TEKNIK ANTI KOMPUTER FORENSIK UNTUK MEMANIPULASI FILE

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana
Jurusan Teknik Informatika

Oleh :

Nama : Dimas Mahendra Kusuma

No. Mahasiswa : 07 523 378

JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

2011

LEMBAR PENGESAHAN PEMBIMBING

TEKNIK ANTI KOMPUTER FORENSIK UNTUK MEMANIPULASI FILE

TUGAS AKHIR

Oleh :

Nama : Dimas Mahendra Kusuma

No. Mahasiswa : 07 523 378

Pembimbing

Yudi Prayudi. S.si, M.kom.

LEMBAR PENGESAHAN PENGUJI

TEKNIK ANTI KOMPUTER FORENSIK UNTUK MEMANIPULASI FILE

Oleh :

Nama : Dimas Mahendra Kusuma

No. Mahasiswa : 07 523 378

Telah Dipertahankan di Depan Sidang Penguji Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Jurusan Teknik Informatika
Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, Agustus 2011

Tim Penguji	**Tanda Tangan**
Ketua	
Yudi Prayudi, S.Si., M.Kom.	
Anggota I	
Syarif Hidayat, S.kom.,M.I.T.	
Anggota II	
R. Teduh Dirgahayu, ST., M.Sc., Ph.D.	

Mengetahui,
Ketua Jurusan Teknik Informatika
Universitas Islam Indonesia

(Yudi Prayudi, S.Si, M.Kom)

HALAMAN PERSEMBAHAN

Kupersembahkan Tugas Akhir Ini
Dengan Setulus Hatiku Untuk

Yang Tercinta, Terkasih dan Tersayang :
Ayahanda Abdullah, SH dan Ibunda Sri Susilowati
Kakakku Devi Rahmadhona dan Dewi Permata Sari
Serta Kekasihku Bella Dwi Saputri
Yang Selalu Memberikan Do'a, Semangat dan Dukungan
Yang Tada Hentinya Untuk Menyelesaikan Studiku

HALAMAN MOTTO

"Jadikanlah Dirimu Oleh Dirimu Sendiri"

"Hari ini Harus Lebih Baik dari Hari Kemarin dan Hari Esok Harus Lebih Baik dari Hari Ini"

KATA PENGANTAR

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيْمِ

Assalamu'alaikum Wr. Wb

Puji syukur Alhamdulillah penulis panjatkan kepada hadirat Allah SWT, yang telah memberikan rahmat, hidayah, dan karunia-Nya sehingga laporan tugas akhir dapat penulis selesaikan dengan baik. Serta tidak lupa untuk memanjatkan shalawat serta salam kepada junjungan kita Nabi Muhammad SAW yang menjadi panutan kita hingga akhir zaman.

Guna Tugas Akhir ini dibuat sebagai salah satu syarat yang nantinya diperlukan untuk memperoleh gelar sarjana di kampus tercinta yaitu Universitas Islam Indonesia Jurusan Teknik Informatika.

Tugas Akhir saya adalah Teknik anti komputer forensik, yang dimana teknik ini digunakan untuk usaha melindungin data-data pribadi dari orang-orang yang tidak baik, serta untuk kemajuan dari teknik komputer forensik itu sendiri. Dalam kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Allah SWT. Atas segala hidayah, barokah dan taufiq-Nya.
2. Bapak Ir. Gumbolo Hadi Susanto M.Sc, selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
3. Bapak Yudi Prayudi, S.Si, M.Kom, selaku ketua Jurusan Teknik Informatika, dan selaku dosen pembimbing Tugas Akhir yang telah memberikan pengarahan dan bimbingan selama pelaksanaan tugas akhir dan penulisan laporan ini.
4. Kedua orang tuaku Ayahanda Abdullah dan Ibunda Sri Susilowati, kedua kakakku Devi Rahmadhona dan Dewi Permata Sari, dan keluarga tercinta yang senantiasa memberikan doa dan dorongan semangat hingga selesainya tugas akhir ini.
5. Kekasih Tercintaku "Endut" yang telah memberikan doa dan motivasi selama mengerjakan tugas akhir.
6. Teman-teman seperjuangan Teknik Informatika angkatan 2007 "INCLUDE" yang tidak bisa disebutkan satu persatu.

Penulis menyadari bahwa penyusunan laporan ini masih belum sempurna, karena keterbatasan kemampuan dan pengalaman. Oleh karena itu penulis mengharapkan kritik dan saran yang membangun untuk membantu penulis di masa yang akan datang.

Akhir kata penulis berharap agar laporan ini dapat bermanfaat bagi semua pihak. Amin..

Wassalamu'alaikum Wr.Wb.

Yogyakarta, Agustus 2011

Penulis

SARI

Anti komputer forensik adalah adalah lawan dari bidang komputer forensik. Jika bidang komputer forensik menitik beratkan pada upaya mencari dan menemukan data, menjaga integritas data, bidang anti komputer forensik justru berfokus pada sisi sebaliknya: bagaimana data tetap aman, tetap tidak bisa diakses (kecuali oleh sang pemilik atau pembuat data tersebut).

Manipulasi File adalah sebuah proses rekayasa dengan melakukan penambahan, penyembunyian, penghilangan atau penghapusan terhadap bagian atau keseluruhan dari file-file yang ada didalam sebuah perangkat komputer.

Melakukan percobaan teknik anti komputer forensik untuk memanipulasi file tanpa bantuan dari software anti forensic dan melakukan manipulasi file dengan bantuan software anti forensik serta melakukan pengujian forensik untuk membandingkan hasil yang diperoleh dari percobaan tersebut.

Kata Kunci : Anti Komputer Forensik, Manipulasi File

TAKARIR

Timestamp	: Pencatatan Tanggal dan Waktu
Secure Delete	: Penghapusan secara aman
Data Recovery	: Pemulihan data
Data Restore	: Pengembalian data
History Cleaner	: Pembersihan jejak-jejak

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Komputer forensik adalah sebuah ilmu yang mengumpulkan dan menganalisa data dari berbagai sumber daya komputer, dengan menggunakan metode pengumpulan barang bukti dari sistem komputer mencakup : sistem komputer, jaringan, komputer dan juga berbagai media penyimpanan yang dikatakan layak untuk diajukan dalam sidang pengadilan. Serta mempertahankan, identifikasi, menafsirkan dan mendokumentasikan bukti-bukti komputer guna melengkapi persyaratan barang bukti, prosedur resmi, melaporkan informasi yang ditemukan dipengadilan [HAM10].

Anti komputer forensik adalah adalah lawan dari bidang komputer forensik. Jika bidang komputer forensik menitik beratkan pada upaya mencari dan menemukan data, menjaga integritas data, bidang anti komputer forensik justru berfokus pada sisi sebaliknya: bagaimana data tetap aman, tetap tidak bisa diakses (kecuali oleh sang pemilik atau pembuat data tersebut) [ARR10].

Penggunaan teknik anti forensik jika ditinjau dari sisi batasan waktu, bertujuan untuk menyulitkan pakar komputer forensik sehingga membutuhkan waktu dan proses yang jauh lebih lama untuk mencari data-data yang mereka butuhkan. Tentu yang paling ideal adalah jika data-data tersebut tidak berhasil ditemukan. Akan tetapi jika data tersebut berhasil ditemukan, maka harus diupayakan bahwa data tersebut sudah terganggu integritasnya.

Ditinjau dari sisi kelegalitasnya, tidak ada satu pasal pun dalam undang-undang ITE (informasi dan transaksi elektronik) yang melarang seseorang untuk mengedit filenya sendiri, menghapus filenya sendiri, menyembunyikan filenya sendiri, maupun merusak filenya sendiri. Sepanjang hal-hal tersebut tidak merugikan orang lain.

Permasalahan yang terjadi sekarang ini adalah banyak tersebarnya *software-software* komputer forensik didunia maya sehingga dapat diakses maupun di*download* dengan mudahnya. Padahal jika ditinjau dari penggunaannya *software* komputer forensik bersifat netral tergantung dari penggunanya (selain bisa digunakan untuk kebaikan juga bisa digunakan untuk kejahatan).

Dari permasalah diatas banyak orang dengan mudahnya mendapatkan *software* forensik. Akan tetapi jika penggunaan tidak sesuai dengan yang kegunaan aslinya akan membahayakan orang banyak, seperti : digunakan untuk mencari atau muncuri file-file pribadi orang lain, me*recovery* kembali file-file orang yang telah dihapus, memata-matai *history* maupun log dari penggunaan komputer seseorang, dan lain-lain.

Tidak ada salahnya untuk menggunakan *software* atau teknik anti komputer forensik untuk melindungi file-file pribadi. Dengan melakukan teknik anti forensik untuk manipulasi file tentu dapat membantu dalam melindungin file-file pribadi dan apabila file-file pribadi tersebut masih dapat ditemukan maka diusahakan untuk merusak integritasnya dengan melakukan pengubahan pada pencatatan timestamp di file tersebut. Selain itu teknik maupun *software* anti komputer forensik dapat menjadi tolak ukur seberapa baik atau buruknya *software-software* forensik dan mendorong para ahli forensik yang membuat *software* forensik yang lebih baik lagi.

1.2 Rumusan Masalah

Dari latar belakang dan dasar pemikiran di atas dapat dirumuskan permasalahan yang dihadapi yaitu bagaimana mempelajari dan mengimplementasikan teknik dan metode anti forensik yang benar dalam memanipulasi file seperti

a. Menyamarkan file
b. Menyamarkan timestamp file
c. Secure delete
d. History cleaner

1.3 Batasan Masalah

Teknik dalam mengatasi komputer forensik biasanya memiliki cakupan yang cukup luas untuk dibahas. Oleh karena itu, diperlukan adanya suatu pembatasan penyelesaian masalah. Berikut ini beberapa batasan masalah :

a. Aktivitas anti forensik yang akan diteliti : penyamaran file, penyamaran pencatatan waktu file, *secure delete*, dan *history cleaner*.
b. Untuk teknik penyamaran file hanya dapat menyamarkan file .exe dan .zip saja.

1.4 Tujuan Penelitian

Sesuai dengan judul diatas tujuan penggunaan *software-software* dan metode anti komputer forensik untuk :

a. Merusak integritas file agar tidak berlaku dijadikan sebagai barang bukti
b. Menghapus file yang dianggap sangat penting sehingga tidak dapat di*recovery* kembali
c. Menghapus jejak-jejak yang dibuat oleh sistem, aplikasi, maupun situs sehingga jejak-jejak tersebut tidak dapat diketehui oleh orang lain
d. Mengenali teknik-teknik anti komputer forensik sebagai saran untuk memajukan teknik komputer forensik.

1.5 Manfaat Penelitian

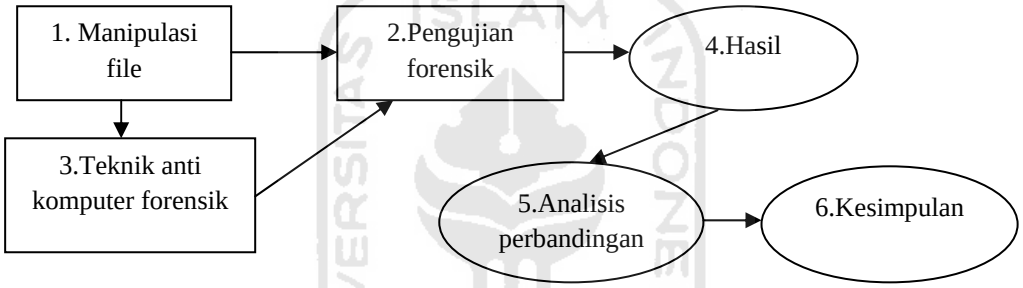
Manfaat yang diperoleh dalam mengerjakan penelitian atau tugas akhir adalah:

a. Dapat menggunakan teknik anti forensik untuk melindungin data-data pribadi yang ada dikomputer.
b. Mendorong perkembangan teknik komputer forensik yang lebih baik
c. Membuktikan bahwa barang bukti komputer rapuh, mudah berubah, dan dimanipulasi sehingga perlu diperbaiki untuk bisa dipakai secara layak di pengadilan.

d. Sebagai wacana untuk perumusan standar barang bukti pengadilan yang semakin lama semakin baik
e. Membuktikan bahwa otomatisasi dengan software forensik dengan mengabaikan aspek sisi sumber daya manusia berpotensi berbahaya karena alat bantu yang bersifat otomatis bisa dimanipulasi
f. Sebagai tolak ukur penilaian dari sebuah *tools* komputer forensik maupun *tools* anti komputer forensik.

1.6 Metodologi Penelitian

Metodologi yang akan digunakan seperti :



Gambar 1.1 Metodologi penelitian.

Penjelasan :

1. Melakukan menipulasi file secara sederhana.
2. Melakukan pengujian dengan menggunakan *software* komputer forensik.
3. Melakukan memanipulasi file dengan teknik dan bantuan *software* anti komputer forensik.
4. Hasil dari manipulasi file secara sederhana dan yang menggunakan teknik anti komputer forensik apakah gagal atau berhasil.
5. Melakukan analisis perbandingan teknik dan *software* yang digunakan.
6. Kesimpulan yang didapatkan setelah menggunakan teknik anti komputer forensik untuk memanipulasi file.

1.7 Sistematika Penulisan

Untuk mempermudah proses pembacaan dan memberikan gambaran secara menyeluruh masalah yang akan dibahas dalam laporan ini, maka laporan tugas akhir disajikan ke dalam lima bab.

BAB 1 Pendahuluan, pada bab ini membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan laporan.

BAB 2 Landasan Teori, pada bab ini membahas tentang teori-teori yang terkait dalam teknik anti komputer forensik.

BAB 3 Metodologi, pada bab ini membahas tentang metodologi yang akan digunakan dalam anti komputer forensik.

BAB 4 Hasil dan Pembahasan, pada bab ini berisi tentang tahap uji coba teknik anti komputer forensik, dan melihat efek dari *software* komputer forensik.

BAB 5 Kesimpulan dan Saran, pada bab ini berisi tentang kesimpulan dari penggunaan teknik anti komputer forensik, serta saran-saran yang dianggap perlu dengan mendasarkan pada hasil-hasil yang telah dicapai.

BAB II
LANDASAN TEORI

2.1 Komputer forensik

2.1.1 Definisi komputer forensik

Komputer forensik adalah [HAM10]:

a. Pengumpulan dan analisa data dari berbagai sumber daya komputer, mencakup : sistem komputer, jaringan, komputer dan juga berbagai media penyimpanan yang dikatakan layak untuk diajukan dalam sidang pengadilan.
b. Salah satu metode pengumpulan barang bukti dari sistem komputer dan semua media penyimpanannya yang dapat dikemukakan dalam persidangan dalam bentuk yang jelas dan dapat dimengerti.
c. Proses mempertahankan, identifikasi, menafsirkan dan mendokumentasikan bukti-bukti komputer guna melengkapi persyaratan barang bukti, prosedur resmi, melaporkan informasi yang ditemukan serta menyediakan pandangan ahli dalam persidangan.
d. Ilmu menemukan, memproses dan menyelidiki data dari sistem komputer menggunakan suatu metode yang mana data yang ditemukan harus dapat diterima di dalam persidangan.

2.1.2 Tujuan Komputer Forensik

Berikut adalah tujuan dari komputer forensik [HAM10]:

a. Untuk memulihkan, menganalisis, dan melindungi komputer dan alat yang terkait lainnya sedemikian rupa sehingga dapat disajikan sebagai bukti di pengadilan.

b. Untuk mengidentifikasi bukti dalam waktu singkat, memperkirakan potensi adanya dampak dari kejahatan pada yang terjadi kepada korban, dan menilai maksud dan identitas dari pelaku kejahatan.

2.1.3 Fase-Fase Penyidikan:

Untuk melakukan penelitian penyidik harus melakukan langkah-langkah berikut ini [BUD11]:

a. Mengamankan komputer untuk menjamin bahwa peralatan dan data dapat diselamatkan. Penyidik harus memastikan bahwa tidak ada seorangpun yang dapat mengakses komputer atau media penyimpanan selama proses penyidikan, tanpa sepengetahuan dan seijinnya. Jika komputer terhubung dengan internet atau LAN, penyidik harus memutuskan terlebih dahulu.

b. Menemukan semua file dalam komputer, termasuk file yang dienkripsi, dilindungi dengan *password*, disembunyikan atau bahkan dihapus selama belum ditimpa oleh file lain. Penyidik harus membuat semua salinan file dalam komputer, baik yang berada didalam harddisk maupun media penyimpanan lainnya. Karena setiap akses dapat mengubah file, penyidik hanya boleh bekerja dengan salinan file untuk mencari bukti-bukti yang diperlukan. File asli harus tersimpan rapi dan utuh.

c. Mengambil semua file yang terhapus sebanyak mungkin dengan menggunakan aplikasi khusus untuk mendeteksi.

d. Membuka isi semua file yang telah disembunyikan, dengan program yang didesain khusus untuk mendeteksi data-data yang tersembunyi.

e. Mendekripsi dan mengakses mengakses file-file yang dilindungi.

f. Menganalisis area khusus dalam *harddisk*, (*unallocated space* yang mungkin digunakan untuk menyimpan file atau bagian file yang memiliki hubungan dengan kasus yang diselidiki).

g. Mencatat setiap langkah yang dilakukan dalam selama proses sesuai prosedur, tanpa merusak atau mengubah satu file pun.

h. Menyimpan kesaksian dipengadilan sebagai saksi ahli dalam bidang komputer forensik.

Untuk dapat diajukan ke pengadilan, hasil komputer forensik harus [BUD11] :

a. Memenuhi Standar tertentu yaitu:

1. Admissible

2. Authentic

3. Believeable

4. Reliable

b. *Tools* komputer forensik harus dapat divalidasi metodologinya.

c. Media elektronik yang diperiksa harus jelas *Chain of Custody* nya sejak mulai pengambilan awal sampai akhirnya diajukan ke pengadilan.

d. Pada umumnya pemeriksaan media penyimpanan elektronik harus dilakukan atas izin dari pemiliknya, kecuali atas otoritas hukum.

2.2 Anti Komputer Forensik

2.2.1 Definisi Anti Komputer Forensik

Seperti namanya, Anti komputer forensik adalah lawan dari bidang komputer forensik. Jika bidang komputer forensik menitik beratkan pada upaya mencari dan

menemukan data, menjaga integritas data, bidang anti komputer forensik justru berfokus pada sisi sebaliknya [ARR10]:

a. Bagaimana agar data tetap aman dari sentuhan orang lain maupun dari pihak komputer forensik itu sendiri sehingga data tersebut tidak terganggu privasinya.
b. Bagaimana agar data tersebut tetap tidak bisa diakses (kecuali oleh sang pemilik atau pembuat data tersebut).
c. Bagaimana cara merusak integritas data tersebut agar tidak berlaku integritasnya dipengadilan atau tidak dapat dijadikan sebagai barang bukti.

2.2.2 Tujuan Anti Komputer Forensik

Berikut adalah tujuan secara umum dari anti komputer forensik [WIK11]:

a. Bagaimana membuat data supaya data tidak bisa ditemukan atau dibuka, misalnya dengan disembunyikan (*hidden*), di*secure delete*, dan sebagainya.
b. Bagaimana mengupayakan agar andaikata suatu data berhasil ditemukan, maka data tersebut tetap tidak layak sesuai dengan standar hukum, mungkin karena integritasnya sudah rusak dan meragukan misalnya dengan mengubah tanggal dan sebagainya.

2.2.3 Tindakan Mendasar Pada Anti-Forensik:

Tindakan dasar pada anti komputer forensik[ARR10] :

a. mengupayakan supaya jejak tidak ada,
b. mengupayakan jejak dihapus bilamana jejak itu ada.
c. mempersulit pencarian data.

2.2.4 Perbandingan Antara Komputer Forensik dan Anti-Forensik:

Tabel perbandingan penggunaan antara komputer forensik dan anti komputer forensik [ARR10].

