

**ANALISIS *VIRTUAL MACHINE*
UNTUK KEPERLUAN
KOMPUTER FORENSIK**

TUGAS AKHIR

**Diajukan sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana
Jurusan Teknik Informatika**

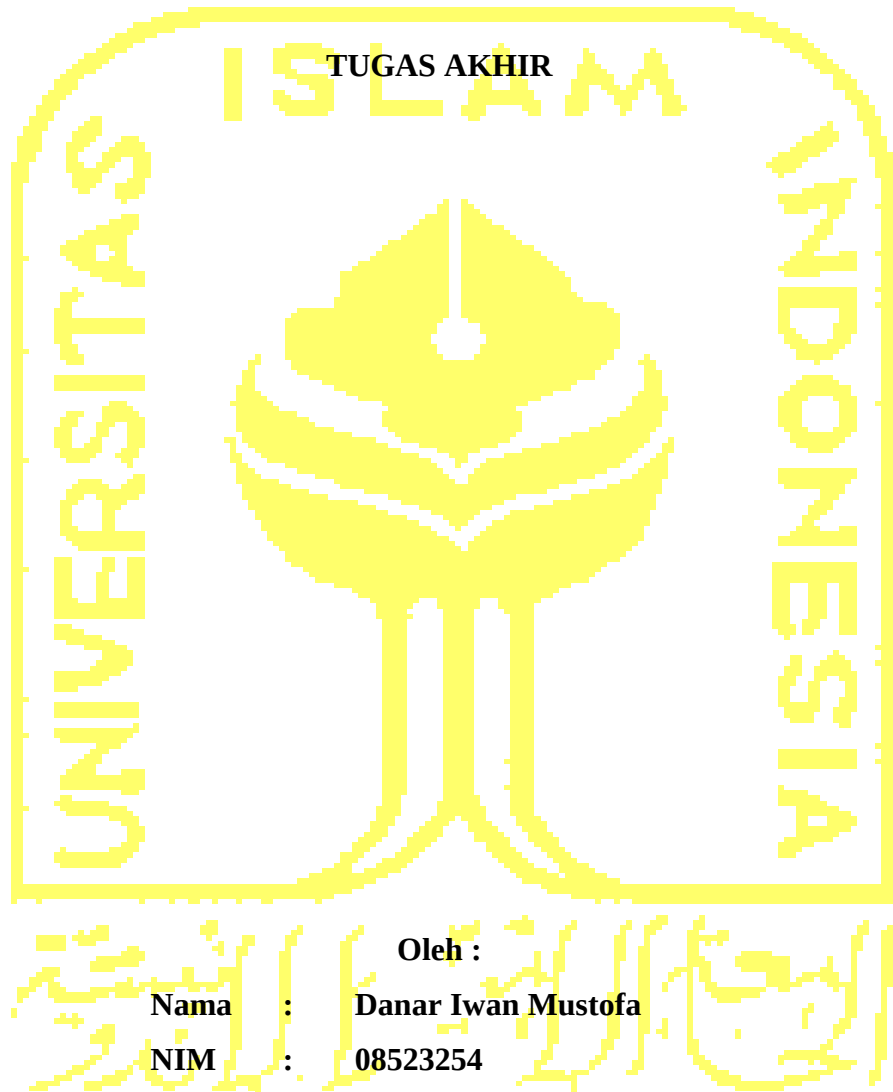


OLEH :

**NAMA : Danar Iwan Mustofa
NO. MAHASISWA : 08523254**

**JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA
2013**

LEMBAR PENGESAHAN DOSEN PEMBIMBING
ANALISIS VIRTUAL MACHINE UNTUK KEPERLUAN KOMPUTER
FORENSIK



Yogyakarta, 28 November 2013

Pembimbing,

Syarif Hidayat S.Kom.,M.IT.

LEMBAR PENGESAHAN PENGUJI

ANALISIS *VIRTUAL MACHINE* UNTUK KEPERLUAN
KOMPUTER FORENSIK

TUGAS AKHIR

Oleh :

Nama : Danar Iwan Mustofa

NIM : 08 523 254

Telah Dipertahankan di Depan Sidang Penguji sebagai Salah Satu Syarat untuk
Memperoleh Gelar Sarjana Jurusan Teknik Informatika Fakultas Teknologi

Industri Universitas Islam Indonesia

Yogyakarta, 6 Desember 2013

Tim Penguji.

Tim Penguji,

Syarif Hidayat, S.Kom., MIT.

Ketua

R. Teduh Dirgahayu, ST., M.Sc., Ph.D.

Anggota 1

Ari Sujarwo, S.Kom., MIT.

