

**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  
MENGUNAKAN 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  
TAMAN UNIVERSITI  
06010 SINTOK  
KEDAH

PROF MADYA DR. SHAMSUL  
SAHIBUDDIN

Nama Penyelia

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)”

Tandatangan : .....

Nama Penyelia I: PROF MADYA DR. SHAMSUL SAHIBUDDIN

Tarikh : MAC 2004

**SISTEM PEMULIHAN DATA: ALAT FORENSIK CAKERA  
MENGUNAKAN 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”.

Tandatangan : .....

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

<b>BAB</b>	<b>PERKARA</b>	<b>MUKASURAT</b>
	<b>JUDUL</b>	i
	<b>PENGAKUAN</b>	ii
	<b>DEDIKASI</b>	iii
	<b>PENGHARGAAN</b>	iv
	<b>ABSTRAK</b>	v
	<b>ABSTRACT</b>	vi
	<b>KANDUNGAN</b>	vii
	<b>SENARAI JADUAL</b>	xiv
	<b>SENARAI RAJAH</b>	xv
	<b>SENARAI SINGKATAN</b>	xviii
	<b>SENARAI LAMPIRAN</b>	xix

## BAHAGIAN SATU

### PENGENALAN

<b>BAB I</b>	<b>PENGENALAN</b>	
	1.1 Pengenalan	1
	1.2 Latar Belakang Kajian	3
	1.3 Penyataan Masalah	6
	1.4 Objektif Kajian	7

1.5	Skop Kajian	8
1.6	Kesimpulan	10

## **BAHAGIAN DUA KAJIAN LITERATUR**

### **BAB II KAJIAN LITERATUR**

2.1	Pengenalan	11
2.2	Forensik Komputer	12
2.2.1	Metodologi Forensik Komputer	16
2.2.1.1	Pengumpulan Data	17
2.2.1.2	Analisis Data	18
2.2.1.3	Persembahan Data	19
2.3	Cabang Forensik Komputer	20
2.3.1	Forensik Cakera	22
2.4	Anatomi Cakera Keras	23
2.4.1	Prinsip Asas Perakaman Magnetik	27
2.4.2	Bagaimana Data Di Simpan Di Dalam Cakera	28
2.4.3	Bagaimana Data Di Padam Dari Cakera Keras	30
2.5	Sistem Fail	31
2.5.1	FAT12	33
2.5.2	FAT16	34
2.5.3	VFAT	35
2.5.4	FAT32	35
2.5.5	NTFS	36
2.6	Teknik Pemulihan Forensik Cakera	37
2.6.1	Imbasan Cakera	40
2.6.2	Analisis Cakera	42

2.7	Prosedur Forensik Cakera untuk Sistem Pengoperasian Windows	43
2.7.1	Fail yang Dipadam dari Sistem Microsoft FAT.	43
2.7.2	Ruang Perlokasian dan Penyahlokasian	45
2.7.3	Operasi Fail	47
2.8	Contoh Aplikasi Pemulihan Data <i>Search and Recover</i>	49
2.9	Kesimpulan	52

## **BAHAGIAN TIGA METODOLOGI**

### **BAB III METODOLOGI**

3.1	Pengenalan	53
3.2	Metodologi Pembangunan Sistem	54
3.3	Fasa-Fasa Pembangunan Sistem	56
3.3.1	Fasa Analisa Keperluan	57
3.3.1.1	Sumber Sekunder	58
3.3.2	Fasa Rekabentuk	58
3.3.2.1	Pendekatan Orientasi Objek	59
3.3.2.2	UML – Unified Modelling Language	59
3.3.2.3	Konsep Unified Modeling Language	61
3.3.2.4	Rajah Kes Guna ( <i>Use Case Diagram</i> )	61
3.3.2.5	Rajah Jujukan ( <i>Sequence Diagram</i> )	62

3.3.3	Fasa Pembangunan	62
3.3.3.1	Perisian	63
3.3.3.2.1	Microsoft Visual C++	63
3.3.3.2	Perkakasan	64
3.3.4	Fasa Pengujian dan Penyelenggaraan	64
3.4	Kesimpulan	65

## **BAHAGIAN EMPAT REKABENTUK DAN KEPERLUAN SISTEM**

### **BAB IV REKABENTUK DAN KEPERLUAN SISTEM**

4.1	Pengenalan	66
4.2	Rekabentuk Prototaip	67
4.2.1	Nama Fail Yang Hendak Dipulihkan	68
4.2.2	Fungsi Pemulihan Data	69
4.2.3	Fail Yang Dipulihkan	69
4.3	Rekabentuk UML	69
4.3.1	Rajah Kes Guna	70
4.3.2	Rajah Jujukan	72
4.4	Keperluan Rekabentuk Prototaip	72
4.4.1	Keperluan Pengguna	73
4.4.2	Keperluan Antaramuka	73
4.4.3	Keperluan Perisian	73
4.4.3.1	Sistem Pengoperasian	74
4.4.3.2	Perisian Pengaturcaraan	74
4.4.3.3	Perisian Lain	75
4.4.4	Keperluan Perkakasan	75
4.4.5	Spesifikasi Input, Proses dan Output	76