Tabel 2.1 Perbandingan Forensik dan Anti-Forensik

KOMPUTER FORENSIK	**ANTI-FORENSIK**
Menembus Proteksi	Mengamankan Proteksi
Memulihkan data yang telah dihapus	Memastikan data yang telah dihapus tidak bisa kembalikan lagi.
Mengakses data	Melindungi data
Membuka penyamaran data	Menyamarkan suatu data agar tidak terdeteksi
Mencari jejak yang dilakukan oleh tersangka	Menghapus semua jejak yang ada
Melacak kejahatan	Mengamankan data dan melindungi privasi

2.3 Manipulasi File

2.3.1 Definisi Manipulasi File

Manipulasi File adalah sebuah proses rekayasa dengan melakukan penambahan, penyembunyian, penghilangan atau penghapusan terhadap bagian atau keseluruhan dari file-file yang ada didalam sebuah perangkat komputer.

2.3.2 Penyamaran File

Penyamaran file adalah sebuah teknik untuk mencapur, mengkamuflasekan antara data penting dengan data tidak penting, dan melakukan perubahan nama file, lokasi file, format file, serta isi file tersebut sehingga sulit untuk dilacak.

2.3.3 Kode ASCII

Kode Standar Amerika untuk Pertukaran Informasi atau ASCII (*American Standard Code for Information Interchange*) merupakan suatu standar internasional dalam kode huruf dan simbol seperti *Hex* dan *Unicode* tetapi ASCII lebih bersifat *universal*, contohnya 124 adalah untuk karakter "|". Ia selalu digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks. Kode ASCII sebenarnya memiliki komposisi bilangan biner sebanyak 8 bit. Dimulai dari 0000 0000 hingga 1111 1111. Total kombinasi yang dihasilkan sebanyak 256, dimulai dari kode 0 hingga 255 dalam sistem bilangan Desimal [WIC11].

2.3.4 Penyamaran Waktu File

Penyamaran waktu file adalah sebuah teknik untuk merubah pencatatan *timestamp* yang ada dalam sebuah file. Seperti, merubah pencatatan kapan file dibuat, diedit, dan diakses. Sehingga integritas dari file tersebut sudah rusak dan tidak sesuai dengan standar hukum yang ada.

2.3.5 TimeStamp

Timestamp adalah urutan karakter, yang menunjukkan tanggal dan atau waktu di mana peristiwa tertentu terjadi. *Timestamp* adalah waktu di mana peristiwa dicatat oleh komputer, bukan waktu peristiwa itu sendiri. Dalam banyak kasus, perbedaan mungkin tidak penting: waktu di mana peristiwa dicatat oleh timestamp (misalnya, masuk ke dalam sebuah file *log*) harus sangat, sangat dekat dengan waktu terjadinya peristiwa yang direkam. Dalam beberapa kasus, *timestamp* dapat hanya penomoran

peristiwa, penggunaan format *date_time* untuk menyimpan *timestamp* kemudian tidak wajib.

Data ini biasanya disajikan dalam format yang konsisten, yang memungkinkan untuk memudahkan perbandingan dari dua catatan yang berbeda dan pelacakan kemajuan dari waktu ke waktu, praktek cap waktu rekaman dalam cara yang konsisten bersama dengan data yang sebenarnya disebut timestamping.

Cap biasanya digunakan untuk acara penebangan, dalam hal mana setiap peristiwa dalam log ditandai dengan timestamp. Dalam *file system, timestamp* bisa berarti tanggal disimpan waktu pembuatan atau modifikasi file [WIK10].

2.3.6 TimeStomp

Timestomp memiliki kemampuan untuk mengubah atau menghapus nilai timestamp diakses, dibuat, dimodifikasi dan entri diubah pada sistem NTFS. Ini juga dikenal sebagai atribut atau nilai *timestamp* Mace. Timestomp diciptakan oleh dua orang bernama James Foster dan Vincent Liu. [MAX11].

2.3.7 Secure Delete

Secure delete adalah sebuah teknik untuk melakukan penghapusan file dengan benar-benar dihapus atau sebagian data tidak bisa dipulihkan lagi dengan *software recovery* data. Agar data yang sudah dihapus atau data yang sudah terhapus tidak dapat diakses bahkan disalah gunakan oleh orang lain.

2.3.8 *Recovery* Data

Recovery data adalah proses menyelamatkan data dari rusak, gagal, rusak, atau tidak dapat diakses media penyimpanan sekunder ketika itu tidak dapat diakses normal. Sering kali data sedang diselamatkan dari media penyimpanan seperti internal atau eksternal *harddisk drive, drive solid state* (SSD), USB *flash*, kaset penyimpanan, CD, DVD, RAID, dan elektronik lainnya. Pemulihan mungkin

diperlukan karena kerusakan fisik pada perangkat penyimpanan atau kerusakan logis untuk sistem file yang mencegah dari yang dipasang oleh sistem operasi host.

Yang paling umum "data *recovery*" skenario melibatkan sistem operasi (OS) gagal (biasanya pada disk tunggal, tunggal-partisi, satu OS sistem), dalam hal ini tujuannya adalah hanya untuk menyalin semua file yang ingin ke disk lain. Hal ini dapat dengan mudah dicapai dengan *Live* CD, sebagian besar yang menyediakan sarana untuk me-mount sistem drive dan disk cadangan atau *removable* media, dan untuk memindahkan file dari disk sistem ke media *backup* dengan manajer file atau perangkat lunak *disc authoring* optik . Kasus seperti itu sering dapat diatasi dengan partisi disk dan konsisten menyimpan file data berharga (atau salinan dari mereka) pada partisi yang berbeda dari file sistem OS tergantikan.

Skenario lain melibatkan kegagalan disk-tingkat, seperti sistem file terganggu atau partisi disk atau kegagalan *hard disk*. Dalam setiap kasus ini, data tidak dapat dengan mudah dibaca. Tergantung pada situasi, solusi melibatkan memperbaiki sistem file, tabel partisi atau *master boot record*, atau teknik pemulihan *hard disk* mulai dari perangkat lunak berbasis pemulihan data yang rusak untuk penggantian *hardware* pada disk rusak secara fisik. Jika pemulihan *hard disk* diperlukan, disk itu sendiri telah biasanya gagal secara permanen, dan fokusnya adalah lebih pada pemulihan satu kali, menyelamatkan data apa pun yang dapat dibaca.

Dalam skenario ketiga, file sudah "dihapus" dari media penyimpanan. Biasanya, file yang dihapus tidak segera terhapus, melainkan referensi kepada mereka dalam struktur direktori dihapus, dan ruang yang mereka tempati dibuat tersedia untuk nanti Timpa. Sementara itu, file asli dapat dipulihkan. Meskipun ada beberapa kebingungan istilah, "data *recovery*" juga dapat digunakan dalam konteks aplikasi forensik atau spionase [GUT11].

2.3.9 Metode Peter Gutmann

Cara penghapusan yang aman pada media magnetik adalah seperti yang dikembangkan oleh Peter Gutmann dari Universitas Auckland. Pada metoda ini Peter Gutmann mengembangkan pola tertentu yang disesuaikan dengan cara pengkodean pada harddisk seperti RLL, MFM, dan PRLM. Konsep dengan cara *overwrite* ini adalah dengan membalik bidang magnetik pada disk bolak-balik sebanyak mungkin tanpa menulis pola yang sama berturut-turut.

Pada paper ini akan dikemukakan beberapa metode untuk mengembalikan data yang dihapus dan menampilkan skema bagaimana agar *data recovery* sulit untuk dilakukan [GUT11].

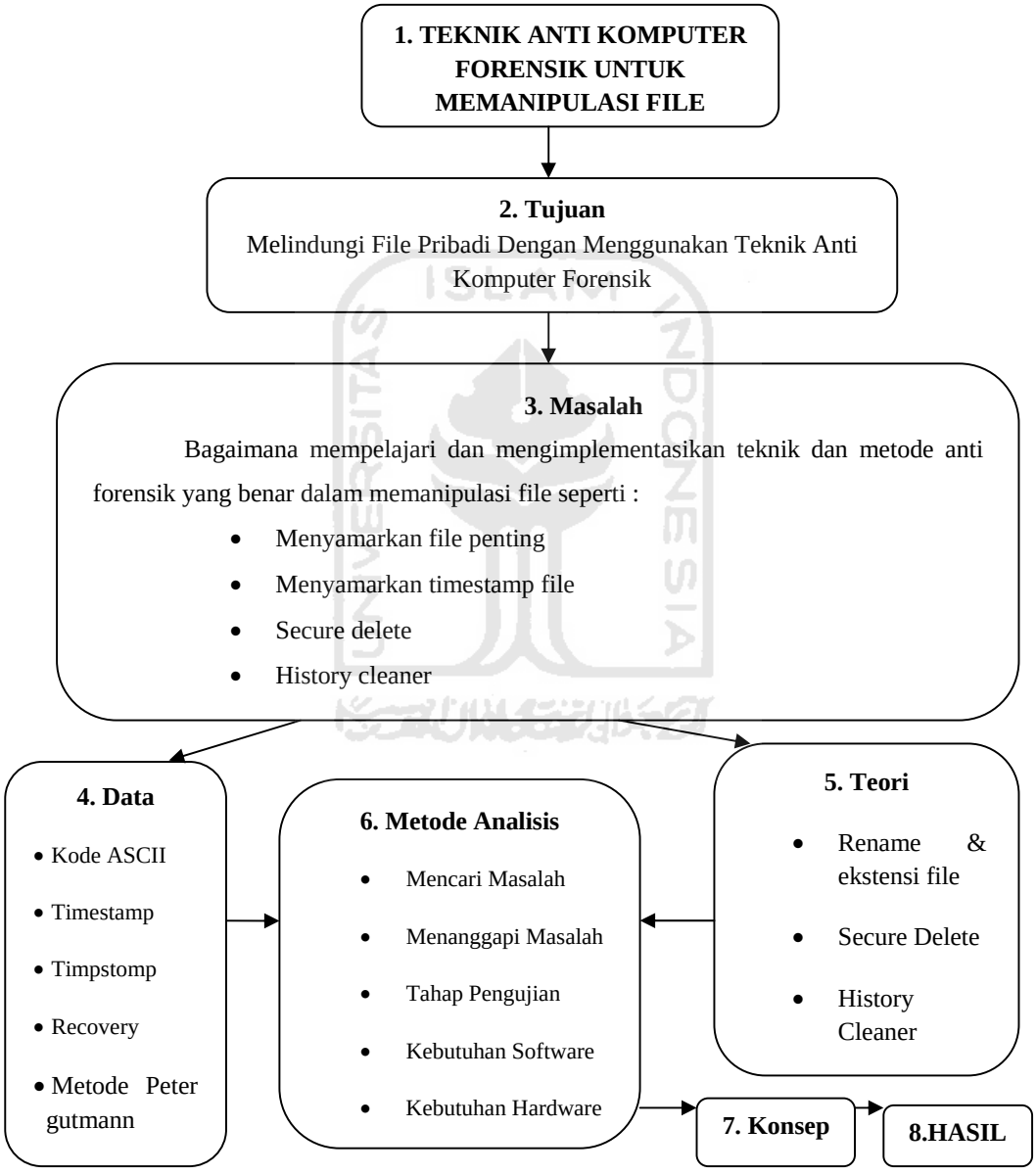
2.3.10 History Cleaner

History cleaner adalah sebuah teknik untuk melakukan pembersihan atau penghapusan jejak-jejak yang ada atau dibuat oleh sistem operasi, *software*, situs dan sebagainya. Sehingga jejak-jejak tersebut tidak bisa deketahui oleh siapapun.

BAB III

METODOLOGI

3.1 Kerangka Pola Fikir



Gambar 3.1 Alur pola fikir dasar penelitian

Penjelasan :

1. Judul yang digunakan untuk melakukan penelitian adalah teknik anti komputer forensik untuk memanipulasi file.
2. Tujuan yang didapatkan sesuai dari judul yang digunakan yaitu bagaimana melindungi file pribadi dengan menggunakan teknik anti komputer forensik.
3. Masalah yang didapatkan untuk mencapai tujuan seperti bagaimana mempelajari teknik dan metode anti komputer forensik yang benar dalam memanipulasi file.
4. Memperoleh data yang digunakan untuk menangani masalah seperti data tentang kode *ASCII, timestamp, timestomp, data recovery*, dan metode Peter Gutmann.
5. Memperoleh teori yang digunakan untuk menangani masalah seperti teori *rename* & merubah ekstensi file, *secure delete*, dan *history cleaner*.
6. Metode analisis disusun setelah mendapatkan data-data dan teori yang dibutuhkan.
7. Membuat konsep yang digunakan untuk menangani masalah.
8. Hasil yang didapatkan setelah melakukan teknik anti komputer forensik untuk memanipulasi file.

3.2 Metode Analisis

Metode analisis dilakukan untuk mengetahui semua permasalahan serta kebutuhan yang diperlukan dalam melakukan penelitian tugas akhir dengan judul teknik anti komputer forensik untuk memanipulasi file. metode yang akan digunakan

dengan mencari masalah, menanggapi masalah yang dihadapi dan tahap pengujian serta semua kebutuhan seperti, analisis kebutuhan *software*, dan analisis kebutuhan *hardware*.

Teknik anti komputer forensik yang akan digunakan utuk memanipulasi file seperti menyamarkan file, menyamarkan *timestamp*, *secure delete*, dan *history cleaner*. Teknik memanipulasin file tersebut menggunakan beberapa software anti komputer forensik sebagai alat bantu, serta menggunakan *software* komputer forensik untuk tahap pengujian apakah teknik anti komputer forensik tersebut telah berhasil tidak terdeteksi oleh *software-sof*tware komputer forensik.

3.3 Analisis Kebutuhan *Software*

Hardware komputer tidak akan berati tanpa adanya *software* begitu juga sebaliknya. Sehingga *software* yang akan digunakan untuk melakukan teknik anti komputer forensik sebagai berikut :

a. Windows XP atau 7 : Sistem operasi yang digunakan.

b. *Software* anti komputer forensik :

   1. Hex Editor Neo : Fungsi untuk melakukan pengeditan *ASCII header* pada file.

      http://www.hhdsoftware.com/free-hex-editor

   2. Notepad : Fungsi untuk melakukan pengeditan *ASCII header* pada file.

   3. Cygnus Hex Editor : Fungsi untuk melakukan pengeditan *ASCII header* pada file.

      http://www.softcircuits.com/cygnus/fe/

4. TimeStomp : Fungsi untuk menyamarkan *timestamp* pada file.

   http://www.forensicswiki.org/wiki/Timestomp

5. SetFileDate : Fungsi untuk menyamarkan *timestamp* pada file

   http://setfiledate.en.softonic.com/

6. eXpress TimeStamp Toucher : Fungsi untuk menyamarkan *timestamp* pada file

   http://www.irnis.net/soft/xtst/

7. BCWipe : Fungsi untuk *secure delete.*

   http://www.jetico.com/wiping-bcwipe/

8. TuneUp Utility : Fungsi untuk *secure delete.*

   http://www.tune-up.com/products/tuneup-utilities/?tracking=UA-en-US%2C&utm_campaign=tuu2011&utm_medium=sem&utm_source=google&utm_content=tuubuy&x-rest=&gclid=CMTj_OH3oaoCFYN66wodknANUw

9. Ccleaner : Fungsi untuk *history cleaner*.

   http://download.cnet.com/ccleaner/

c. *Software* komputer forensik :

1. File Investigator File Find : Fungsi untuk mendeteksi penyamaran file.

   http://www.brothersoft.com/file-investigator-file-find-101519.html

2. Hex Editor Neo : Fungsi untuk mendeteksi penyamaran *timestamp*.

   http://www.hhdsoftware.com/free-hex-editor

3. Recuva : Fungsi untuk *recovery* file yang telah dihapus

http://www.scanwith.com/download/Recuva.htm

4. R-Wipe&Clean : Fungsi untuk menganalisa history yang belum dihapus.

   http://download.cnet.com/R-Wipe-and-Clean/3000-2144_4-10159835.html

3.4 Analisis kebutuhan *Hardware*

Hardware komputer yang akan digunakan adalah yang dapat mendukung perangkat lunak memiliki kemampuan yang baik, seperti :

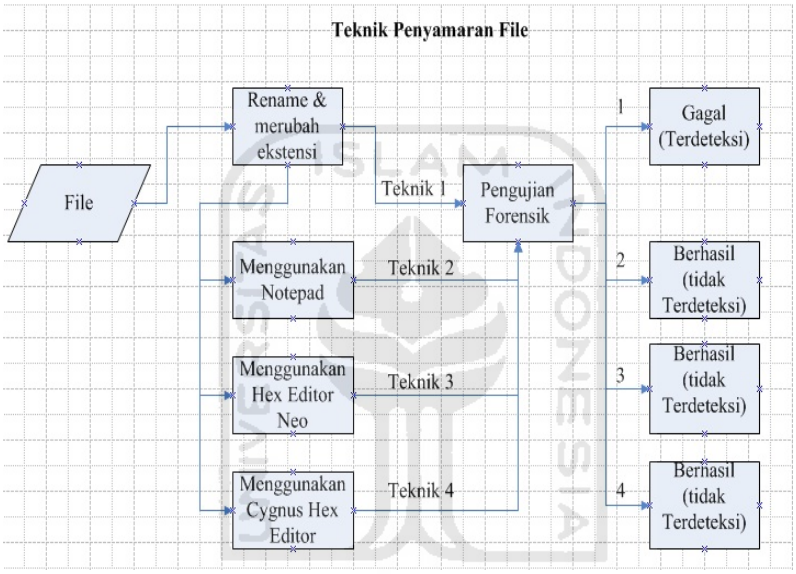
a. Prosesor minimal intel atom 1,2 Ghz
b. RAM 1GB
c. Harddisk 40GB
d. Monitor
e. Keyboard dan Mouse

3.5 Konsep

Manipulasi file disini akan dibagi menjadi empat teknik yaitu :

a. Teknik menyamarkan file : Melakukan percobaan melakukan penyamaran penyamaran file seperti merubah nama file, ekstensi file, maupun merubah ACII header yang ada pada file tersebut dengan menggunakan *software* anti komputer forensik. Pada percobaan akan disimulasikan proses menyamarkan file dengan teknik 1 terlebih dahulu seperti merubah nama file dan ekstensi file, dan dilakukan peroses pengujian dengan

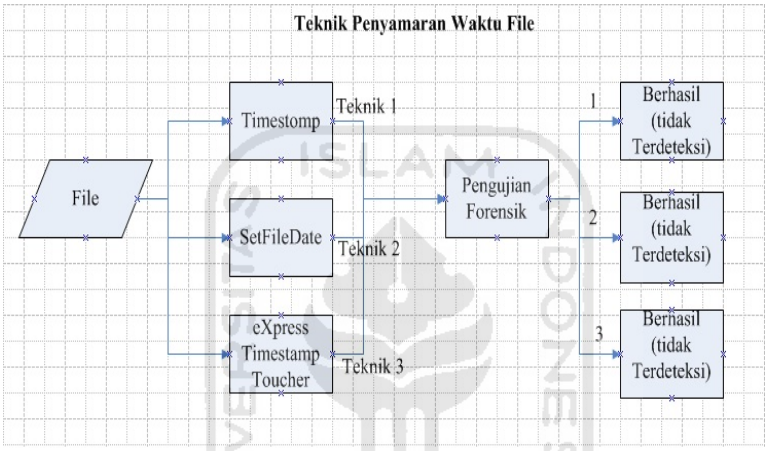
menggunakan *software* komputer forensik, apakah masih terdeksi atau sudah tidak terdeteksi. Jika masih terdeteksi maka akan melakukan teknik ke 2,3 dan 4 yang selajutnya sampai dengan sudah berhasil tidak terdeksi, apabila sudah tidak terdeksi maka teknik tersebut sudah berhasil mengelabuhi *software* komputer forensik tersebut. struktur yang akan digunakan dalam teknik menyamarkan file, seperti pada gambar 3.2