Anggota 2

Mengetahui

Ketua Jurusan Teknik Informatika

Fakultas Teknologi Industri

Universitas Islam Indonesia



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

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Saya yang bertandatangan dibawah ini,

Nama : Danar Iwan Mustofa

NIM : 08 523 254

Menyatakan bahwa komponen dan seluruh isi dalam Laporan Tugas Akhir ini adalah hasil karya saya sendiri. Apabila dikemudian hari terbukti bahwa ada beberapa bagian dari karya ini adalah bukan hasil karya saya sendiri, maka saya akan siap menanggung resiko dan konsekuensi apapun.

Demikian pernyataan ini saya buat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 28 November 2013

Danar Iwan Mustofa

PERSEMBAHAN

Untuk Ayah dan Ibu,dan adik-adik tercinta...

MOTTO

*“Sesungguhnya jika kamu bersyukur,
pasti Kami akan menambah (ni'mat) kepadamu,
dan jika kamu mengingkari (ni'mat-Ku), maka sesungguhnya azab-Ku
sangat pedih” (QS Ibrahim : 7)*

*Ya Rabbku, lapangkanlah untukku dadaku, dan mudahkanlah untukku
urusanku, dan lepaskanlah kekakuan dari lidahku, supaya mereka
mengerti perkataanku” (QS Thoha: 25-28)*

*Ketika kita merasa gagal dan putus asa, serta berpikir untuk berhenti
berusaha, sebenarnya kita hanya berjarak tiga kaki dari kesuksesan
(Napoleon Hill)*

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Assalamu'alaikum Wr. Wb.,

Alhamdulillah, puji syukur kehadiran Allah SWT, yang telah melimpahkan rahmat serta hidayah-Nya, sehingga penulis dapat menyusun dan menyelesaikan tugas akhir ini dengan baik.

Laporan tugas akhir ini disusun sebagai salah satu syarat guna memperoleh gelar Sarjana Teknik Informatika pada Universitas Islam Indonesia serta merupakan sarana untuk mempraktekan secara langsung ilmu dan teori yang telah diperoleh selama menjalani masa studi di Jurusan Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.

Penulisan tugas akhir ini tidak lepas dari bantuan, serta bimbingan dari berbagai pihak. Oleh karena itu, pada kesempatan kali ini, penulis ingin mengucapkan rasa terima kasih yang sebesar-besarnya kepada:

1. Allah 'azza wa jalla, yang telah memberikan rahmat, serta hidayah-Nya sehingga penulis dapat menyelesaikan tugas akhir ini dengan baik. Semoga apa yang telah penulis kerjakan dapat bermanfaat di kemudian hari. Baik bagi diri penulis sendiri maupun bagi orang lain.
2. Untuk kedua orangtua saya, Bp. Sukirwan dan Ibu Umi Masri'ah, yang telah memberikan kasih sayang yang melimpah, yang telah memberi dukungan, serta yang tak pernah berhenti mendoakan.
3. Bapak Ir. Gumbolo Hadi Susanto, MSc., Selaku Dekan Fakultas Teknologi Industri Universitas Islam Indonesia.
4. Bapak Yudi Prayudi S.Si., M.Kom., selaku Ketua Jurusan Teknik Informatika.
5. Bapak Syarif Hidayat S.Kom., MIT., Selaku Dosen Pembimbing. Terima kasih atas segala bantuan, dukungan, serta bimbingan yang telah diberikan kepada penulis, dalam penyusunan skripsi ini.
6. Isna dan Rizal, kedua adik tersayang.

7. Teman-teman seperjuangan Teknik Informatika, khususnya angkatan 2008.
8. Teman-teman KKN angkatan 42 unit 74.

Dalam penyelesaian laporan ini penulis menyadari bahwa masih banyak terdapat kesalahan dan kekurangannya, untuk itu penulis mengharapkan kritik dan saran yang membangun agar dapat berguna dikemudian hari, dan pada akhirnya semoga laporan ini banyak berguna dan bermanfaat bagi kita semua.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 28 November 2013

Danar Iwan Mustofa

SARI

Komputer merupakan perangkat elektronik yang memungkinkan penggunaanya dapat melakukan berbagai hal untuk menunjang masyarakat. Oleh karena itu, sebuah komputer sangat rentan penggunaannya sebagai alat untuk melakukan tindak kejahatan. Dengan semakin meningkatnya kebutuhan akan komputer, maka semakin kompleks pula aplikasi yang tersedia. Salah satu contohnya adalah penggunaan aplikasi *virtual machine* yang memungkinkan pengguna dapat menjalankan beberapa sistem operasi sekaligus dalam waktu yang sama. Karena karakteristik *virtual machine* ini hampir sama dengan karakteristik pada sistem operasi yang sebenarnya, maka tidak menutup kemungkinan bahwa *virtual machine* dapat pula dimanfaatkan sebagai alat untuk melakukan tindak kejahatan.

