SISTEM PEMULIHAN DATA: ALAT FORENSIK CAKERA MENGGUNAKAN TEKNIK IMBASAN CAKERA UNTUK SISTEM PENGOPERASIAN WINDOWS (FAT 32)

ABD HADI ABD RAZAK

UNIVERSITI TEKNOLOGI MALAYSIA

UNIVERSITI TEKNOLOGI MALAYSIA

BORANG PENGESAHAN STATUS TESIS♦

JUDUL: SISTEM PEMULIHAN DATA: ALAT FORENSIK CAKERA MENGGUNAKAN TEKNIK IMBASAN CAKERA UNTUK SISTEM PENGOPERASIAN WINDOWS (FAT 32)

SESI PENGAJIAN: 2003/2004

Saya ABD HADI BIN ABD RAZAK

mengaku membenarkan tesis (~~PSM~~/Sarjana/~~Doktor Falsafah~~)* ini disimpan di perpustakaan Universiti Teknologi Malaysia dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Teknologi Malaysia.
2. Perpustakaan Universiti Teknologi Malaysia dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran di antara institut pengajian tinggi.
4. ** Sila tandakan (✓)

☐	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau Kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
☐	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)
☑	TIDAK TERHAD	

Disahkan oleh

_____	_____
(TANDATANGAN PENULIS)	(TANDATANGAN PENYELIA)
Alamat Tetap:	
226, JALAN UNIVERSITI 7	PROF MADYA DR. SHAMSUL
TAMAN UNIVERSITI	SAHIBUDDIN
06010 SINTOK	Nama Penyelia
KEDAH	
Tarikh: Mac 2004	Tarikh: Mac 2004

CATATAN: * Potong yang tidak berkenaan

** Jika tesis ini SULIT atau TERHAD, sila lampirkan dari pihak berkuasa/organisasi berkenaan dengan mengatakan sekali sebab dan tempoh tesis ini perlu dikelaskan sebagai SULIT dan TERHAD.

♦ Tesis dimaksudkan sebagai tesis bagi Ijazah Doktor Falsafah dan Sarjana secara Penyelidikan atau disertasi bagi pengajian secara kerja kursus dan penyelidikan, Laporan Projek Sarjana Muda (PSM)

"Saya akui bahawa saya telah membaca karya ini dan pada pandangan saya karya ini adalah memadai dari segi skop dan kualiti untuk tujuan penganugerahan ijazah Sarjana Sains (Sains Komputer)"

Tandangan : ……..……

Nama Penyelia I: PROF MADYA DR. SHAMSUL SAHIBUDDIN

Tarikh : MAC 2004

SISTEM PEMULIHAN DATA: ALAT FORENSIK CAKERA MENGGUNAKAN TEKNIK IMBASAN CAKERA UNTUK SISTEM PENGOPERASIAN WINDOWS (FAT 32)

ABD HADI ABD RAZAK

Laporan Projek ini dikemukakan
sebagai memenuhi sebahagian daripada syarat
penganugerahan ijazah
Sarjana Sains (Sains Komputer)

Fakulti Sains Komputer dan Sistem Maklumat
Universiti Teknologi Malaysia

MAC, 2004

"Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang tiap-tiap satunya telah saya jelaskan sumbernya".

Tandangan : ……...

Nama Penulis : ABD HADI ABD RAZAK

Tarikh : MAC 2003

Teristimewa buat keluarga tersayang,
terima kasih atas dorongan dan doa kalian

Untuk Tunang tersayang, Ijan,
para pendidik sekalian,
serta rakan-rakan seperjuangan

Terima kasih untuk segalanya

PENGHARGAAN

Alhamdulillah, syukur ke hadrat Ilahi di atas segala rezeki dan kesempatan yang dikurniakan kepada saya sepanjang melaksanakan Projek Sarjana pada sesi 2003/2004.

Saya ingin merakamkan setinggi-tinggi penghargaan kepada Prof. Madya Dr. Shamsul Sahibuddin selaku penyelia projek di atas bimbingan dan tunjuk ajar beliau sepanjang tempoh kajian projek ini dijalankan. Kebijaksanaan bimbingan dan nasihat beliau telah mendorong saya untuk menyiapkan projek ini dengan penuh yakin.

Penghargaan juga ditujukan kepada semua pensyarah–pensyarah yang terlibat yang nama mereka tidak disertakan sama ada secara langsung atau tidak dalam menjayakan projek penyelidikan ini. Akhir sekali setinggi-tinggi penghargaan kepada ibu bapa dan keluarga saya serta rakan-rakan seperjuangan yang turut memberi dorongan.