Gambar 3.2 struktur teknik menyamarkan file

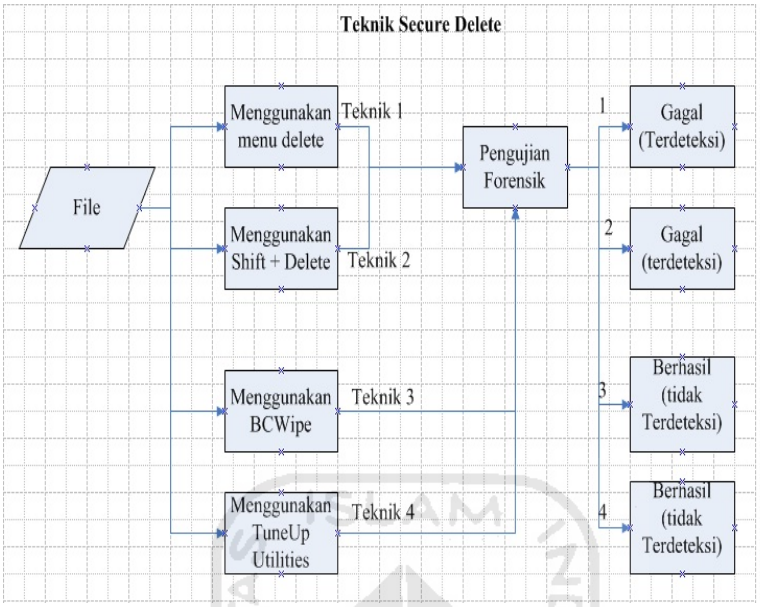
b. Teknik menyamarkan waktu file : Melakukan percobaan menyamarkan waktu file yang telah tercantum pada *propertise* file tersebut seperti *created, modified,* dan *accessed*. Pada percobaannya dengan menggunakan *software* anti komputer forensik sebagai bantuan untuk merubah pencacatan waktunya dan selanjutnya melakukan pengujian dengan *software* komputer forensik apakah sudah tidak terdeteksi atau

masih terdeteksi perubahan yang telah dilakukan. Jika terdeteksi maka akan melakukan percobaan yang selajutnya sampai dengan sudah berhasil tidak terdeksi, apabila sudah tidak terdeksi maka melakukan teknik lainnya agar dapat membedakan antara teknik 1,teknik 2, dan teknik 3. struktur yang akan digunakan dalam teknik menyamarkan waktu file, seperti pada gambar 3.3



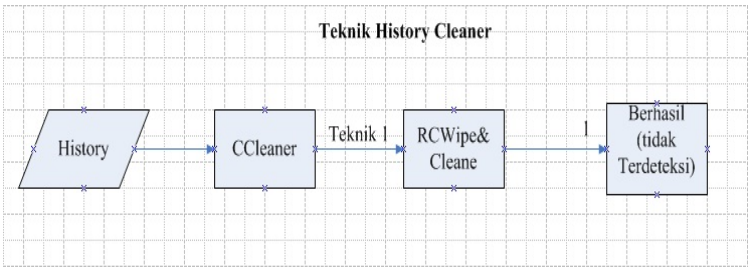
Gambar 3.3 Struktur teknik penyamaran waktu file

c. Teknik *secure delete* : Melakukan percobaan menghapus file secara aman. Pada percobaan *secure delete* akan disimulasikan dari percobaan sederhana seperti menghapus biasa sampai dengan menghapus menggunakan *software* anti komputer forensik, dan melakukan pengujian menggunakan *software* komputer forensik apakah sudah tidak terdeteksi atau masih terdeteksi. Jika masih terdeteksi maka akan melakukan percobaan yang selajutnya sampai dengan sudah berhasil tidak terdeksi, apabila sudah tidak terdeksi maka akan mencoba teknik lainnya untuk membedakan hasil antara teknik 3 dan teknik 4. struktur yang akan digunakan dalam teknik *secure delete*, seperti pada gambar 3.4



Gambar 3.4 Struktur teknik *secure delete*

d. Teknik *History Cleaner* : Melakukan percobaan menghapus history secara aman. Pada percobaan *history cleaner* akan disimulasikan melakukan pengahapusan *history* baik yang dibuat oleh *system* maupun yang dibuat oleh *software* dengan bantuan *software* anti komputer forensik dan pengujian menggunakan *software* komputer forensik apakah sudah tidak terdeteksi atau masih terdeteksi. Jika masih terdeteksi maka akan melakukan percobaan yang selajutnya sampai dengan sudah berhasil tidak terdeksi, apabila sudah tidak terdeksi maka teknik tersebut sudah berhasil mengelabuhi *software* komputer forensik tersebut. struktur yang akan digunakan dalam teknik *history cleaner*, seperti pada gambar 3.5



Gambar 3.5 Struktur teknik *history cleaner*

BAB IV

HASIL DAN PEMBAHASAN

4.1 Manipulasi File

4.2 Penyamaran File

Penyamaran file adalah sebuah teknik untuk mencampur, mengkamuflasekan antara data penting dengan data tidak penting, dan melakukan perubahan nama file, lokasi file, format file, serta isi file tersebut sehingga sulit untuk dilacak.

4.2.1 Mencari Masalah

Susuai pengertian dari kata penyamaran file, masalah yang didapatkan adalah bagaimana cara menyamarkan suatu file dengan menggunakan metode dan teknik anti forensik agar tidak terdeteksi oleh *scanner* forensik.

4.2.2 Menanggapi Masalah

Menanggapi masalah diatas, bagaimana cara melakukan penyamaran file. Terlebih dahulu mencoba beberapa metode untuk mengenali jenis file seperti :

a. Mengenali ekstensi file tersebut, misalnya file .mp3 identik dengan file lagu, file .jpg identik dengan file gambar, file .doc atau .docx identik dengan file dokumen, dan sebagainya.
b. Mengenali *signature* file tersebut, misalnya saja adanya *ASCII header* mz mengindikasi file tersebut adalah file *executable*, adanya *ASCII header* PK mengindikasikan file tersebut adalah sejenis file Zip, dan sebagainya.

Karena jenis file dikenali dari ekstensi dan signaturnya, untuk menyamarkan jenis file, maka perlu memanipulasi ekstensi atau signature file tersebut. Tujuan dari penyamaran file ini adalah untuk menyembunyikan file yang dianggap sangat rahasia

agar tidak mudah ditemukan oleh seseorang maupun oleh seorang ahli komputer forensik.

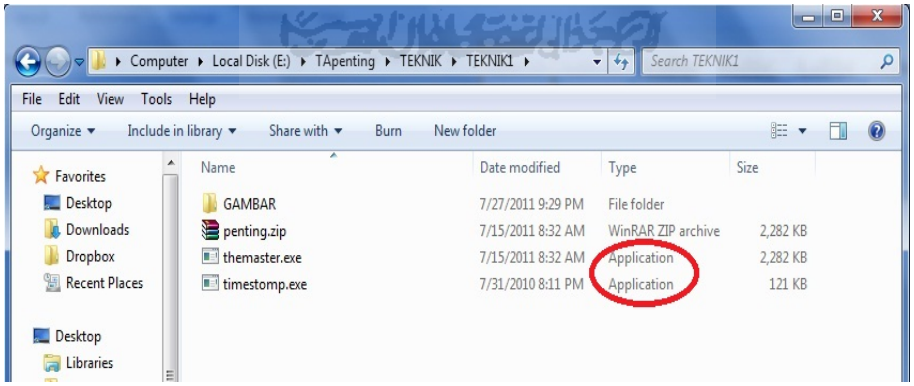
Pertama-tama buat sebuah file berektensi .zip yang akan digunakan sebagai percobaan penyamaran file, misalanya file tersebut ”penting.zip”. Selanjutnya membuat beberapa percobaan dengan menggunakan teknik anti forensik agar file ”penting.zip” tersebut disamarkan dan tidak dapat ditemukan oleh software komputer forensik.

Berikut adalah tahap pengujian dengan menggunakan beberapa teknik anti komputer forensik dalam penyamaran file.

4.2.3 Tahap Pengujian

4.2.3.1 Teknik pertama

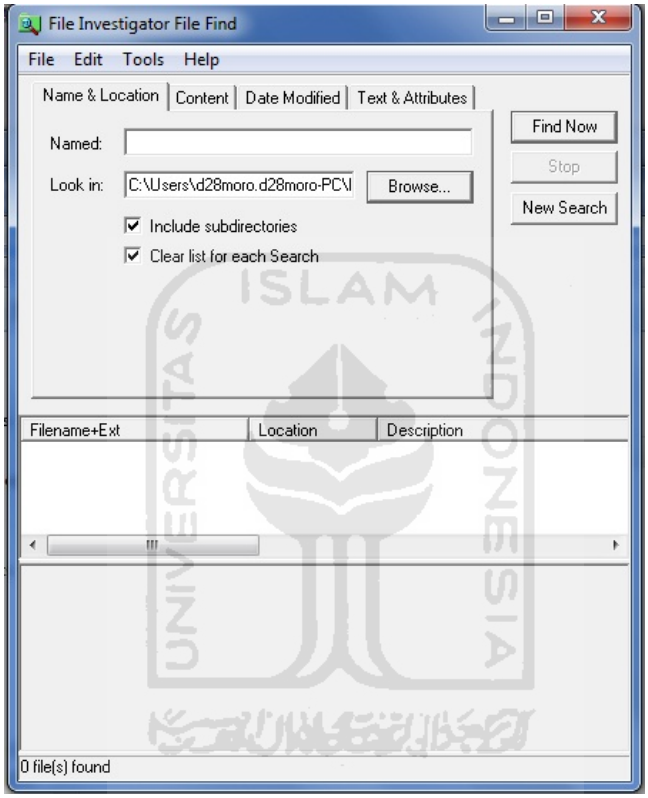
Pada teknik pertama, akan mencoba secara sederhana yaitu hanya merubah nama dan file extensinya saja. Contoh : dari file ”penting.zip” di*rename* menjadi ”themaster.exe”, file asli ”penting.zip” harus di-*backup* terlebih dahulu agar bisa menjadi perbandingan antara file asli dengan file yang telah di-rename menjadi ekstensi lain. Seperti terlihat pada gambar 4.1:



Gambar 4.1 Persamaan antara file asli .exe dengan file yang telah di*rename*.

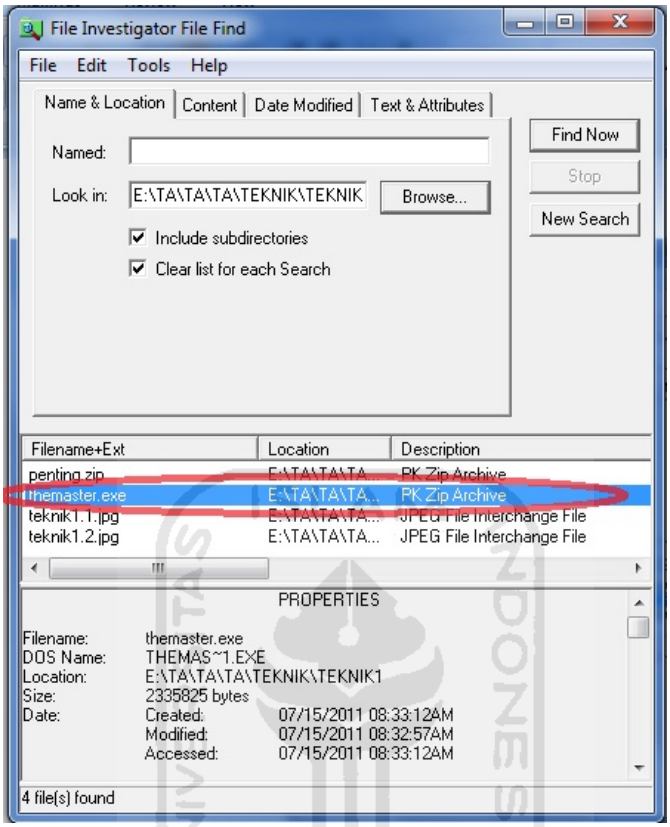
Melalui proses yang sederhana tersebut fitur find standar *windows* pun tidak dapat mengenali ekstensi file .exe samaran. Akan tetapi dengan menggunakan

semacam *scanner* pelacak file, file yang telah di*rename* ekstensinya akan cepat diketahui apa jenis file sebenarnya. *Tools* pelacak yang akan digunakan merupakan alat bantu forensik, yang bernama *File Investigator File Find*. Contoh *tool*nya seperti yang terlihat pada gambar 4.2:



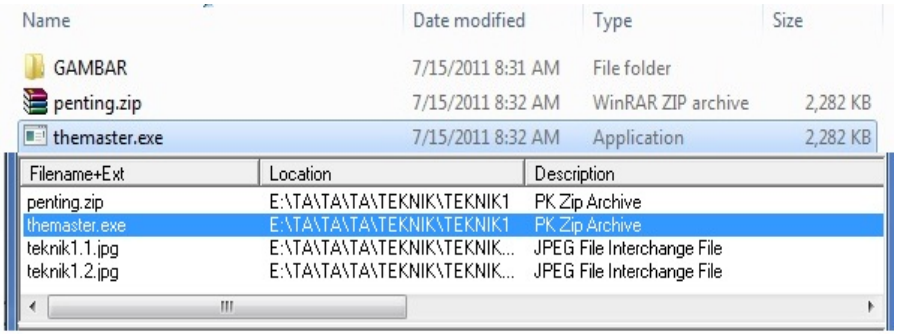
Gambar 4.2 *Tools* komputer forensik *File Investigator File Find*

Dan inilah hasil yang didapatkan setelah menggunakan *tool* komputer forensik *File Investigator file find* pada file yang telah direname ekstensinya tadi. Seperti terlihat pada gambar 4.3 :



Gambar 4.3 *Tools* forensik mendeteksi ekstensi file yang asli

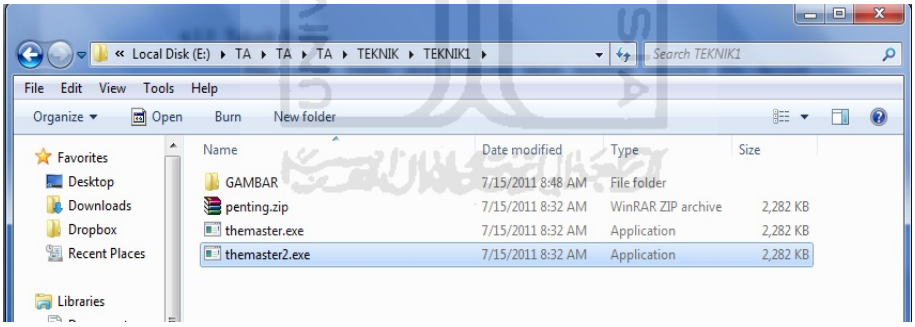
Dari hasil pencarian diatas *software File Investigator File Find* berhasil mendeteksi bahwa file dengan ekstensi .exe bernama themaster.exe sesungguhnya adalah file .zip. Disini dapat diketahui bahwa *software* tersebut selain dapat mengenali file dari ekstensinya, ternyata juga mampu mendeteksi *signature* file, khususnya *header* file. Bisa dilihat dari perbedaan antara *find* standar *windows* dengan *software* pelacak forensik, seperti pada gambar 4.4 :



Gambar 4.4 Perbandingan hasil *find* standar dan pelacakan *software* forensik.

4.2.3.2 Teknik Kedua

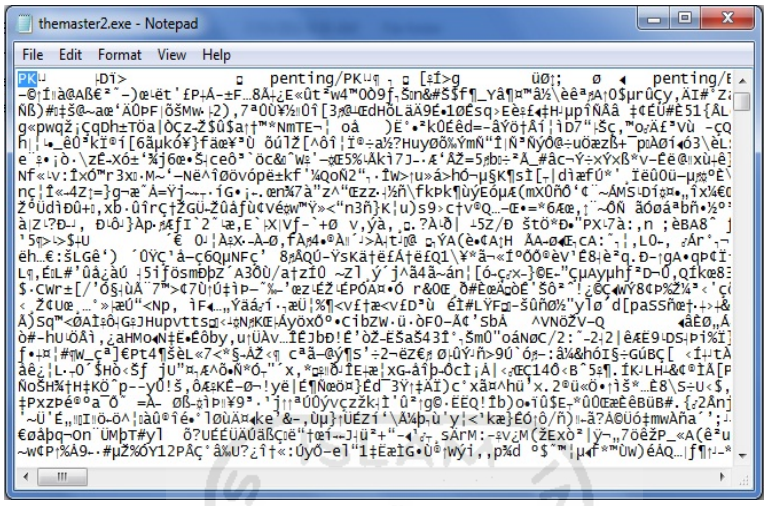
Pada teknik kedua, akan mencoba untuk merubah *signature* file, dengan menggunakan bantuan dari Notepad. Contoh : mencoba membuat *backup* dari file "themaster.exe" dan diberi nama "themaster2.exe", agar bisa dibedakan antara hasil dari teknik yang pertama dengan hasil teknik kedua. Seperti pada gambar 4.5 :



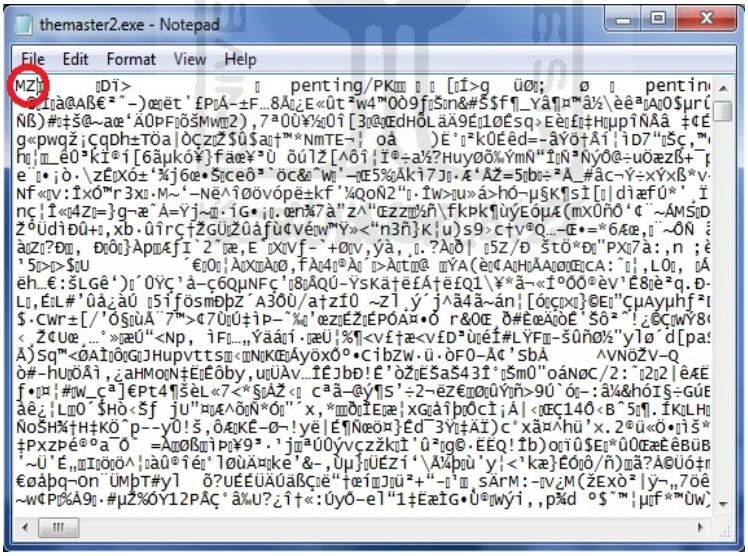
Gambar 4.5 *Backup* file hasil teknik pertama

Dari gambar file diatas dapat diketahui bahwa file yang baru dibuat juga terbaca file ekstensinya sebagai .exe oleh *find* standar *windows*. Langkah selanjutnya mencoba agar ekstensi .exe palsu yang dibuat tidak berhasil dikenali oleh software computer forensic yaitu *File Investigator File Find*.

a. Buka file "themaster2.exe" dengan menggunakan *Notepad*.
b. Ubahlah ASCII *header* pada file "themaster2.exe" dari PK (file .zip). Seperti pada contoh gambar 4.6 : dan gambar 4.7 :



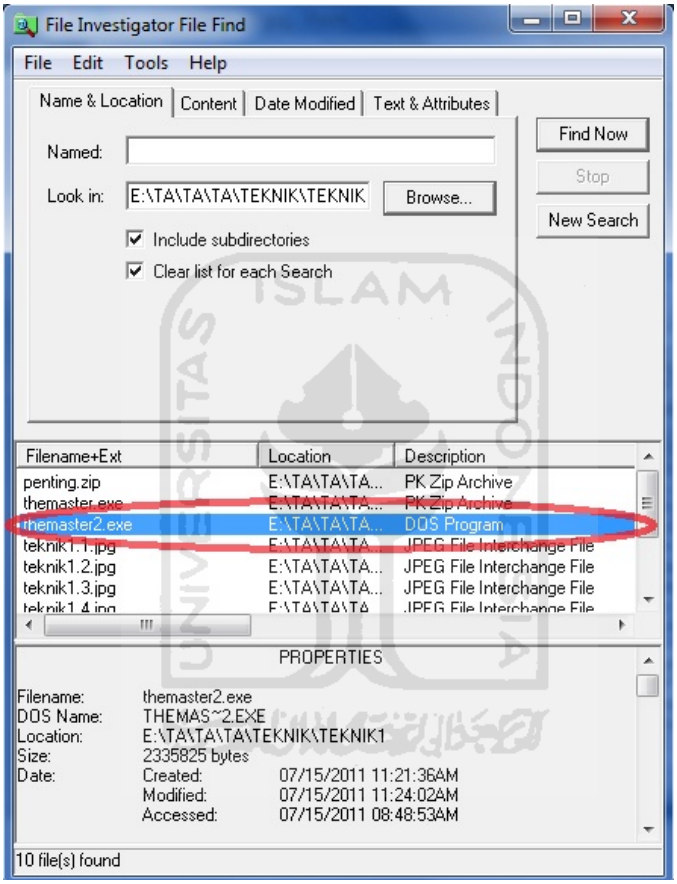
Gambar 4.6 *ASCII Heade*r pada file “themaster2.exe” sebelum diubah.



