetahuan yang menyeluruh bagaimana sesuatu teknik atau peralatan di dalam bidang forensik komputer. Walaupun dengan sumber dan maklumat yang terhad, kajian telah berjaya dilakukan dan hasil daripada kajian tersebut telah dijadikan panduan dalam pembangunan prototaip sistem pemulihan data ini. Namun terdapat beberapa aspek lagi yang perlu dikaji dengan lebih mendalam dari masa ke semasa kerana kepesatan pembangunan bidang forensik komputer dan pengkaji perlu lebih peka mengenainya.

Sumbangan yang dapat diberikan oleh kajian dan pembangunan prototaip sistem pemulihan data ini adalah dari segi penggunaan teknologi yang digunakan oleh pembangun sistem pemulihan data seperti Search and Recover, Encase, Active Undelete dan pelbagai lagi dapat dikenal pasti dan diketahui. Ini adalah kerana sebelum ini, semua perisian tersebut adalah merupakan perisian komersial dan maklumat mengenainya dilindungi dari pengetahuan umum. Dari hasil yang diperolehi dalam proses pengujian, sesuatu sistem pemulihan data itu dapat dibangunkan dari kajian yang mendalam dan bantuan teknologi pengaturcaraan yang ada pada masa sekarang. Untuk kes ini MFC digunakan di dalam pembangunan sistem dan ianya amat membantu dalam menjayakan kajian yang dilakukan.

Kajian ini mendapati untuk memulihkan data yang dipadam, ianya memerlukan pengaturcaraan yang boleh berinteraksi dengan sistem pengoperasian Windows. Ini adalah kerana perlunya mengetahui parameter direktori, bilangan kemasukan, saiz kluster dan pelbagai lagi bagi mencari fail yang telah dipadam dari komputer. Selain dari itu, kajian ini juga mendapati fail yang telah dipadam dari komputer akan bermula dengan tanda "_" dan ianya tidak dipadam secara terus dari komputer. Fail tersebut masih ada dan perlu dicari untuk dipulihkan kembali.

Justeru itu, kajian ini boleh dijadikan sebagai rujukan kepada penyelidik yang ingin mengetahui dan memahami bagaimana proses pemulihan dilakukan. Kajian ini adalah merupakan langkah awal di dalam membangunkan satu perisian yang benar-benar boleh diguna pakai sebagai alat untuk forensik komputer. Antara kajian lanjutan yang boleh dilakukan terhadap sistem ini adalah seperti meningkatkan keberkesanan model bagi pengimbasan fail yang telah dipadam di mana pengguna tidak perlu memasukkan nama fail yang perlu dilakukan pada prototaip ini dan proses tersebut boleh dilakukan secara automatik apabila proses imbasan dilakukan. Pengguna boleh menjelajah direktori-direktori di dalam sistem pengoperasian dan melaksanakan imbasan pada mana-mana folder yang dikehendaki. Proses ini adalah lebih efisien dan memudahkan pengguna untuk memulihkan fail yang telah dipadam.

Kesimpulan

Secara kesimpulannya, kajian ini telah pun mencapai objektif dan memenuhi skop yang dicadangkan. Hasil dari kajian yang telah dilaksanakan menunjukkan bahawa proses pemulihan dapat dilakukan dan dibangunkan. Sistem ini diharap dapat memberikan pendedahan di dalam proses pemulihan data dan dapat diperkembangkan lagi. Pembangunan sistem ini diharapkan dapat memberi manfaat kepada penulis dan penyelidik yang seterusnya. Dengan adanya inisiatif untuk melakukan penyelidikan lanjutan, diharapkan agar sistem ini mampu untuk menjadi alat forensik komputer yang baik dan memenuhi piawaian forensik komputer antarabangsa. Potensi untuk melakukan kajian lanjutan untuk pemulihan data bagi forensik komputer adalah begitu memberangsangkan kerana bidang ini baru saja diketengahkan dan memerlukan para penyelidik yang mempunyai inisiatif untuk menyelidikinya.

Rujukan

Barba, M. (2001). *Computer Forensic Investigation.* Computer Forensic Service.

Barish, S. (2002). *Windows Forensics: A Case Study, Part One.* InFoucus. Security Focus.

Bates, J. (1997). *Fundamentals of Computer Forensics.* Forensic Computing. Retrieved on 5 July 2003. [On-line] Available: http://www.forensic-computing.com/archives/fundamentals.html

Carrier, B. (2002a). *Defining Digital Forensic Examination and Analysis Tools.* New York: Digital Forensic Research Workshop 2002.