ABSTRAK

Kajian ini dijalankan bertujuan untuk memahami bidang forensik komputer yang sedang hangat diperkatakan sebagai konsep keselamatan komputer. Forensik komputer telah menjadi bidang yang penting kepada pihak penguatkuasa undang-undang bagi membawa penjenayah komputer dan siber ke muka pengadilan. Pada masa kini jenayah yang dilakukan oleh penjenayah bukan sahaja bersifat fizikal seperti merompak, membunuh, mencuri dan sebagainya. Malah pada masa sekarang, komputer dijadikan alat untuk melakukan sesuatu jenayah. Forensik komputer diperlukan bagi mengesan dan mendapatkan bukti jenayah tersebut. Antara kaedah yang sering digunakan oleh penganalisis forensik bagi mendapatkan bukti adalah melalui kaedah forensik cakera. Kaedah forensik cakera ini dilakukan menerusi teknik imbasan cakera. Kajian yang dijalankan bertujuan untuk mendapatkan fail atau data yang telah dipadam dari komputer dan kemudian dipulihkan. Objektif kajian ini adalah untuk mengetahui bagaimana data yang telah dipadam tersebut dapat dipulihkan dan kemudiannya dijadikan bahan bukti jika terdapat unsur-unsur jenayah di dalamnya. Satu prototaip sistem pemulihan data akan dibangunkan bagi mengimplementasikan kaedah dan teknik yang dijelaskan di dalam kajian ini.

ABSTRACT

The purpose of this study is to understand the field of computer forensics that has been discussed lately through the computer security concept. Computer forensics is an important field for law enforcement agencies because it can be used to bring computers or cyber criminals to court. At this moment, crime does not only involve the physical-based crimes such as robbery, killing, stealing and others, but also involve computers as a medium in doing crime. Computer forensics is needed to determine and detect evidence of computer crime. Methods being used by forensic analysts today are to gather the evidence by using disk forensic. One of these techniques is through data recovery. This study has been done to recover deleted files or data from a computer. The main objective of this study is to determine how the data or file that has been deleted can be recovered and then to determined whether it is evidence or not. A recovering system prototype has been implemented using method and technique described in this research.

KANDUNGAN

BAHAGIAN DUA
KAJIAN LITERATUR

BAB II KAJIAN LITERATUR

BAHAGIAN TIGA

METODOLOGI

BAB III METODOLOGI

BAHAGIAN EMPAT

REKABENTUK DAN KEPERLUAN SISTEM

BAB IV REKABENTUK DAN KEPERLUAN SISTEM

BAHAGIAN TUJUH
RUJUKAN

BAHAGIAN LAPAN
LAMPIRAN

SENARAI JADUAL

SENARAI RAJAH

SENARAI SINGKATAN

CFI	Computer Forensic International
CPU	Central Processing Unit
CRC	Cyclical Redundancy Checksum
CSI	Crime Scene Investigation
FAT	File Allocation Table
FBI	Federal Bureau Investigation
Gb	Gigabyte
HDD	High Double Density
Kb	Kilobyte
Mb	Megabyte
MD	Message Digest
MFC	Microsoft Foundation Class
MFT	Master File Table
NISER	National Security Malaysia
NTFS	New Technology File System
PC	Personal Computer
RAM	Random Access Memory
RAMAC	Random, Access, Method of Accounting And Control
UML	Unified Modeling Language
USB	Universal Bus
VFAT	Virtual File Allocation Table

SENARAI LAMPIRAN

BAB I

BAB I

PENGENALAN

1.1 Pengenalan

Sejajar dengan perkembangan dunia IT yang semakin pesat membangun pada masa kini, pelbagai aplikasi dan perisian telah dibangunkan bagi menyokong keperluan hidup manusia yang semakin rumit. Bagi mereka yang mengambil jalan mudah untuk berjaya, komputer telah dieksploitasi dan disalahgunakan bagi merealisasikan matlamat itu. Maka wujudlah kes-kes jenayah komputer seperti penjualan maklumat organisasi, capaian bahan lucah, perisikan dan lain-lain lagi.

Sejak kebelakangan ini, jenayah komputer semakin berkembang kesan dari perkembangan ICT yang menyeluruh di seluruh dunia. Selain itu jenayah ini 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

The contents of the thesis is for internal user only

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. http://www.forensic-computing.com/archives/fundamentals.html (5 Julai 2003).

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. 133 – 166.

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

Computer Forensic International. (2002). “How Hard Disk Work.” CFI. http://www.computerforensicinternational.com (10 Julai 2003).

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.” http://www.dibs.com/computerforensic.html (10 Julai 2003).

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. http://www.porcupine.org/forensics/handouts.html (21 Jun 2003).

Foster, K., 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. http://www.fineartforum.org/staff/daniel/compEvid01.pdf (5 Julai 2003).

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

Holley, J. (2001). “Computer Forensics.” On-line SC Info Security Magazine.

Iolo Technologies, LLC. “Recover Deleted Pictures, Videos, Email Documents and Much More”.
http://www.iolo_technologies.com (15 Januari 2004).

Kay, R. (2001). “Anatomy of a Hard Disk.” Computerworld.
http://www.computerworld.com (10 Julai 2003).

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.
http ://www.forensics-intl.com/define.html (5 Julai 2003).

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.
http://www.powerquest.com/ (5 Julai 2003).

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.
http://www.cnn.com/2001/TECH/industry/09/12/tech.forensics.idg/index.htm
(5 Julai 2003).

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.”
http://www.ddj.com/documents/s=878/ddj0012h/0012h.htm (5 Julai 2003).