Gambar 4.7 *ASCII Header* pada file “themaster2.exe” setelah diubah.

c. Kemudian simpanlah file yang telah diubah tersebut.

Dan inilah hasil yang didapatkan setelah menggunakan *tool* komputer forensik *File Investigator file find* pada file yang telah diubah *ASCII Header*nya . Seperti terlihat pada gambar 4.8 :

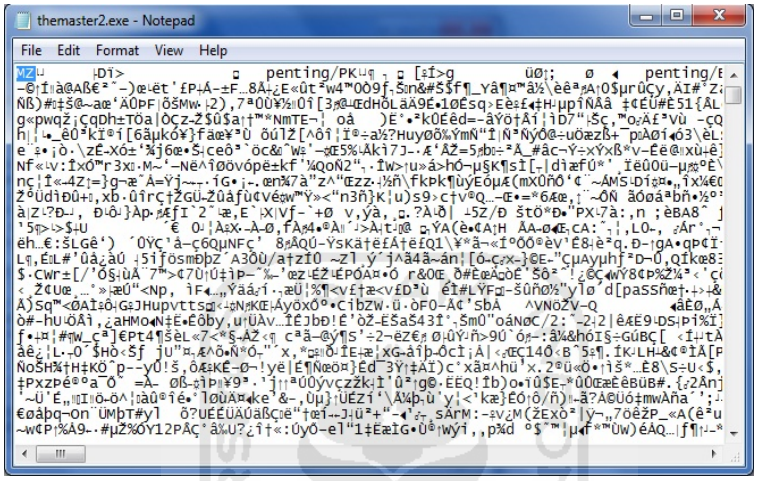


Gambar 4.*8 Tools* forensic tidak mendeteksi ekstensi file asli

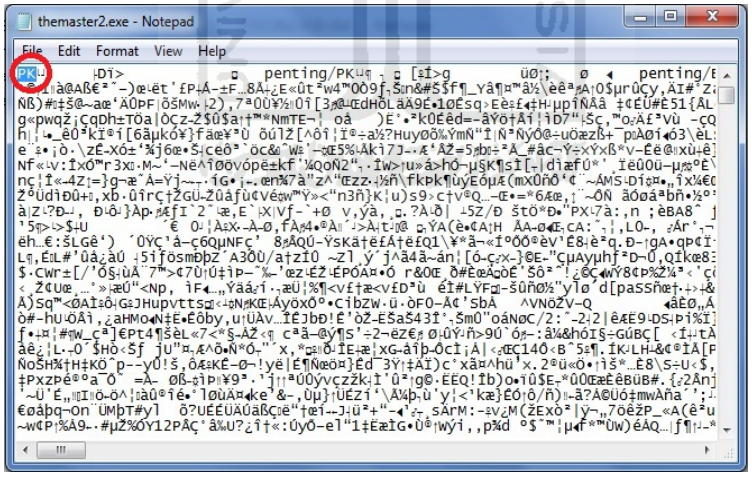
Dari teknik kedua diatas dapat dilihat bahwa *software* computer forensic *File Investigator File Find* tidak berhasil mengenali bahwa file “themaster2.exe” yang sebenarnya adalah file .zip tetapi terdeteksinya sebagai file .exe. Akan tetapi file “themaster2.exe” yang telah diubah ASCII headernya dengan menggunakan notepad bisa menyebabkan file tersebut tidak dapat diakses kembali pada saat telah dikembalikan menjadi .zip seperti awalnya. Seperti percobaan berikut :

a. Buka file “themaster2.exe” dengan menggunakan *Notepad*.

b. Ubahlah ASCII *header* pada file “themaster2.exe” dari MZ (file .exe). Seperti pada contoh gambar 4.9 : dan gambar 4.10 :



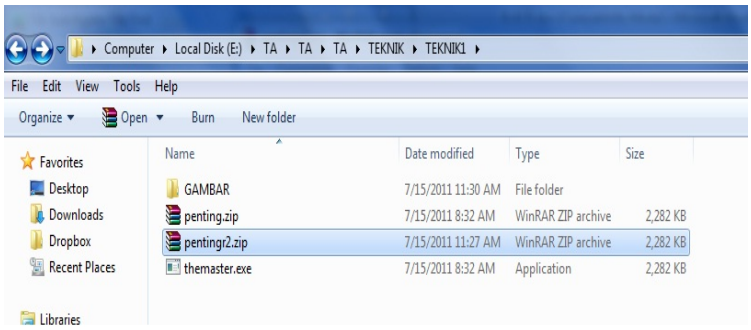
Gambar 4.9 *ASCII Header* pada file “themaster2.exe” sebelum diubah.



Gambar 4.10 contoh ASCII *Header* pada file “themaster2.exe” setelah diubah.

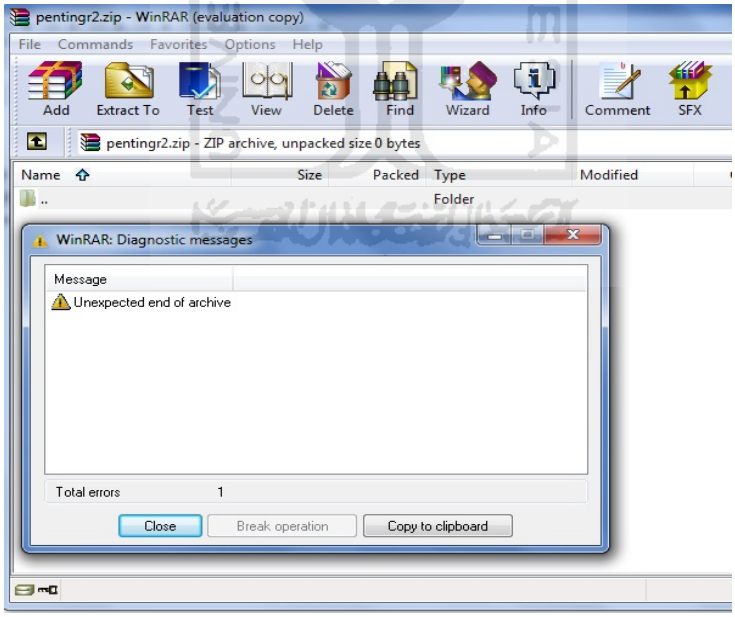
c. Kemudian simpanlah file yang telah diubah tersebut.

d. Rename dan ubah kembali ektensi pada file”themaster2.exe” menjadi “penting2.zip” seperti pada gambar 4.11



Gambar 4.11 Rename file “themaster2.exe” menjadi “penting2.zip”

e. Buka file “penting2.zip” dengan menggunakan winrar, seperti pada gambar 4.12



Gambar 4.12 File “penting2.zip” tidak dapat diakses.

Dari teknik kedua diatas dapat dipersingkat dengan menggunakan perintah batch atau dibuat menjadi file .bat. Perintah batch yang akan digunakan sebagai berikut : *@echo off*

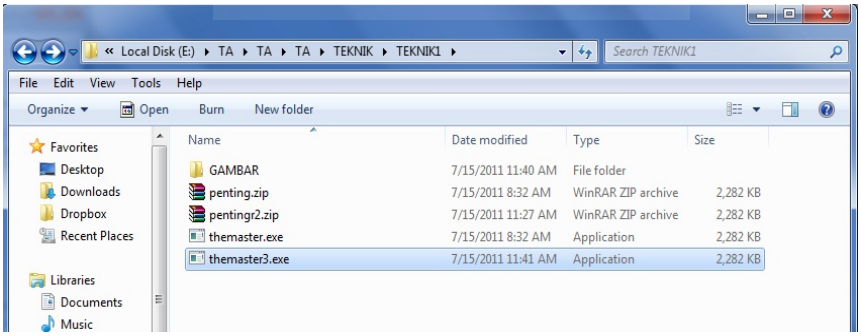
Echo MZ > penting2.zip

Ren penting2.zip themaster2.exe.

Perintah batch program tersebut akan disimpan dalam file batch.bat. file batch.bat tersebut akan dijaldalam folder yang sama dengan file yang akan dieksekusi yaitu file penting2.zip. Tetapi perintah menggunakan file .bat ini memiliki kelemahan yang sama dengan menggunakan notepad yaitu tidak bisa diakses kembalinya file .zip tersebut dan juga hanya dapat melakukan perintah terhadap satu file tujuan saja.

4.2.3.3 Teknik Ketiga

Pada teknik ketiga, akan mencoba untuk merubah *signature* file, dengan menggunakan bantuan dari software forensik Hex Editor Neo. Contoh : mencoba membuat *backup* dari file “themaster.exe” dan diberi nama “themaster3.exe”, agar bisa dibedakan antara hasil dari teknik yang pertama dan kedua dengan hasil teknik ketiga. Seperti pada gambar 4.13 :

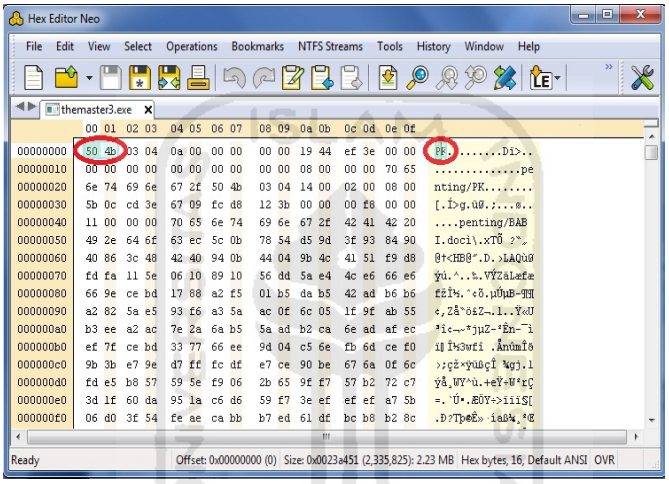


Gambar 4.13 *Backup* file hasil Teknik pertama.

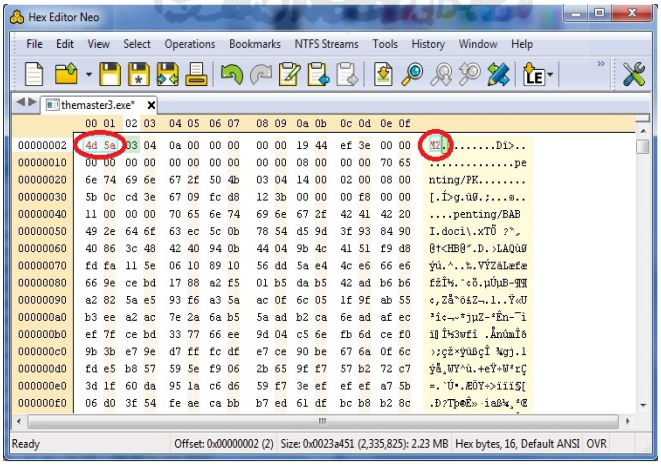
Dari gambar file diatas dapat diketahui bahwa file yang baru dibuat juga terbaca file ekstensinya sebagai .exe oleh *find* standar *windows*. Langkah selanjutnya

mencoba agar ekstensi .exe palsu yang dibuat tidak berhasil dikenali oleh software computer forensic yaitu *File Investigator File Find*.

a. Buka file percobaan 2.zip dengan menggunakan *Hex Editor*.
b. Ubahlah ASCII *header* pada file "themaster3.exe" dari PK (file .zip) atau *hexadecimal*nya 50 4b diubah menjadi MZ (file .exe) atau *hexadecimal*nya 4d 5a. Seperti pada contoh gambar 4.14 : dan gambar 4.15 :



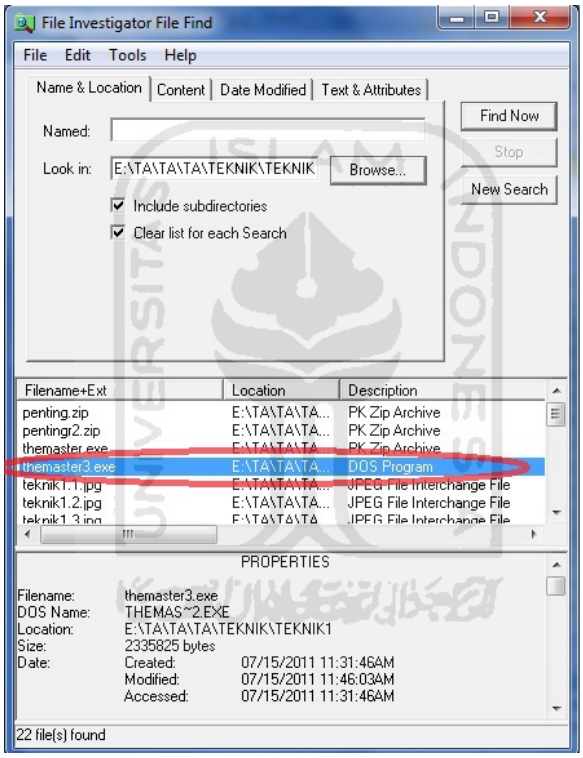
Gambar 4.14 *ASCII Heade*r pada file "themaster3.exe" sebelum diubah.



Gambar 4.15 *ASCII Header* pada file "themaster3.exe" setelah diubah.

c. Kemudian simpanlah file yang telah diubah tersebut.

Dan inilah hasil yang didapatkan setelah menggunakan *tool* komputer forensik *File Investigator file find* pada file yang telah diubah *ASCII Header*nya . Seperti terlihat pada gambar 4.16 :

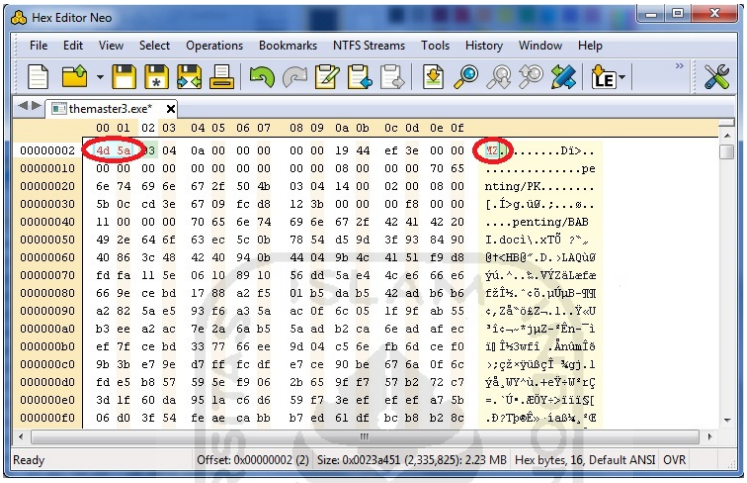


Gambar 4.16 *Tools* forensic tidak mendeteksi ekstensi file asli

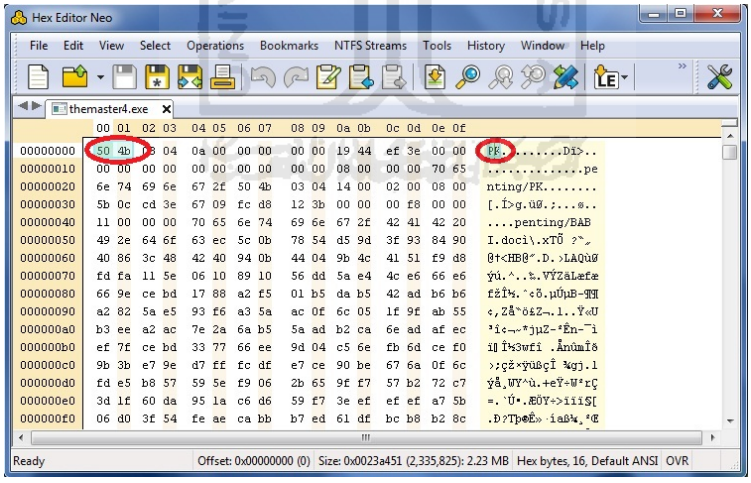
Dari teknik ketiga diatas dapat dilihat bahwa *software* computer forensic *File Investigator File Find* tidak berhasil mengenali bahwa file “themaster3.exe” yang sebenarnya adalah file .zip tetapi terdeteksinya sebagai file .exe. Dengan bantuan dari software anti forensic Hex Editor Neo file “themaster3.exe” dapat dikembalikan seperti semula yaitu file ekstensi .zip dan dapat diakses kembali, seperti pada percobaan berikut :

a. Buka file “themaster3.exe” dengan menggunakan *Hex Editor Neo* .

b. Ubahlah ASCII *header* pada file “themaster3.exe” dari MZ (file .exe). Seperti pada contoh gambar 4.17 : dan gambar 4.18 :



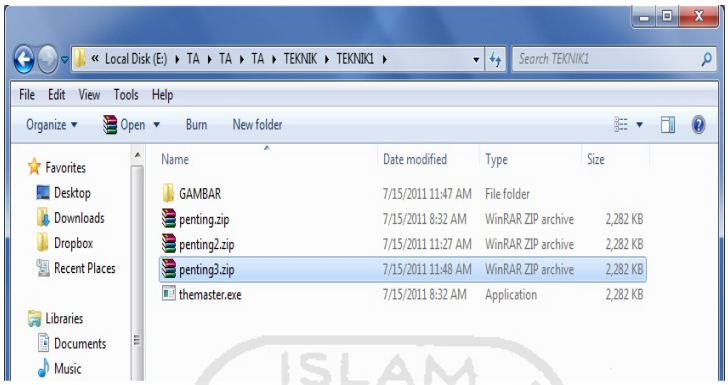
Gambar 4.17 *ASCII Heade*r pada file “themaster3.exe” sebelum diubah.



Gambar 4.18 *ASCII Header* pada file “themaster3.exe” setelah diubah.

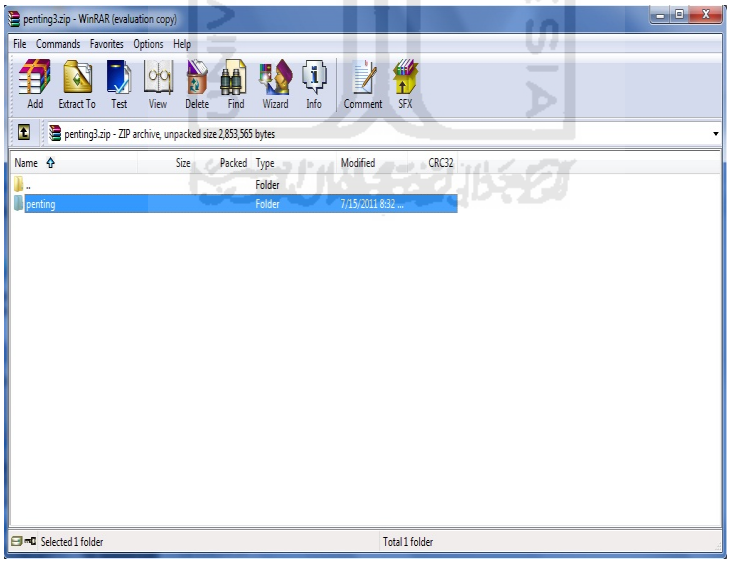
c. Kemudian simpanlah file yang telah diubah tersebut.

d. Rename dan ubah kembali ektensi pada file”themaster3.exe” menjadi “penting3.zip” seperti pada gambar 4.19



Gambar 4.19 *Rename* file “themaster3.exe” menjadi “penting3.zip”

e. Buka file “penting3.zip” dengan menggunakan winrar, seperti pada gambar 4.20



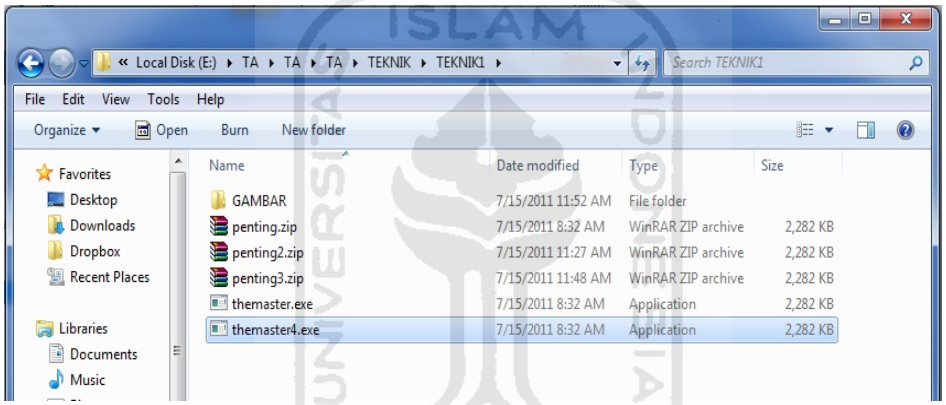
Gambar 4.20 File “penting3.zip” dapat diakses.