4.4.5.1	Spesifikasi Input	76
4.4.5.2	Spesifikasi Proses	76
4.4.5.3	Spesifikasi Output	77
4.5	Rekabentuk Pembangunan Prototaip	77
4.5.1	Modul Imbasan Fail	79
4.5.2	Modul Pemulihan Data	80
4.5.2.1	Sub Modul Sistem Pengoperasian	81
4.5.2.2	Sub Modul Sistem Fail	82
4.5.2.3	Sub Modul Baca Blok Parameter Pemacu	82
4.5.2.4	Sub Modul Maklumat Fail dan Pemacu	83
4.5.2.5	Sub Modul Baca Nama Fail Panjang dan Lokasi Nama Fail Pendek	84
4.5.2.6	Sub Modul Baca Kluster	85
4.5.2.7	Sub Modul Pemulihan	85
4.6	Kesimpulan	86

**BAHAGIAN LIMA**  
**IMPLEMENTASI SISTEM DAN HASIL**  
**PROJEK**

**BAB V    PEMBANGUNAN SISTEM DAN**  
**PENGUJIAN PROJEK**

5.1	Pengenalan	88
5.2	Microsoft Foundation Class(MFC)	89
5.3	Implementasi Sistem	90
5.3.1	Antaramuka Menu Prototaip	91
5.3.2	Aplikasi Imbasan Fail	92

5.3.3	Aplikasi Periksa Sistem Pengoperasian	93
5.3.4	Aplikasi Periksa Sistem Fail	93
5.3.5	Aplikasi Baca Blok Parameter Pemacu	94
5.3.6	Aplikasi Periksa Maklumat Fail dan Pemacu	95
5.3.7	Aplikasi Baca Nama Fail Panjang dan Lokasi Nama Fail Pendek	97
5.3.8	Aplikasi Baca Kluster	98
5.3.9	Aplikasi Pemulihan	99
5.4	Pengujian dan Analisa Prototaip	100
5.4.1	Pengujian Pertama	100
5.4.2	Pengujian Kedua	104
5.4.3	Analisa Hasil	109
5.5	Kesimpulan	110

## **BAHAGIAN ENAM**

### **PERBINCANGAN DAN KESIMPULAN**

#### **BAB VI PERBINCANGAN DAN KESIMPULAN**

6.1	Pengenalan	111
6.2	Perbincangan	112
6.3	Kebolehan Sistem	114
6.4	Kekangan Sistem	115
6.5	Sumbangan Kajian	116
6.6	Kajian Lanjutan	117
6.7	Kesimpulan	118

**BAHAGIAN TUJUH  
RUJUKAN**

RUJUKAN 120

**BAHAGIAN LAPAN  
LAMPIRAN**

LAMPIRAN A-E 123-150



**SENARAI JADUAL**

<b>NO. JADUAL</b>	<b>TAJUK</b>	<b>MUKASURAT</b>
2.0	Penerangan Cabang Forensik Cakera	21
2.1	Konsep Asas Pemacu	26
2.2	Sistem Pengoperasian Windows dan Korelasi Sistem Fail	32
3.0	Cara Notasi UML Menyokong Pandangan- Pandangan Dalam Proses Pembangunan Perisian.	60
5.0	Fungsi Fail Aplikasi Yang Dicipta Secara Automatik Oleh AppWizard	90

**SENARAI RAJAH**

<b>NO. RAJAH</b>	<b>TAJUK</b>	<b>MUKASURAT</b>
2.0	Statistik Jenis Serangan Dan Jenayah Di Amerika Syarikat Untuk Tahun 2001	13
2.1	Model Piawaian	16
2.2	Hubung Kait Antara Ketelusan Bukti Dan Keperluan Sumber	17
2.3	Metodologi Forensik Komputer	19
2.4	Cabang Forensik Komputer	20
2.5	Cakera Keras	23
2.6	Komponen Cakera Keras	24
2.7	Bagaimana Cakera Keras Berfungsi	25
2.8	Organisasi Logikal Dan Fizikal Pemacu	26
2.9	Proses Menulis Ke Dalam Cakera Keras	28
2.10	Pecahan Cakera Di Dalam Cakera Keras	29
2.11	FAT Dan Direktori <i>Entry</i>	30
2.12	FAT Dan Direktori <i>Entries</i> Apabila Fail Dipadam	31
2.13	Kedudukan Sektor Di Atas Cakera	38
2.14	Aplikasi <i>Search and Recover</i>	49
3.0	Mengimplementasikan Sistem Pemulihan Data Ke Dalam Model Prototaip	55