Carrier, B. (2002b). *Open Source Digital Forensic Tools: The Legal Argument.* Astake: Laporan Tesis.
Carrier, B. (2002c). *Open Source Software in Digital Forensics.* Astake.

Casey, E. (2002). *Handbook Computer Crime Investigation.* San Diego: Academic Press: pp. 133 – 166.

Civie, V. dan Civie, R. (1998) *Future Technologies From Trends in Computer Forensic Science.*IEEE: pp. 105-108.

Computer Forensic International. (2002). *How Hard Disk Work.* CFI. Retrieved on 10 Julai 2003. [On-line] Available: http://www.computerforensicinternational.com.

Dewan Bahasa dan Pustaka. (1991). *Kamus Dwibahasa: Bahasa Inggeris – Bahasa Malaysia.* Ampang: Percetakan Dewan Bahasa dan Pustaka.

DIBS Computer Forensic (2002). *The History of Image Copying Technology.* Retrived on 10 Julai 2003. [On-line] Available: http://www.dibs.com/computerforensic.html.

Eckert, W. G. (1997). *Introduction to Forensic Sciences.* CRC Press.

Fan, R. (2002). *Data Recovery Possibilities and Forensics.* Ibas.

Farmer, D and Venema, W. (1999). *Computer Forensic Analysis Class.* Porcupine. Retrieved on 21Jun 2003. [On-line] Available: http //www.porcupine.org/forensics/handouts.html

Foster, K. and R Huber. (1997). *Judging Science: Scientific Knowledge and the Federal Courts.* MIT Press.

Guttman, B. (2003). *Computer Forensics Standards: Tool Testing and National Software Reference Library.* National Institute of Standard and Technology.

Heinonen, D. (2001). *Computer Forensics-The Criminal Advantage.*Version. Retrieved on 5 Julai 2003. [On-line] Available: http://www.firmeartforum.org/staff/daniel/compEvid01.pdf.

Holley, J. (1999) *Computer Forensics in the New Millennium.* SC Info Security Magazine. [On-line].

Holley, J. (2001). *Computer Forensics.* SC Info Security Magazine. [On-line].

Iolo Technologies, LLC. *Recover Deleted Pictures, Videos, Email Documents and Much More.* Retrieved on 15

Januari 2004. [On-line] Available: http://www.iolo_technologies.com

Kay, R. (2001). *Anatomy of a Hard Disk.* Computerworld. Retrieved on 10 Julai 2003.[On-line] Available: http:// www.computerworld.com

Madihah Mohd Saudi. (2002). *An Overview of Disk Imaging Tools in Computer Forensics.* NISER.

Morris, R. (2001). *Uncovering a User's Hidden Tracks.* IEEE: Laporan Tesis.

New Technologies Armor, Inc. *Computer Forensics Definition.* Forensic International. Retrieved on 5 Julai 2003. [On-line] Available: http : //www.forensics-intl.com/define.html

Noblett, M.G., Pollitt, M. M. dan Presley, L. A. (2000). *Recovering and Examining Computer Forensic Evidence.* Federal Bureau of Investigation: Forensic Science Communications.

PowerQuest Corporation. *Drive Image Pro White Paper Exact Imaging for Fast Windows Deployment.* Power Quest. Retrieved on 5 Julai 2003. [On-line] Available: http://www.powerquest.com/

Rivest, R. (1992). *The MD4 Message Digest Algorithm.* RFC 1320, MIT dan RSA Data Security, Inc.

Rohde, L. (2001). *Forensic Tools may play Role in Investigation.* CNN. Retrieved on 5 July 2003. [On-line] Available: http://www.cnn.com/2001/TECH/industry/09/12/tech.forensics.idg/index.htm.

Shinder, D. L. (2002). *Scene of The Cybercrime Computer Forensics Handbook.* United States: Syngress Shinder Books

Sommer, Peter. (2002). *Digital Evidence Emerging Problems in Forensic Computing.*

Venema, W. (2000). *File Recovery Techniques.* Retrieved on 5 July 2003. [On-line] Available: http://www.ddj.com/ documents/s=878/ddj0012h/0012h.htm.

ABD HADI ABD RAZAK, Jabatan Multimedia, Fakulti Teknologi Maklumat, Universiti Utara Malaysia, 06010 Sintok, Kedah. ahadiar@uum.edu.my