Dapat disimpulkan dengan merubah *ASCII header* file menggunakan *software* Hex Editor Neo lebih aman dari pada menggunakan notepad, karena file tersebut

masih dapat diakses kembali pada saat dikembalikan keekstensi awalnya. Seperti pada percobaan yang telah dilakukan diatas.

4.2.3.4 Teknik Keempat

Pada teknik keempat, akan mencoba untuk merubah *signature* file, dengan menggunakan bantuan dari software anti forensik Cygnus Hex Editor. Contoh : mencoba membuat *backup* dari file "themaster.exe" dan diberi nama "themaster4.exe", agar bisa dibedakan antara hasil dari teknik yang pertama, kedua dan ketiga dengan hasil teknik keempat. Seperti pada gambar 4.21 :

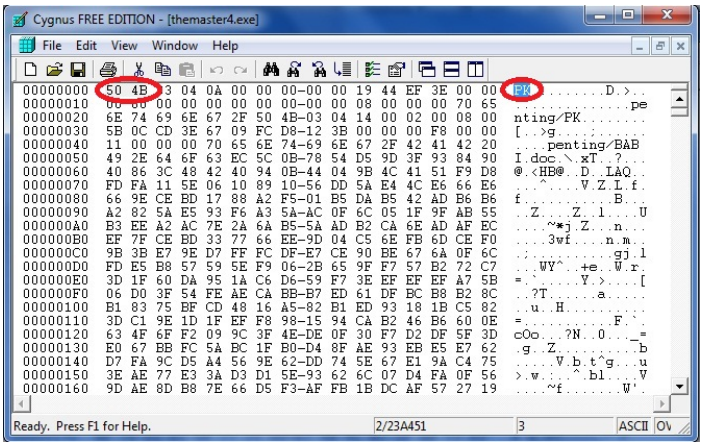


Gambar 4.21 *Backup* file hasil Teknik pertama.

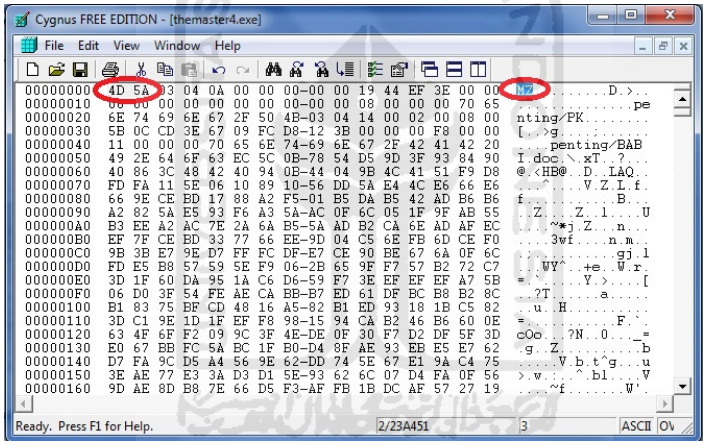
Dari gambar file diatas dapat diketahui bahwa file yang baru dibuat juga terbaca file ekstensinya sebagai .exe oleh *find* standar *windows*. Langkah selanjutnya mencoba agar ekstensi .exe palsu yang dibuat tidak berhasil dikenali oleh software computer forensic yaitu *File Investigator File Find*.

d. Buka file "themaster4.exe" dengan menggunakan Cygnus *Hex Editor*.
e. Ubahlah ASCII *header* pada file "themaster4.exe" dari PK (file .zip) atau *hexadecimal*nya 50 4b diubah menjadi MZ (file .exe) atau *hexadecimal*nya 4d 5a .

   Seperti pada contoh gambar 4.22 : dan gambar 4.23 :



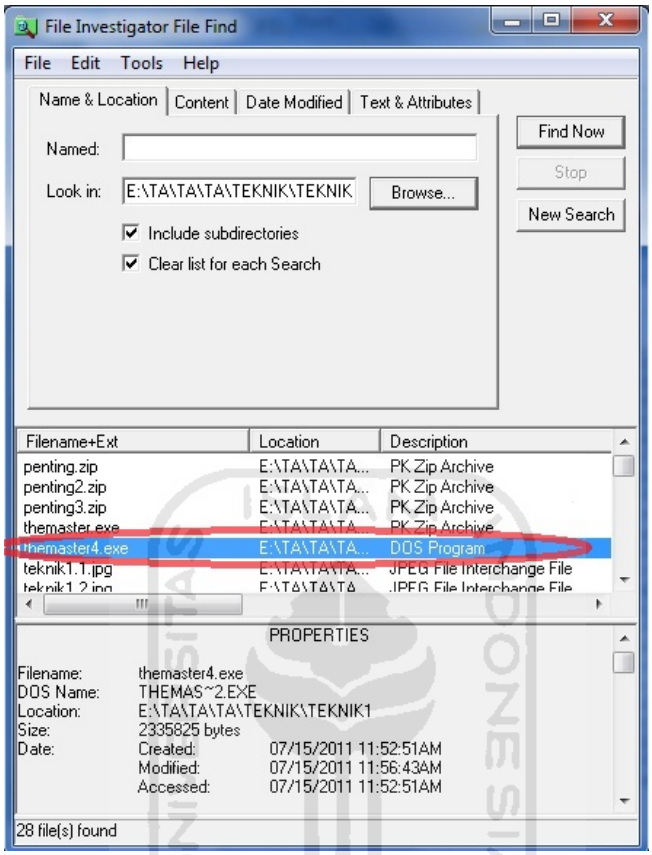
Gambar 4.22 *ASCII Heade*r pada file "themaster4.exe" sebelum diubah.



Gambar 4.23 *ASCII Header* pada file "themaster4.exe" setelah diubah.

f. Kemudian simpanlah file yang telah diubah tersebut.

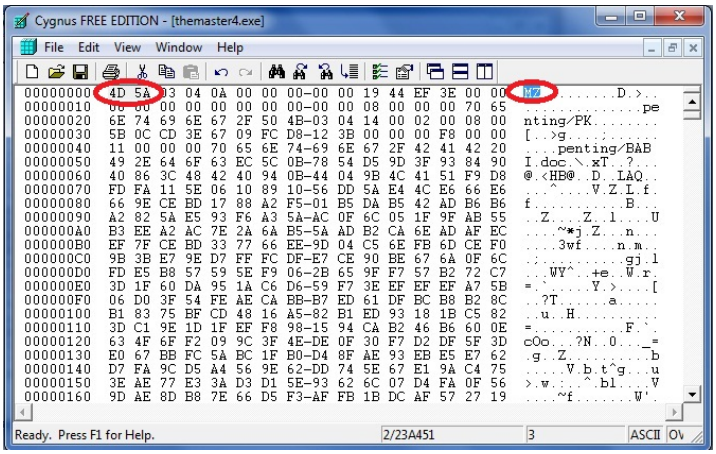
Dan inilah hasil yang didapatkan setelah menggunakan *tool* komputer forensik *File Investigator file find* pada file yang telah diubah *ASCII Header*nya . Seperti terlihat pada gambar 4.24 :



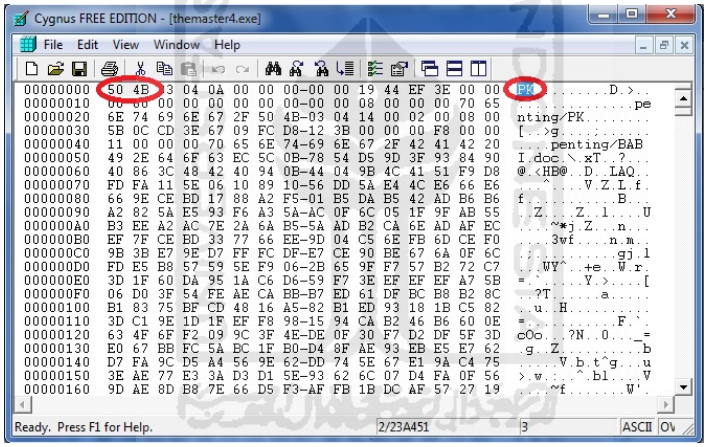
Gambar 4.24 *Tools* forensic tidak mendeteksi ekstensi

Dari teknik keempat diatas dapat dilihat bahwa *software* computer forensic *File Investigator File Find* tidak berhasil mengenali bahwa file “themaster4.exe” yang sebenarnya adalah file .zip tetapi terdeteksinya sebagai file .exe. Dengan bantuan dari software anti forensic Cygnus Hex Editor file “themaster4.exe” dapat dikembalikan seperti semula yaitu file ekstensi .zip dan dapat diakses kembali, seperti pada percobaan berikut :

a. Buka file “themaster4.exe” dengan menggunakan Cygnus *Hex Editor* .
b. Ubahlah ASCII *header* pada file “themaster4.exe” dari MZ (file .exe). Seperti pada contoh gambar 4.25 : dan gambar 4.26 :



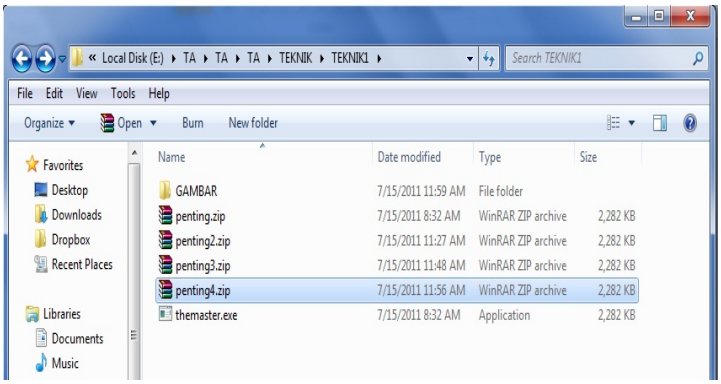
Gambar 4.25 *ASCII Heade*r pada file “themaster4.exe” sebelum diubah.



Gambar 4.26 *ASCII Header* pada file “themaster4.exe” setelah diubah.

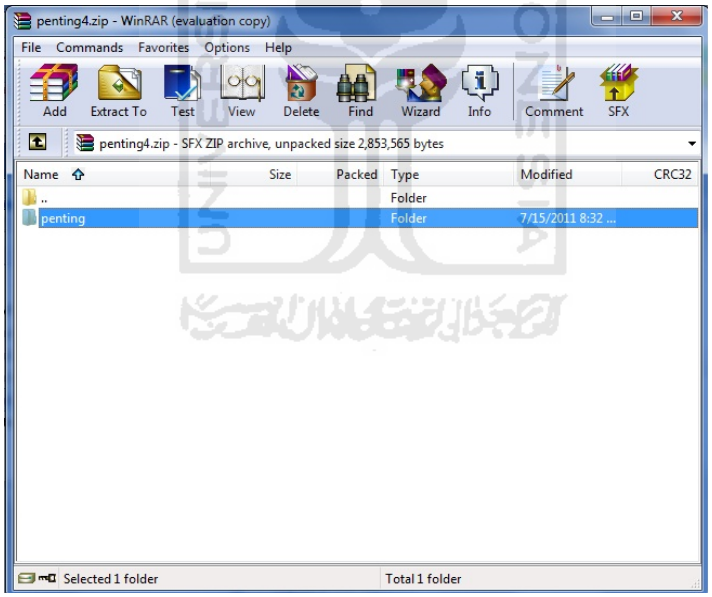
c. Kemudian simpanlah file yang telah diubah tersebut.

d. Rename dan ubah kembali ektensi pada file”themaster4.exe” menjadi “penting4.zip” seperti pada gambar 4.27



Gambar 4.27 Rename file “themaster4.exe” menjadi “penting4.zip”

e. Buka file “penting4.zip” dengan menggunakan winrar, seperti pada gambar 4.28



Gambar 4.28 File “penting4.zip” dapat diakses

Dapat disimpulkan dengan merubah ASCII header file menggunakan software Cygnus Hex Editor sama amannya seperti menggunakan software Hex Editor Neo,

karena file tersebut masih dapat diakses kembali pada saat dikembalikan keekstensi awalnya. Seperti pada percobaan yang telah dilakukan diatas.

4.2.4 Kesimpulan Akhir Penyamaran File

Hasil kesimpulan yang didapatkan setelah melakukan pengujian teknik-teknik diatas adalah sebagai berikut :

Tabel 4.1 Kesimpulan hasil akhir penyamaran file

TEKNIK	METODE	SOFTWARE	PENGUJIAN FORENSIK	PENGEMBALIAN KE FILE AWAL
Teknik 1	Manual(*rename* & merubah ekstensi)	-	Gagal(terdeteksi)	-
Teknik 2	Manual(*rename* & merubah ekstensi)	Notepad	Berhasil(tidak terdeteksi)	Gagal(file error)
Teknik 3	Manual(*rename* & merubah ekstensi)	Hex Editor Neo	Berhasil(tidak terdeteksi)	Berhasil
Teknik 4	Manual(*rename* & merubah ekstensi)	Cygnus Hex Editor	Berhasil(tidak terdeteksi)	Berhasil

4.3 Menyamarkan waktu file

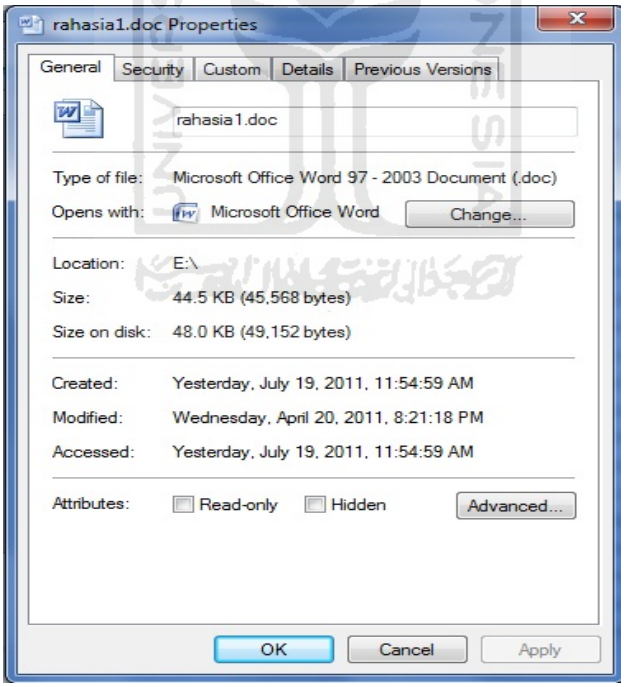
Penyamaran waktu file adalah sebuah teknik untuk merubah pencatatan *timestamp* yang ada dalam sebuah file. Seperti, merubah pencatatan kapan file dibuat, diedit, dan diakses. Sehingga integritas dari file tersebut sudah rusak dan tidak sesuai dengan standar hukum yang ada.

4.3.1 Mencari Masalah

Susuai pengertian dari kata penyamaran waktu file, masalah yang didapatkan adalah bagaimana cara menyamarkan pencatatan waktu file dengan menggunakan metode dan teknik anti forensic agar tidak terdeteksi oleh software forensik.

4.3.2 Menanggapi Masalah

Menanggapi masalah diatas, terlebih dahulu mengetahui pencatatan waktu atau yang biasa disbut *Timestamp* dari suatu file tersebut. Timestamp mencangkup tanggal file dalam sistem yang bersangkutan atau *created*, tanggal file di*edit* atau *modified*, serta tanggal file diakses atau *accesed*, dengan melihat di *properties*. Seperti pada gambar 4.29 :



Gambar 4.9 Tampilan *properties* pada file rahasia1.doc

Tanggal-tanggal yang terbaca di dalam file tersebut bisa bermanfaat dalam penyelidikan komputer forensik. Misalnya saja dari tanggal kita bisa tahu kapan file

tersebt bisa di akses. Ini bisa menjadi bukti atau indikasi atau setidaknya bisa dipakai untuk mempersempit proses pencarian data tertentu.

Penjelasan :

Tanggal file dibuat atau *Created Date* adalah tanggal pertama kali saat file dibuat dalam sistem yang bersangkutan.

Tanggal file diakses atau di *Access Date* kaitannya dengan aksen ke file, seperti *open file, copy, move* dan sebagainya.

Tanggal file dimodifikasi atau ditulis, atau *Modified Date* atau *Last Written Date,* kaitannya kapan file dibuat atau di*edit*.

MFT entry modified kaitannya lebih luas dengan aneka perubahan pada file, misalnya mengubah *parent folder* , juga akan mengubah *MFT entry modified* . *Entry modified* terus berubah mengikuti apapun perubahan pada file. Karena sifatnya, seringkali *entry modified* isinya sesuai dengan *accessed date*. *Entry modified* ini bisa dilihat memakai beberapa *tool* forensik, misalnya *encase*. Tentu saja *MFT entry* juga bisa dilihat dengan tool *TimeStomp* itu sendiri.

Pertama-tama buat sebuah file yang akan digunakan sebagai percobaan penyamaran waktu file, misalanya file tersebut ”rahasia.doc”. Selanjutnya membuat beberapa percobaan dengan menggunakan teknik anti forensik agar file ”rahasia.doc” tersebut rusak integritasnya, dan tidak dapat dijadiakan bukti digital lagi.

Berikut adalah tahap pengujian menggunakan beberapa teknik untuk melakukan percobaan dalam penyamaran waktu file.

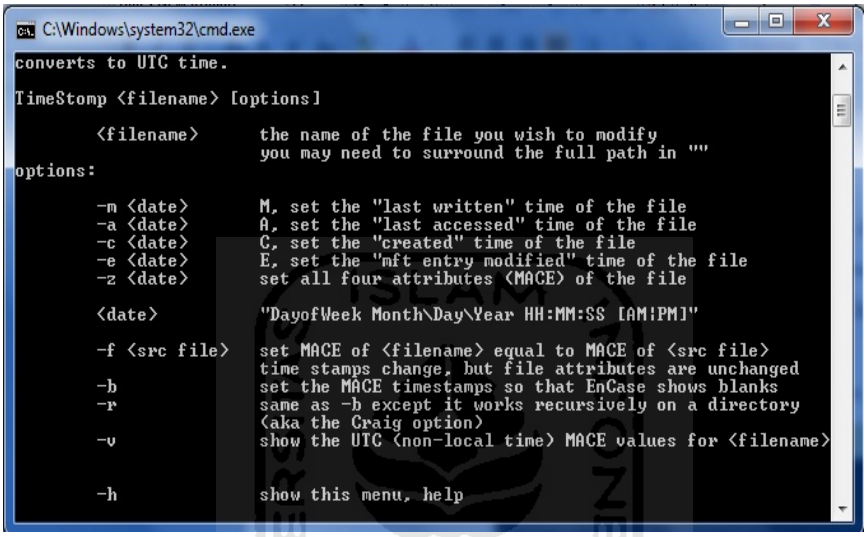
4.3.3 Tahap Pengujian

4.3.3.1 Teknik Pertama

Teknik pertama akan menggunakan bantuan dari salah satu *tool* yang bisa pakai untuk mengganti *Timestamp* tersebut benama *TimeStomp,* yang merupakan salah satu

bagian dari kumpulan tool anti forensik *MAFIA* (*Metasploit Anti Forensic Investigation Arsenal*).