3.1	Fasa-Fasa Yang Terlibat Dalam Pembangunan Sistem	56
3.2	Aktiviti Analisis Sistem	57
3.3	Pandangan-Pandangan Dalam Senibina Perisian	60
3.4	Rajah Ringkas Kes Guna Sistem Pemulihan Data	62
3.5	Aktiviti Implementasi Dan Pengujian	65
4.0	Rekabentuk Rangka Kerja Untuk Prototaip Sistem Pemulihan Data	67
4.1	Rekabentuk Prototaip Sistem Pemulihan	78
4.2	Kod Pseudo Untuk Modul Imbasan Fail	79
4.3	Kod Pseudo Untuk Modul Pemulihan	80
4.4	Kod Pseudo Untuk Sub Modul Sistem Pengoperasian	81
4.5	Kod Pseudo Untuk Sub Modul Sistem Fail	82
4.6	Kod Pseudo Untuk Sub Modul Baca Blok Parameter Pemacu	83
4.7	Kod Pseudo Untuk Sub Modul Maklumat Fail dan Pemacu	84
4.8	Kod Pseudo Untuk Sub Modul Baca Nama Fail Panjang dan Lokasi Fail Pendek	84
4.9	Kod Pseudo Untuk Sub Modul Baca Kluster	85
4.10	Kod Pseudo Untuk Sub Modul Pemulihan	86
5.0	Antaramuka Menu Prototaip Sistem Pemulihan Data	91
5.1	Antaramuka Imbasan Fail	92
5.2	Keratan Aturcara Untuk Aplikasi Imbasan Fail	92
5.3	Keratan Aturcara Untuk Aplikasi Sistem Pengoperasian	93
5.4	Keratan Aturcara Untuk Aplikasi Periksa Sistem Fail	94

5.5	Keratan Aturcara Untuk Baca Blok Parameter Pemacu	94
5.6	Keratan Aturcara Untuk Periksa Maklumat Fail dan Pemacu	95
5.7	Keratan Aturcara Untuk Aplikasi Baca Nama Fail Panjang dan Lokasi Fail Pendek	97
5.8	Keratan Aturcara Untuk Aplikasi Baca Kluster	98
5.9	Keratan Aturcara Untuk Aplikasi Pemulihan	99
5.10	Kandungan Fail tugas.txt	100
5.11	Fail tugas.txt Di Dalam <i>RecycleBin</i>	101
5.12	Fail tugas.txt Di Padam Dari <i>RecycleBin</i>	101
5.13	Prototaip Pemulihan Dilaksanakan	102
5.14	Fail Telah Dipulihkan	103
5.15	Aplikasi Untuk Membuka Fail Bukti	103
5.16	Kandungan Fail Bukti	104
5.17	Fail-Fail Di Dalam Folder test	104
5.18	Kandungan Fail-Fail	105
5.19	Fail –Fail Di Dalam <i>RecycleBin</i>	105
5.20	Fail-Fail Tersebut Di Padam Dari <i>RecycleBin</i>	105
5.21	Prototaip Pemulihan Dilaksanakan Pada Fail cubaan2.txt	106
5.22	Prototaip Pemulihan Dilaksanakan Pada Fail cubaan1.txt	107
5.23	Fail Telah Dipulihkan	107
5.24	Aplikasi Untuk Membuka Fail	108
5.25	Kandungan Fail Bukti2 dan Bukti 3	108

**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

LAMPIRAN	TAJUK	MUKASURAT
A1	Perancangan Perlaksanaan Projek I Sarjana Sains Komputer Prototaip Sistem Pemulihan Data	123
A2	Perancangan Perlaksanaan Projek II Sarjana Sains Komputer Prototaip Sistem Pemulihan Data	124-125
B1	Laman Web Aplikasi <i>Search and Recover</i> (1)	126
B2	Laman Web Aplikasi <i>Search and Recover</i> (2)	127
B3	Laman Web Aplikasi <i>Search and Recover</i> (3)	128
B4	Laman Web Aplikasi <i>Search and Recover</i> (4)	129
B5	Antaramuka Menu Utama Perisian <i>Search and Recover</i>	130
B6	Antaramuka Menu <i>File Rescue Wizard</i> Untuk Carian Jenis Fail	131
B7	Antaramuka Menu <i>File Rescue Wizard</i> Untuk Tempat Carian	132
B8	Antaramuka Menu <i>File Rescue Wizard</i> Untuk Proses Pemulihan	133
B9	Antaramuka Menu <i>File Rescue Wizard</i> Untuk Hasil Carian Proses Pemulihan	134

B10	Antaramuka Menu <i>Advanced Deleted File Search</i>	135
B11	Antaramuka Menu <i>Email Recovery</i>	136
B12	Antaramuka Menu <i>Security Tools</i>	137
B13	Antaramuka Menu <i>Working With Disk Images</i>	138
C1	Gambarajah Kes Guna Prototaip Sistem Pemulihan Data	139
C2	Diskripsi Ringkas Kes Guna Membuat Imbasan	140
C3	Diskripsi Ringkas Kes Guna Memulihkan Fail	141
C4	Diskripsi Ringkas Kes Guna Papar Fail	142
D1	Gambarajah Jujukan Membuat Imbasan	143
D2	Gambarajah Jujukan Memulihkan Fail	144
D3	Gambarajah Jujukan Papar Fail	145
E1	Manual Pengguna Prototaip Sistem Pemulihan Data	146

**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." InFocus. 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](http://www.iolo_technologies.com) (15 Januari 2004).

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

Madiah 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).