Pertama panggil *tool timestomp*.exe melalui *common prompt*, seperti pada gambar 4.30 :



Gambar 4.30 Tampilan *Options* dari *software Timestomp*

Dari situ dapat diketahui opsional atau perintah apa saja yang dapat dilakukan melalui *timestomp*, atara lain :

-m <tanggal> untuk mengeset tanggal terakhir file ditulis atau dimodifikasi (*modified).*

-a <tanggal> untuk mengeset kapan file diakses (*accesed).*

-c <tanggal> untuk mengeset kapan pertama kali file dibuat pada sistem tersebut (*created).*

-e <tanggal> untuk mengeset kapan perubahan MFT entry terakhir (*MFT entry modified).*

-z <tanggal> untuk mengeset semua atribut baik m,a,c maupun e.

-v untuk menampilkan tanggal M,A,C dan E.

-f (nama file sumber) untuk mengeset file target sama tanggalnya dengan file tertentu.

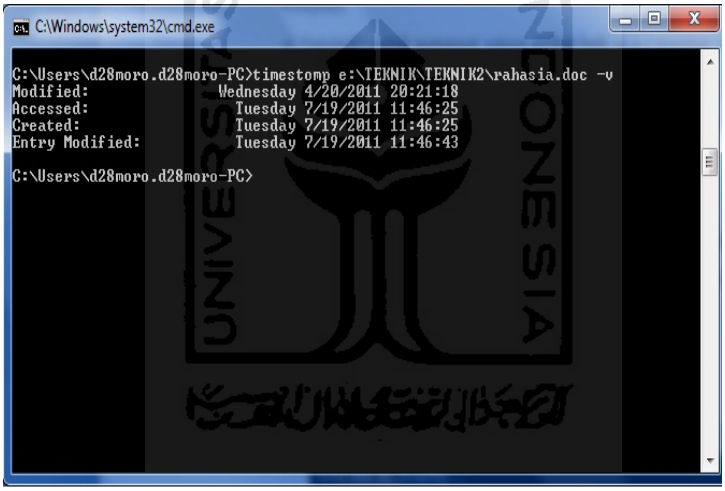
Berikutnya contoh penggunaan tool TimeStomp, seperti :

a. panggil penggunaan timestomp beserta lokasi file nama file yang dinginkan dan kode perintah yang diminta (TimeStomp lokasi file nama file petintah).

   Misalnya menggunakan file rahasiabt.jpg perintah :

   >Timestomp e:\TEKNIK\TEKNIK2\rahasia.doc –v

   Seperti pada gambar 4.31 :



Gambar 4.31 Tampilan *Timpstamp* pada file rahasia.doc

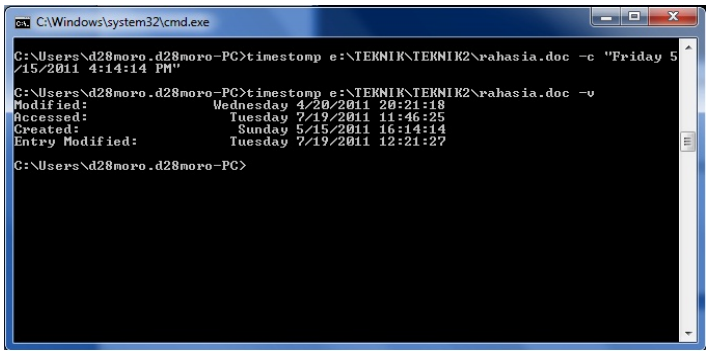
Mencoba untuk mengubah tanggal created dengan perintah :

>TimeStomp e:\TEKNIK\TEKNIK2\rahasia.doc –c ”Friday 5/15/2011 4:14:14 pm”

Lihat hasil ubahan yang telah dilakukan dengan kembali melakukan perintah :

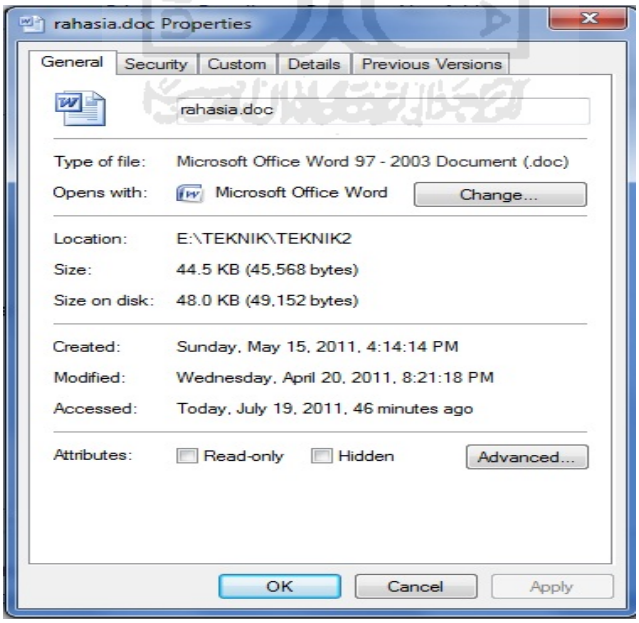
>TimeStomp e:\TEKNIK\TEKNIK2\rahasia.doc –v

Seperti pada gambar 4.32 :



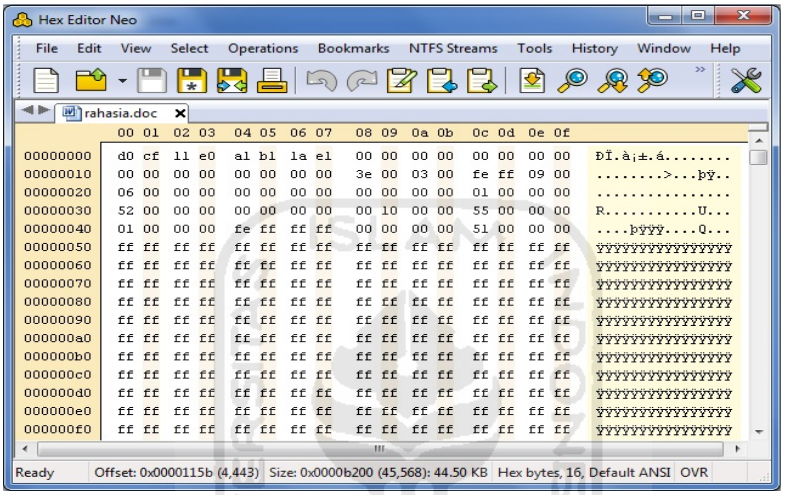
Gambar 4.32 Tampilan perubahan *Timestamp* created pada file rahasia.doc

Dari hasil diatas bisa dilihat bahwa perubahan yang dilakukan tidak sesuai dengan perintahnya, yaitu perintah hari ”Friday” akan tetapi yang berubah menjadi ”sunday”. karena software timestomp ini mencocokkan harinya sesuai dengan tanggal yang diperintahkan. Setelah melakukan perintah diatas mencoba untuk menyamakan dengan file aslinya apakah ubahan yang telah dilakukan akan sama hasilnya dengan properties dari file asli. Seperti pada gambar 4.33 :



Gambar 4.33 Tampilan perubahan properties pada file rahasia.doc

Dari percobaan diatas dapat disimpulkan bahwa penggunaan *software* timestomp dapat mengubah keseluruhan dari pencatatan waktu pada file. Akan tetapi pengubahan yang dilakukan menggunakan *tool timestomp* tidak terdeteksi sebagai modifikasi yang telah dilakukan terhadap file. Seperti pada gambar 4.34 :

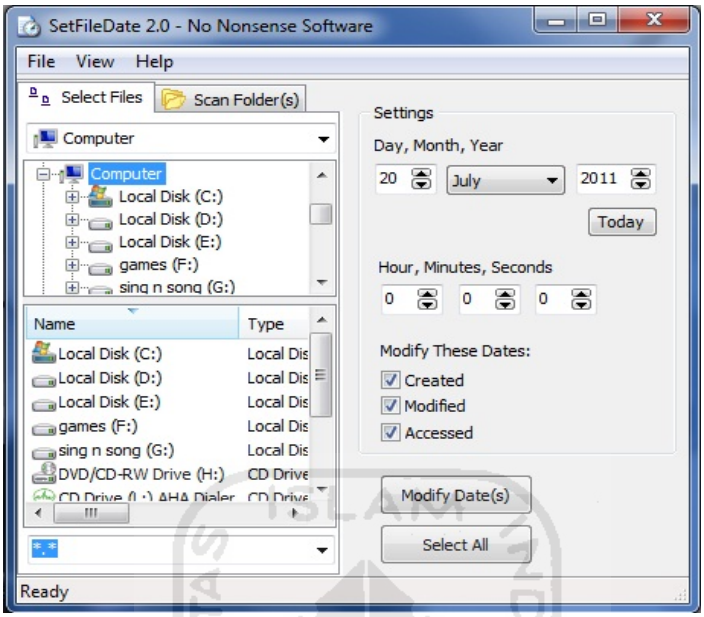


Gambar 4.34 Tampilan pengecekan menggunakan *software Hex Editor*

4.3.3.2 Teknik Kedua

Teknik kedua akan menggunakan bantuan dari software anti komputer forensik yaitu SetFileDate untuk mengganti pencacatan waktu Timestamp. Membuat backup terlebih dahulu untuk membedakan antara mengganti pencatatan waktu pada teknik pertama dengan teknik kedua, file hasil backup diberinama file ”rahasia2.doc”.

Pertama panggil *tool SetFileDate*, seperti pada gambar 4.35 :



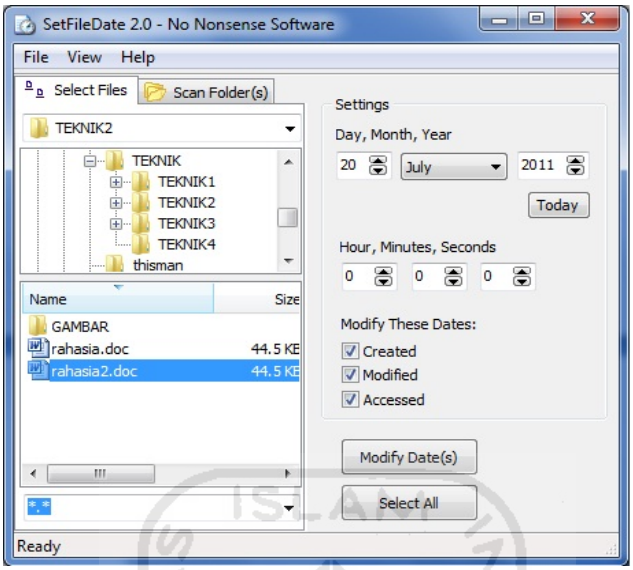
Gambar 4.35 Tampilan dari *software SetFileDate*

Dari situ dapat diketahui opsional atau perintah apa saja yang dapat dilakukan melalui *SetFileDate*.

Berikutnya penggunaan tool SetFileDate, seperti :

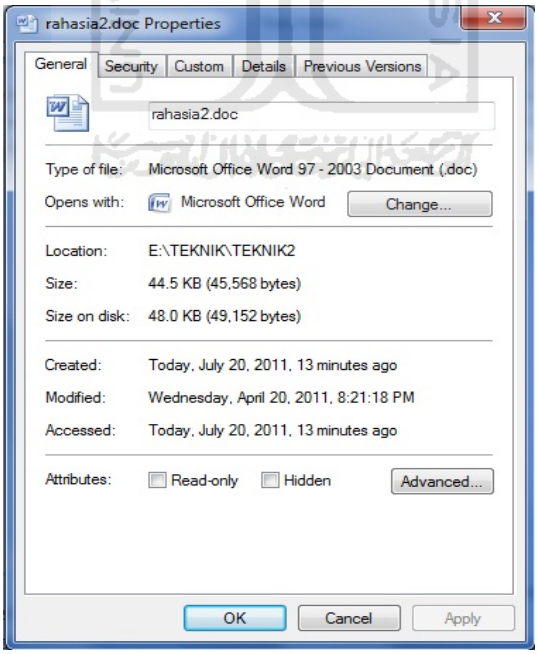
a. Tentukan file yang ingin diubah timestampnya terlebih dahulu, misalanya file ”rahasia2.doc”

   Seperti pada gambar 4.36 :



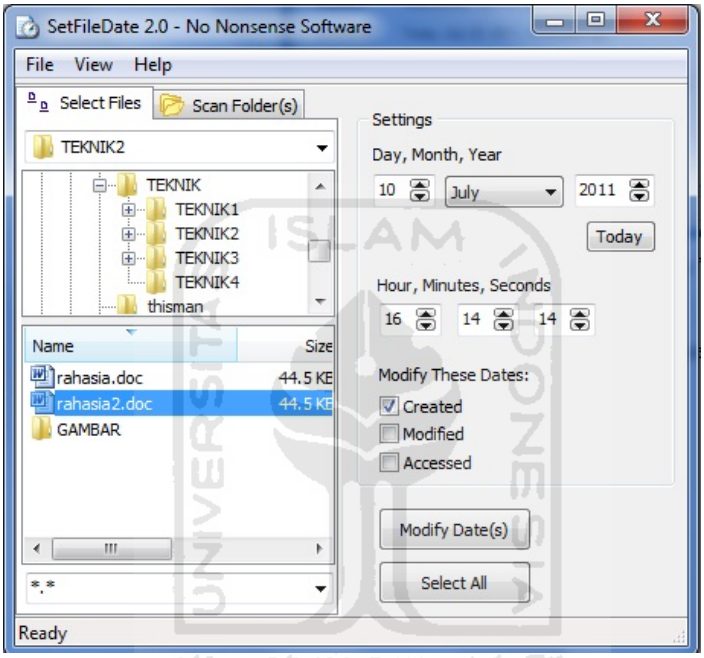
Gambar 4.36 Tampilan file rahasia2.doc pada software *SetFileDate*

b. Buka propertise pada file ”rahasia2.doc”, agar dapat mengetahui timestamp awalnya. Seperti pada gambar 4.37 :



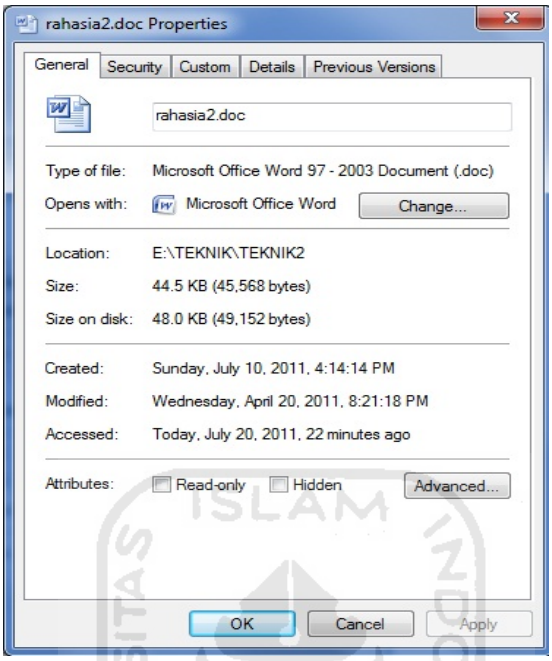
Gambar 4.37 Tampilan *timestamp* pada propertise file ”rahasia2.doc”

c. Mencoba untuk mengubah tanggal created menjadi tanggal ”10 july 2011 jam 4:14:14 PM”
Seperti pada gambar 4.38:



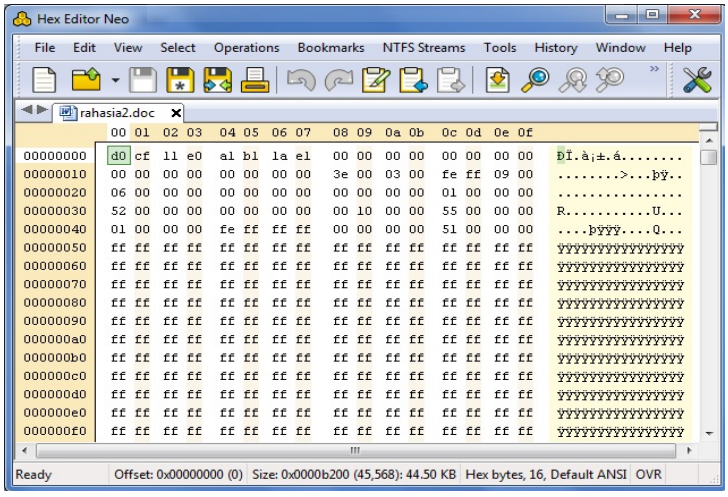
Gambar 4.38 Tampilan merubah *timestamp* created pada file rahasia2.doc

Setelah melakukan perintah diatas mencoba untuk melihat timestamp file aslinya apakah ubahan yang telah dilakukan akan sama hasilnya dengan properties pada file asli. Seperti pada gambar 4.39 :



Gambar 4.39 Tampilan perubahan properties file rahasia2.doc

Dari percobaan diatas dapat disimpulkan bahwa penggunaan software SetFileDate dapat mengubah keseluruhan dari pencatatan waktu pada file. Akan tetapi pengubahan yang dilakukan menggunakan *tool timestomp* tidak terdeteksi sebagai modifikasi yang telah dilakukan terhadap file. Seperti pada gambar 4.40 :

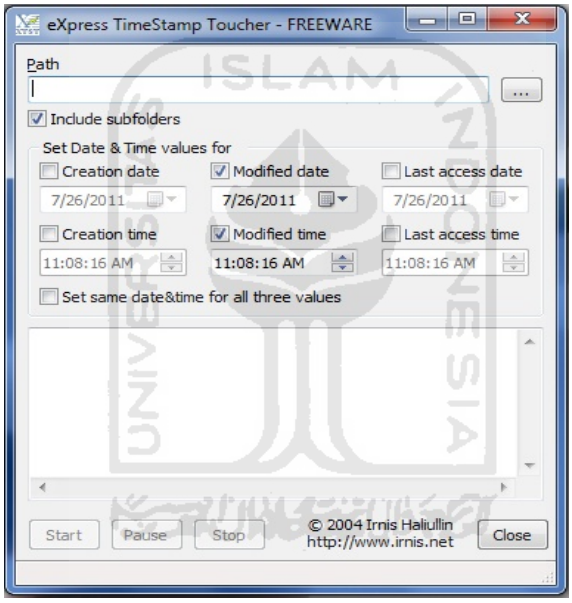


Gambar 4.40 Tampilan pengecekan menggunakan *software Hex Editor*

4.3.3.3 Teknik Ketiga

Teknik ketiga akan menggunakan bantuan dari software anti komputer forensik yaitu eXpress TimeStamp Toucher untuk mengganti pencacatan waktu Timestamp pada file rahasia.doc. Membuat backup terlebih dahulu untuk membedakan antara mengganti pencatatan waktu pada teknik pertama,teknik kedua, dan teknik ketiga. file hasil backup diberinama file ”rahasia3.doc”.

Pertama panggil *tool* eXpress TimeStamp Toucher, seperti pada gambar 4.41 :

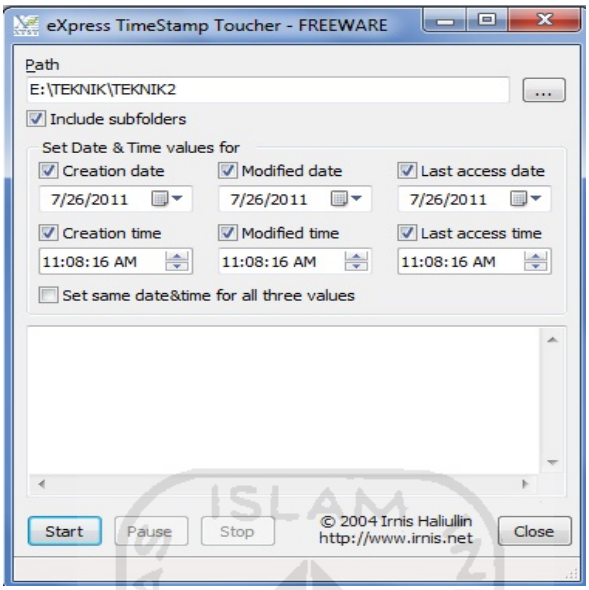


Gambar 4.41 Tampilan dari *software eXpress TimeStamp Toucher*

Dari situ dapat diketahui opsional atau perintah apa saja yang dapat dilakukan melalui eXpress TimeStamp Toucher.

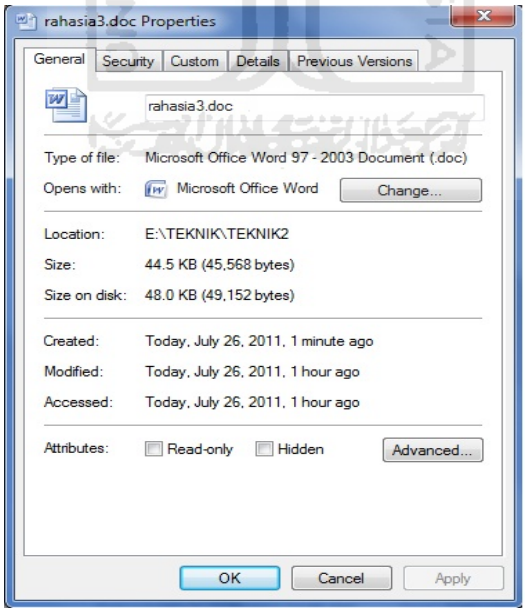
Berikutnya penggunaan tool eXpress TimeStamp Toucher, seperti :

a. Tentukan folder yang ingin diubah timestampnya terlebih dahulu, misalanya pada folder ”TEKNIK2”
   Seperti pada gambar 4.42 :



Gambar 4.42 Tampilan folder ”TEKNIK2” pada *eXpress TimeStamp Toucher*

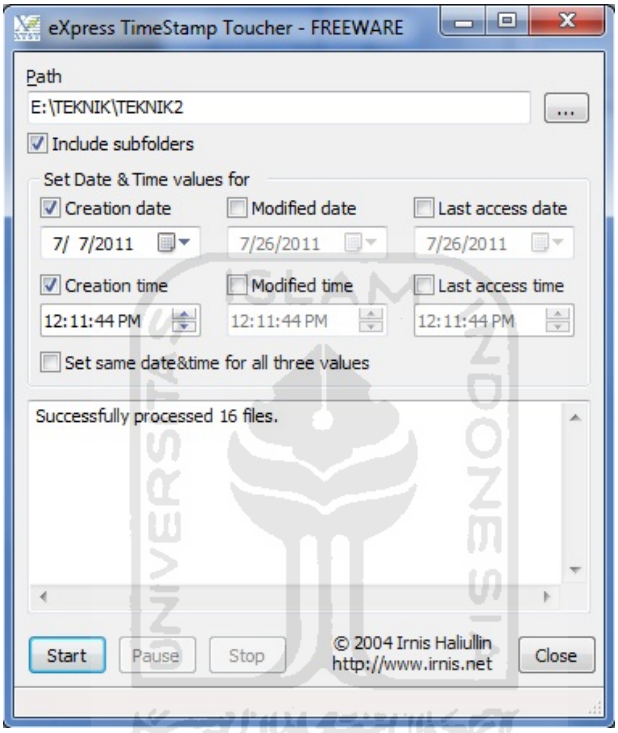
b. Buka propertise pada file ”rahasia3.doc”, agar dapat mengetahui timestamp awalnya. Seperti pada gambar 4.43 :



Gambar 4.43 Tampilan *timestamp* pada propertise file ”rahasia3.doc”

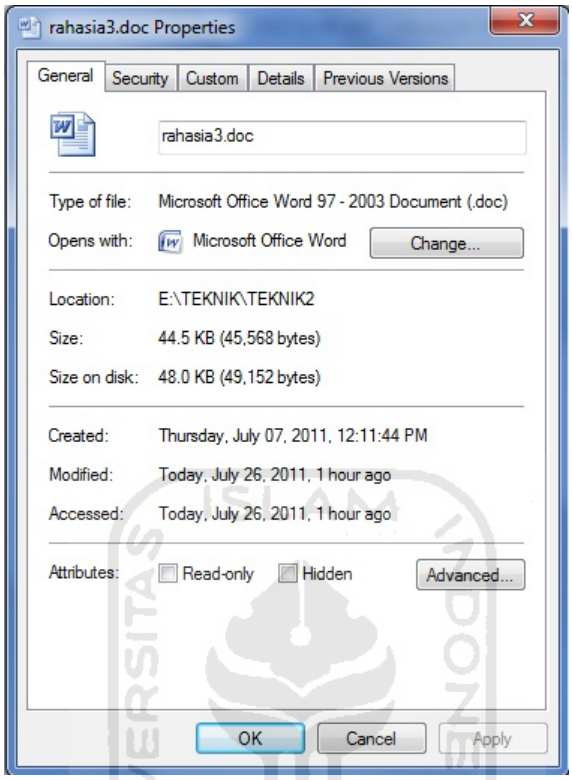
c. Mencoba untuk mengubah tanggal created menjadi tanggal ”7 july 2011 jam 12:11:14 PM”

Seperti pada gambar 4.44 :



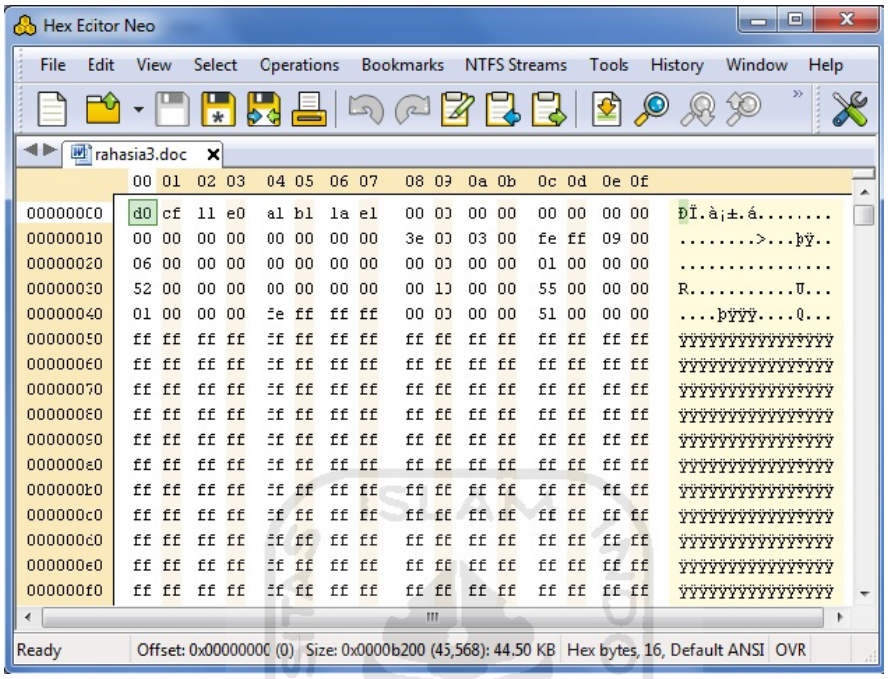
Gambar 4.44 Tampilan merubah *timestamp* created pada folder ”TEKNIK2”

Setelah melakukan perintah diatas mencoba untuk melihat timestamp file aslinya apakah ubahan yang telah dilakukan akan sama hasilnya dengan properties pada file asli. Seperti pada gambar 4.45 :



Gambar 4.45 Tampilan properties yang terjadi pada file ”rahasia3.doc”

Dari percobaan diatas dapat disimpulkan bahwa penggunaan software eXpress TimeStamp Toucher dapat mengubah keseluruhan dari pencatatan waktu pada file. Akan tetapi software eXpress TimeStamp Toucher hanya dapat mengubah timestamp seluruh file yang ada didalam sebuah folder, tidak sepesifik langsung kefile yang dituju atau yang diinginkan. Akan tetapi pengubahan yang dilakukan menggunakan *tool timestomp* tidak terdeteksi sebagai modifikasi yang telah dilakukan terhadap file. Seperti pada gambar 4.46 :



Gambar 4.46 Tampilan pengecekan menggunakan *software Hex Editor*

Dari ketiga teknik dalam menyamarkan waktu file diatas tidak ditemukan ada yang terdeteksi dalam bilangan hexadecimalnya bahwa telah terjadi modifikasi.

4.3.4 Argumen Ketidak Sesuaian

Dari ketiga teknik diatas tidak dapat menampilkan bagaimana contoh kegagalan (yang berhasil terdeteksi oleh *software* komputer forensik), karena untuk sampai saat ini yang berhasil mendeteksi penyamaran *timestamp* hanya *software* komputer forensik *FTK academic*. Dikarenakan keterbatasan penggunaan sehingga tidak dapat menampilkannya disini.

4.3.5 Kesimpulan Akhir Penyamaran Waktu File

Hasil kesimpulan yang didapatkan setelah melakukan pengujian teknik-teknik diatas adalah sebagai berikut :

Tabel 4.2 Kesimpulan hasil akhir penyamaran waktu file

TEKNIK	SOFTWARE	PENGUJIAN FORENSIK
Teknik 1	Timestomp	Berhasil (tidak terdeteksi)
Teknik 2	SetFileDate	Berhasil (tidak terdeteksi)
Teknik 3	eXpress Timestamp Toucher	Berhasil (tidak terdeteksi)

4.4 Secure Delete

Secure delete adalah sebuah teknik untuk melakukan penghapusan file dengan benar-benar dihapus atau sebagian data tidak bisa dipulihkan lagi dengan *software recovery* data. Agar data yang sudah dihapus atau data yang sudah terhapus tidak dapat diakses bahkan disalah gunakan oleh orang lain.

4.4.1 Mencari Masalah

Susuai pengertian dari kata secure delete, masalah yang didapatkan adalah bagaimana cara secure delete dengan menggunakan metode dan teknik anti forensic agar tidak dapat direcovery kembali.

4.4.2 Menanggapi Masalah

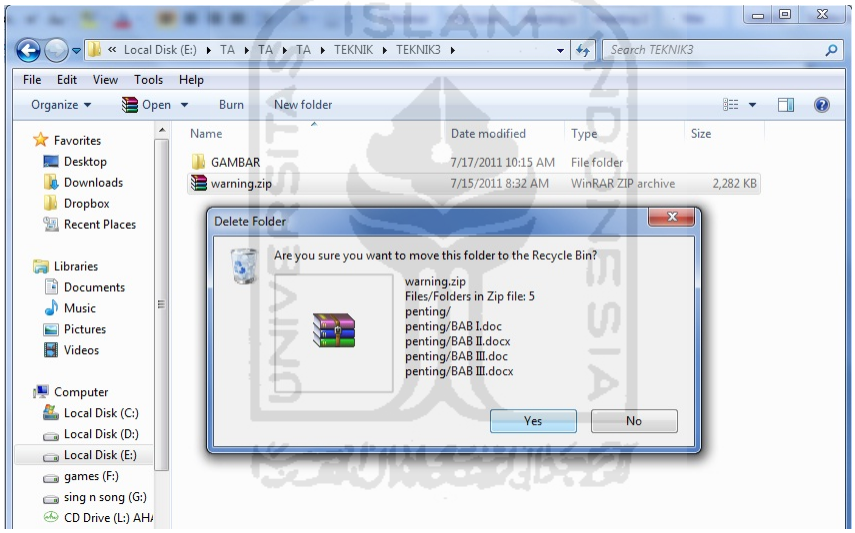
Menanggapi masalah diatas, dengan mencoba melakukan penghapus file tertentu yang diinginkan secara aman atau secure delete sehingga file tersebut tidak dapat ditemukan, direcovery, maupun diakses kembali oleh siapapun. Terlebih dahulu buatlah sebuah file yang akan dijadikan contoh percobaan untuk melakukan secure delete, misalnya file tersebut diberi nama ”warning.zip”. selanjutnya melakukan

beberapa percobaan dengan menggunakan teknik anti forensik untuk scure delete file ”warning.zip” tersebut. Berikut adalah pengujian menggunakan beberapa teknik untuk mencoba melakukan scure delete.

4.4.3 Tahap Pengujian

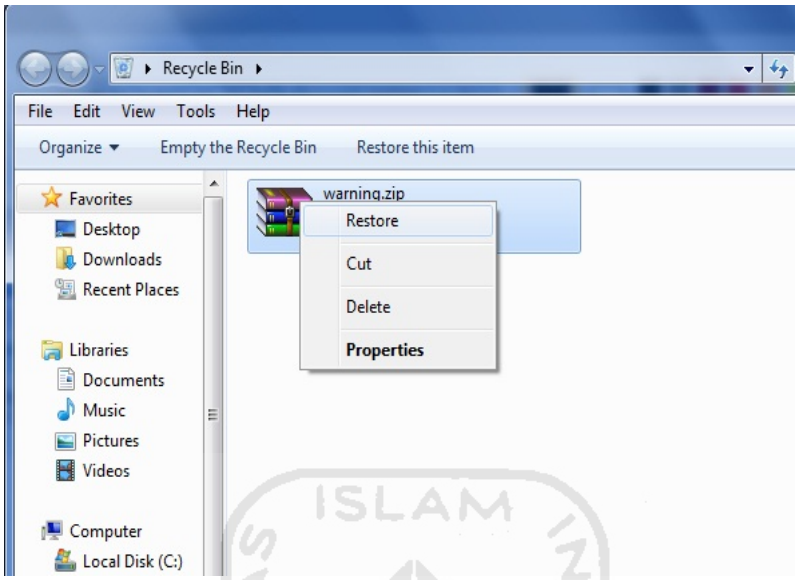
4.4.3.1 Teknik Pertama

Teknik pertama mencoba untuk menghapus file warning.zip dengan cara sederhana yaitu dengan melakukan *delete* biasa melalui menu pada *windows*, seperti gambar 4.47:



Gambar 4.47 Tampilan *delete* file warning.zip menggunakan *menu delete*

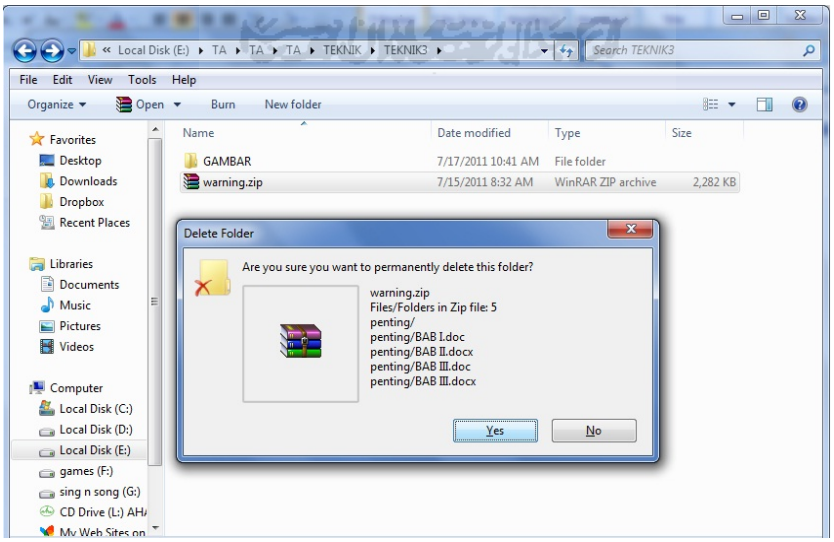
File warning.zip yang telah dihapus di atas dengan cara men*delete* biasa akan menyebabkan file tersebut terkirim ke *recycle bin*, *trash* dan sebagainya. File yang masuk ke *recycle bin* akan sangat mudah untuk dipulihkan kembali sehingga menyebabkan file tersebut dapat diakses kembali atau file tersebut tidak terhapus permanen. Seperti pada gambar 4.48:



Gambar 4.48 Tampilan me*restore* kembali file warning.zip dari *recycle bin*

4.4.3.2 Teknik Kedua

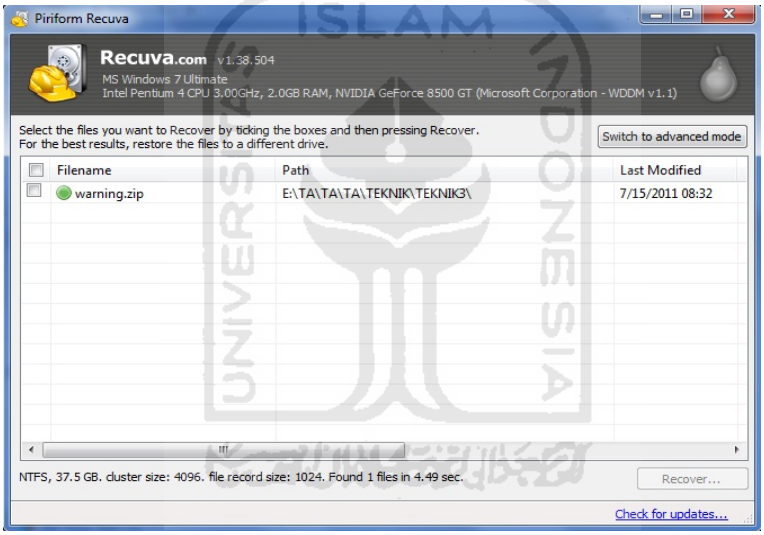
Teknik kedua yang akan dilakukan dengan cara menghapus permanen file warning.zip dengan menekan tombol shift dan tombol delete secara bersamaan. Seperti pada gambar 4.49:



Gambar 4.49 Menghapus file warning.zip dengan *shift + delete*

File warning.zip yang telah di hapus dengan menekan tombol *shift* + *delete* atau *delete* permanen akan menyebabkan file tersebut hilang dari direktori dan juga tidak terdapat didalam *recycle bin*. Untuk membuktikan apakah file tersebut telah berhasil di*delete* permanen akan dibuktikan menggunakan *software data recovery* yaitu recuva.

Mencoba untuk melakukan *recovery* dilokasi file yang telah di*delete* diatas. Setelah selesai melakukan proses *recovery data*, file yang telah dihapus diatas ternyata berhasil ditemukan oleh *software data recovery* recuva. Seperti pada gambar 4.50:

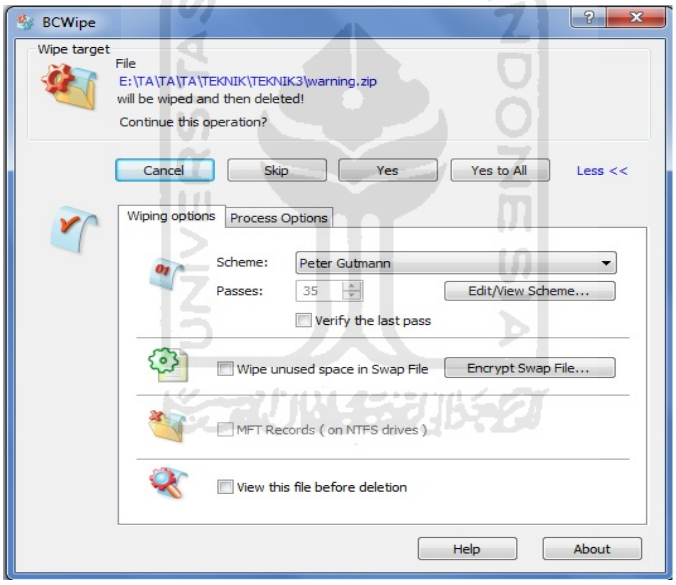


Gambar 4.50 *Software* recuva mendeteksi file “warning.zip”

File warning.zip yang berhasil ditemukan diatas akan dicoba untuk di *recovery* kembali melalu *software* recuva. Dari contoh diatas terlihat bahwa menghapus file secara permanen dengan menggunakan cara menekan tombol *shift* + *delete* masih dapat dipulihkan kembali, sehingga masih belum bisa dapat dikatakan sebagai *scure delete*.

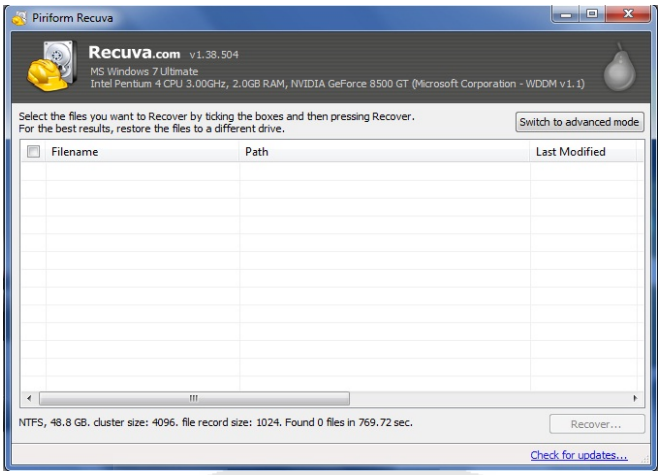
4.4.3.3 Teknik Ketiga

Teknik ketiga menghapus file dengan bantuan *software* anti forensik yaitu BCwipe. Selanjutnya mencoba kembali untuk menghapus file warning.zip yang berhasil di*recovery* diatas dengan menggunakan *software* BCwipe. Pada *software* BCwipe terdapat banyak teknik untuk menghapus file dengan cara menimpa dengan data *random* maupun dengan data tertentu. Sebagai contoh : metode German BCI melakukan proses penimpaan sebanyak tujuh kali, sedangkan metode Peter Gutmann melakukan proses penimpaan sebanyak tiga puluh lima kali. Agar lebih aman mencoba untuk menggunakan metode Peter Gutmann yaitu melakukan penimpaan sebanyak tiga puluh lima kali. Seperti pada gambar 4.51:



Gambar 4.51 Tampilan opsional penghapusan pada *software* BCWipe

Setelah berhasil menghapus file warning.zip dengan menggunakan *software* BCwipe, mencoba untuk me*recovery* file tersebut apakah masih bisa terdeteksi dan di*recovery* atau sudah tidak terdeteksi. Seperti pada gambar 4.52

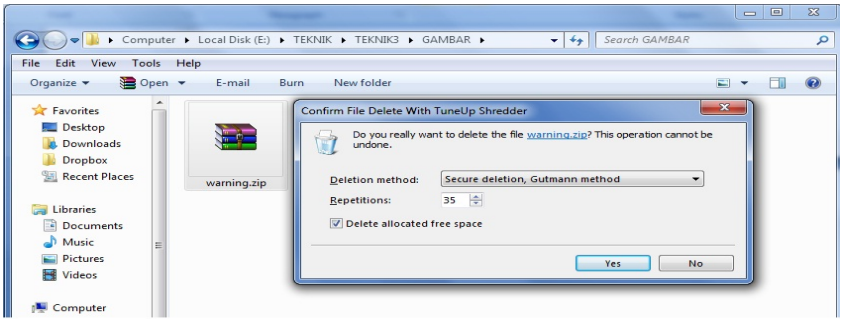


Gambar 4.52 File warning.zip tidak terdeteksi lagi oleh *software* recuva

Dari hasil recovery diatas dapat dibuktikan bahwa file yang telah dihapus dengan menggunakan software BCwipe tidak terdeteksi oleh recuva sehingga file tersebut sudah berhasil didelete secara permanen dan tidak bisa direcovery kembali.

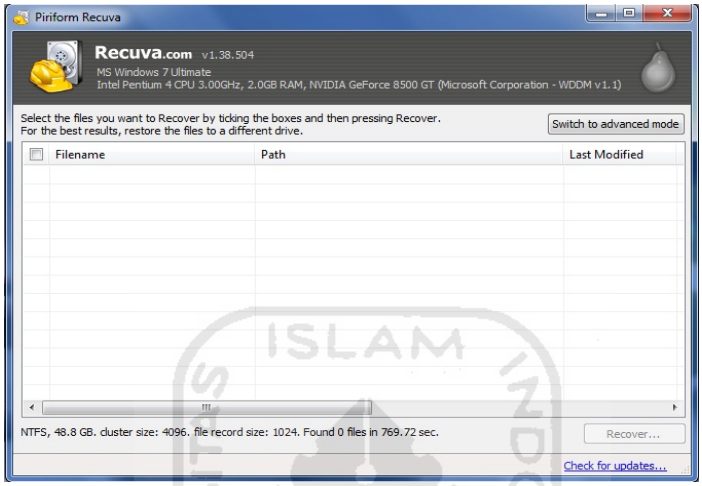
4.4.3.4 Teknik Keempat

Percobaan kempat menghapus file dengan bantuan *software* anti forensik yaitu TuneUp Utility. Selanjutnya membuat kembali sebuah file yang diberi nama "warning.zip" dan mencoba kembali untuk menghapus file "warning.zip" tersebut. Pada *software* TuneUp Utility kembali menggunakan metode Peter Gutmann yaitu melakukan penimpaan sebanyak tiga puluh lima kali. Seperti pada gambar 4.53:



Gambar 4.53 Tampilan opsional penghapusan pada *software* TuneUp Utility.

Setelah berhasil menghapus file warning.zip dengan menggunakan *software* TuneUp Utility, mencoba untuk me*recovery* file tersebut apakah masih bisa terdeteksi dan di*recovery* atau sudah tidak terdeteksi. Seperti pada gambar 4.54:



Gambar 4.54 File warning.zip tidak terdeteksi lagi oleh *software* recuva

Dari hasil recovery diatas dapat dibuktikan bahwa file yang telah dihapus dengan menggunakan software TuneUp Utility tidak terdeteksi oleh recuva sehingga file tersebut sudah berhasil didelete secara permanen dan tidak bisa direcovery kembali.

4.4.4 Kesimpulan Akhir Secure Delete

Hasil kesimpulan yang didapatkan setelah melakukan pengujian teknik-teknik diatas adalah sebagai berikut :

Tabel 4.3 Kesimpulan hasil akhir *secure delete*

TEKNIK	SOFTWARE	METODE YANG DIGUNAKAN	PENGUJIAN FORENSIK
Teknik 1	-	Manual (menggunakan menu delete biasa)	Gagal (dapat direstore kembali)

Teknik 2	-	Manual (menggunakan tombol Shift + Delete)	Gagal (dapat direcovery kembali)
Teknik 3	BCWipe	Metode Peter Gutmann	Berhasil (tidak dapat direcovery)
Teknik 4	TuneUp Utility	Metode Peter Gutmann	Berhasil (tidak dapat direcovery)

4.5 History Cleaner

History cleaner atau jejak-jejak yang ada atau dibuat oleh sistem operasi, *software*, situs dan sebagainya. Sehingga jejak-jejak tersebut tidak bisa deketahui oleh siapapun.

4.5.1 Mencari Masalah

Susuai pengertian dari kata *history cleaner*, masalah yang didapatkan adalah bagaimana cara *history cleaner* pada jejak penggunaan *Microsoft office* 2003 maupun 2007, dengan menggunakan metode dan teknik anti forensik.

4.5.2 Menanggapi masalah

Menanggapi masalah diatas, terlebih dahulu mengetahui software yang akan digunakan untuk history cleaner. Apakah software tersebut dapat menggunakan metode secure delete history atau tidak, dan apakah software tersebut suport dengan aplikasi yang akan dihapus historynya.

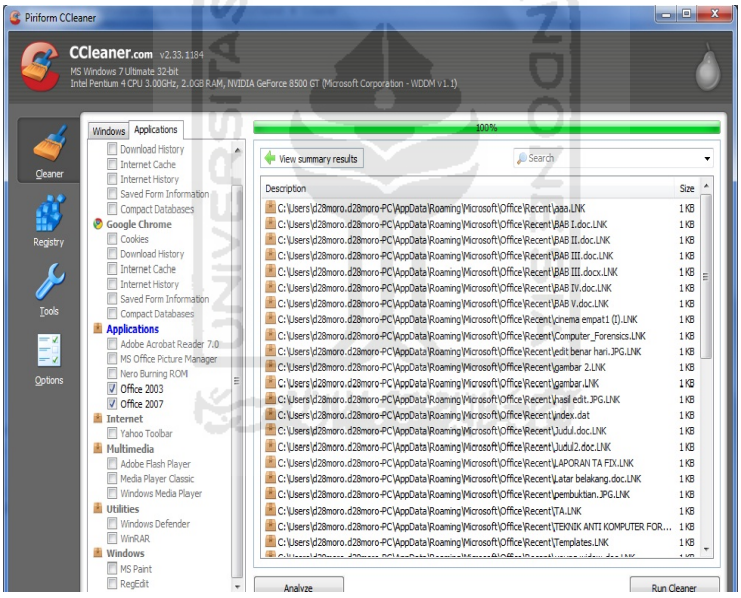
Berikut adalah tahap pengujian dengan menggunakan teknik dan metode anti forensik pada history cleaner.

4.5.3 Tahap Pengujian

4.5.3.1 Teknik Pertama

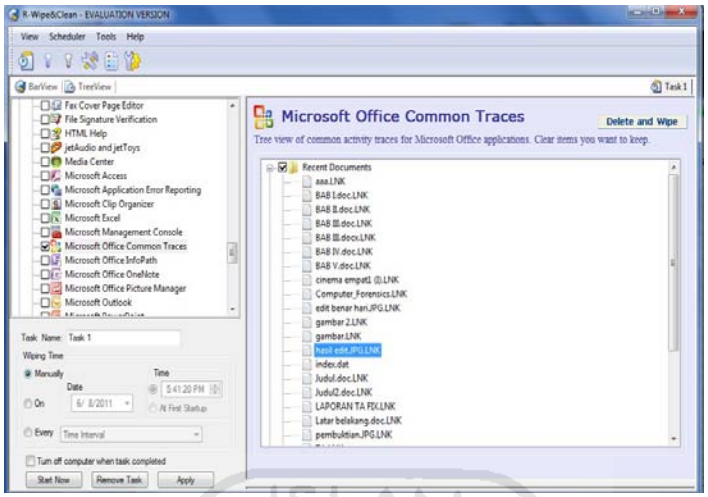
Teknik pertama yaitu menghapus *history* secara aman, yaitu dengan cara :

a. Mencoba untuk menggunakan *software* CCleaner yang berfungsi untuk menghapus *history-history* yang dibuat oleh sistem operasi, *software*, situs dan sebagainya.
b. Mencoba menggunakan *software* R-Wipe&Cleane untuk membuktikan apakah proses penghapusan *history* tersebut berhasil atau tidak berhasil terdeteksi oleh *software* forensic.
c. Pilihlah *history* dari aplikasi yang ingin dihapus dengan menggunakan CCleaner, misalnya aplikasi Office 2003 dan 2007.
d. *Analyze history* dari aplikasi yang telah dipilih, sehingga terlihat *history* yang ada pada aplikasi tersebut. Seperti pada gambar 4.55



Gambar 4.55 Tampilan *analyze history* di software CCleaner

e. Lakukan hal yang sama pada software R-Wipe&Cleane sehingga dapat dibandingkan history yang ada pada aplikasi yang telah dipilih. Seperti pada gambar 4.56:

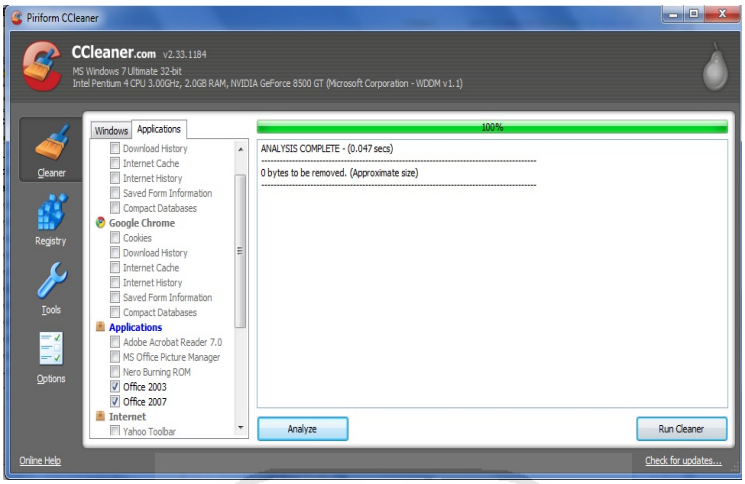


Gambar 4.56 Tampilan analyze history disoftwere R-Wipe&Clean

f. Lakukan pengubahan setingan pada CCleaner dengan menggunakan secure delete dan menggunakan metode Peter Gutmann. Seperti pada gambar 4.57 :

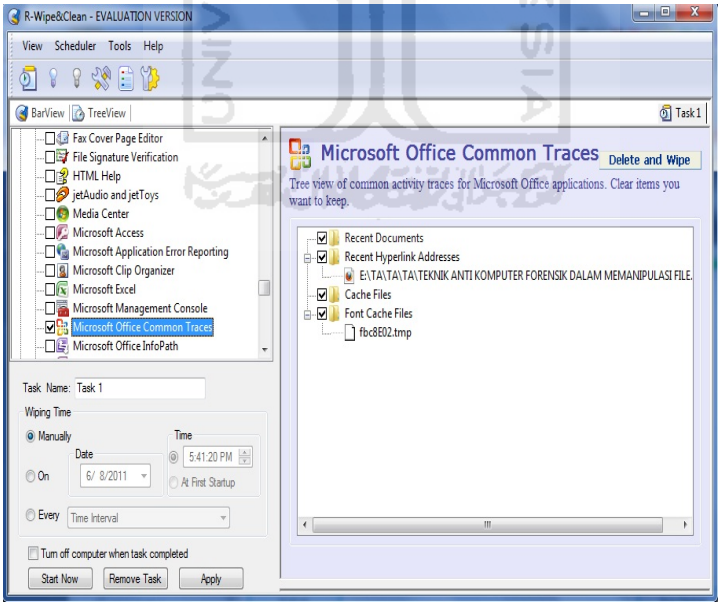
Gambar 4.57 Setting *secure file delete*

g. Lakukan penghapusan history dari aplikasi yang telah dipilih pada CCleaner, seperti pada gambar 4.58:



Gambar 4.58 Tampilan penghapusan history

h. Lakukan pembuktian dengan menscan kembali history pada aplikasi yang telah dipilih dengan menggunakan R-Wipe&Cleane, seperti pada gambar 4.59:



Gambar 4.59 Tampilan *analyze history* pada R-Wipe&Cleane

Sehingga dapat disimpulkan penghapusan yang telah dilakukan barusan berhasil tidak terdeteksi oleh software R-Wipe&Cleane atau *software* komputer forensik.

4.5.4 Kesimpulan Akhir History Cleaner

Hasil kesimpulan yang didapatkan setelah melakukan pengujian teknik-teknik diatas adalah sebagai berikut :

Tabel 4.4 Kesimpulan akhir history cleaner

TEKNIK	METODE	PENGUJIAN FORENSIK
Teknik 1	Peter Gutmann	Berhasil (tidak terdeteksi)

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah menyelesaikan teknik anti komputer forensik untuk memanipulasi file ini, kemudian dilakukan pengujian menggunakan teknik komputer forensik. Maka diambil kesimpulan sebagai berikut :

1. Teknik anti komputer forensik untuk manipulasi file dibagi menjadi 4 teknik yaitu :
    a. Teknik penyamaran file : melakukan penyamaran file dengan rename file, mengubah ekstensinya, dan mengubah kode *ASCII*nya pada satu file bisa membuat file tersebut tidak dapat terdeteksi oleh *software scanner* forensik, sehingga ini adalah solusi yang cukup aman untuk mengamankan file pribadi yang penting.
    b. Teknik penyamaran waktu file : melakukan penyamaran pencatatan waktu file atau *timestamp* dengan menggunakan software anti forensik pada saat ini cukup baik untuk merusak integritas suatu file, karena sangat minimnya software forensic yang bisa mendeteksi perubahan yang terjadi pada *timestamp* yang menyebabkan file tersebut rusak integritasnya.
    c. Teknik Secure Delete : melakukan secure delete dengan software anti forensik dan menggunakan metode Peter Gutmann cukup baik untuk menghapus file-file penting yang tidak ingin diakses kembali, karena dengan menggunakan teknik tersebut file-file yang telah di*secure delete* tidak dapat di*recovery* kembali oleh *software* forensik.
    d. History Cleaner : melakukan history cleaner dengan bantuan *software* anti forensik dan menggunakan metode Peter Gutmann cukup baik digunakan untuk menghapus *history* komputer, karena dengan menggunakan teknik tersebut *history* yang telah dibersihkan tidak dapat dideteksi oleh *software* forensik

2. Teknik anti komputer forensik untuk memanipulasi file adalah sebuah teknik yang membantu seseorang untuk berusaha melindungin data-data pribadinya dari orang lain.
3. Penggunaan teknik anti forensik bertujuan untuk menyulitkan pakar komputer forensik sehingga membutuhkan waktu dan proses yang jauh lebih lama untuk mencari data-data yang mereka butuhkan. Tentu yang paling ideal adalah jika data-data tersebut tidak berhasil ditemukan. Akan tetapi jika data tersebut berhasil ditemukan, maka harus diupayakan bahwa data tersebut sudah terganggu intgritasnya.

5.2 Saran

Saran untuk pengembangan teknik anti komputer forensik untuk memanipulasi file lebih lanjut adalah :

1. Dapat menutupi kelemahan-kelemahan yang ada pada penelitian ini dan dapat melanjutkan penelitian ini (file.bat) yang dapat memanipulasi seluruh jenis file yang ada dikomputer secara bersamaan (satu kali klik).
2. Selalu *Uptodate* dalam informasi perkembangan teknologi baik itu *software* komputer forensik maupun *software* anti komputer forensik karena teknologi akan selalu berkembang sehingga teknik anti komputer forensik yang akan digunakan harus mengikuti perkembangan dari *software* komputer forensik itu sendiri.

DAFTAR PUSAKA

[HAM10] Hamid. 2010. *Computer forensic slide*. Pengenalan Komputer Forensik. Kampus UII Terpadu, Jogjakarta 2010.

[BUD11] Budiman, Rahmadi. 2003. Komputer Forensik Apa dan Bagaimana (online) at http://www.cert.or.id/~budi/courses/ec7010/2003/rahmadi-report.pdf, diunduh pada tanggal 25 Juni 2011.

[ARR10] Arryawan, Eko & SmitDev Community. 2010. Anti Forensik. PT Elex Media Komputindo.

[WIK11] Wikipedia. 2011. *Anti Computer Forensics* (online) at http://en.wikipedia.org/wiki/Anti-computer_forensics#cite_note-rogers-0. Diunduh pada tanggal 24 Juni 2011.

[WIC11] Wicaksana, Adi. 2010. Pengertian ASCII dan Tabel Kode ASCII (online). At http://blog.uad.ac.id/adiwicaksana/2010/05/11/pengertian-ascii-dan-tabel-kode-ascii/ diunduh pada tanggal 23 Juni 2011.

[WIK10] Wikipedia. 2010. *Timestamp* (online). At http://en.wikipedia.org/wiki/Timestamp diunduh pada tanggal 24 Desember 2010.

[MAX11] Max. 2009. *Modify NTFS Timestamps and Cover Your Tracks With Timestomp*.exe (online). at http://www.anti-forensics.com/modify-ntfs-timestamps-and-cover-your-tracks-with-timestomp diunduh pada tanggal 25 Juni 2011.

[GUT11] Gutmann, Peter. 1996. *Secure Deletion of Data from Magnetic and Solid-State Memory* (online). At http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html Diunduh pada tanggal 25 Juni 2011.

LAMPIRAN