Proses penyelidikan dalam komputer forensik antara lain adalah dengan mengumpulkan barang bukti dari tempat kejadian perkara, lalu melakukan *write protect*, kemudian melakukan *cloning* serta *disk imaging*. Langkah – langkah ini perlu dilakukan agar barang bukti asli tidak rusak maupun berubah isinya. Lalu setelah mendapatkan file image dari *virtual machine*, dilakukan analisis menyeluruh dengan menggunakan software Forensic Toolkit (FTK).

Kemudian setelah semua proses analisis selesai, dibuatlah dokumentasi proses penyidikan, serta laporan mengenai hasil temuan yang terindikasi sebagai tindak kejahatan. Laporan tersebut sangat penting dalam pengambilan keputusan di pengadilan, hasil temuan tersebut dapat digunakan untuk menguatkan maupun melemahkan tuntutan kepada tersangka.

Kata kunci: komputer forensik, *virtual forensic*, *virtual machine*, *write protect*

TAKARIR

<i>backup</i>	membuat cadangan data
<i>Booting</i>	proses menghidupkan komputer.
forensik	proses ilmiah dalam mengumpulkan, menganalisis, dan menghadirkan berbagai bukti dalam sidang pengadilan terkait adanya suatu kasus hukum.
<i>Forensic examiner</i>	orang yang melakukan analisis terhadap barang bukti digital
<i>Hashing</i>	proses yang menggunakan algoritma matematika pada data, untuk membuat nilai numerik yang merepresentasikan data tersebut.
<i>imaging</i>	membuat salinan data mentah.
penyidik	orang yang menyidik kasus.
<i>Virtual machine</i>	mesin virtual.
<i>Volatile</i>	bersifat mudah rusak, atau mudah berubah isi-nya.
<i>write blocking</i>	fitur untuk menghalang penggandaan atau penulisan data.

DAFTAR ISI

LEMBAR PENGESAHAN DOSEN PEMBIMBING	ii
LEMBAR PENGESAHAN PENGUJI.....	iii
LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR.....	iv
PERSEMBAHAN	v
MOTTO	vi
KATA PENGANTAR.....	vii
SARI.....	ix
TAKARIR.....	x
DAFTAR ISI.....	xi
DAFTAR GAMBAR.....	xv
DAFTAR TABEL	xvii
BAB I.....	1
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan masalah	3
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
1.6 Review Penelitian.....	4
1.7 Metodologi Penelitian	5
1.7.1 Studi dan Pengumpulan Data.....	5
1.7.2 Analisis Data	5
1.7.3. Penyusunan Laporan	6
1.8 Sistematika Penulisan.....	6
BAB II	8
LANDASAN TEORI	8

2.1	Komputer Forensik.....	8
2.1.1	Definisi Komputer Forensik	8
2.1.2	Tahapan Komputer Forensik.....	9
2.1.2.1	Access	9
2.1.2.2	Acquire.....	9
2.1.2.3	Analyze	9
2.1.2.4	Report.....	10
2.1.3	Tujuan Komputer Forensik	10
2.2	Virtual machine	11
2.2.1	Pengertian <i>Virtual machine</i>	11
2.2.2	Cloud Computing.....	12
2.2.3	Hosted Architecture Virtualization	14
2.2.4	Virtual Machine VMWare	16
2.2.5	VMWare Workstation.....	17
2.3	<i>Virtual Forensic</i>	18
2.4	Hashing.....	18
2.5	<i>Software</i> Pendukung.....	19
BAB III		20
METODOLOGI PENELITIAN		20
3.1	Studi dan Pengumpulan Data	20
3.2	Metode Penelitian.....	21
3.2.1	Skenario Kasus.....	22
3.2.2	Access	23
3.2.3	Acquire.....	24
3.2.3.1	Write Protect	24

3.2.3.2 Back Up	24
3.2.3.3 Imaging	24
3.2.4 Analyze	25
3.2.4.1 Analisis oleh Teknisi.....	25
3.2.4.2 Analisis oleh <i>Forensic Examiner</i>	26
3.2.5 Report.....	26
3.3 Analisis dan Pengadaan Perangkat Keras	27
3.4 Analisis dan Pengadaan Perangkat Lunak.....	28
3.5 Instalasi dan Konfigurasi Perangkat Lunak	28
BAB IV	30
HASIL DAN PEMBAHASAN	30
4.1 Skenario Kasus	30
4.2 Access.....	31
4.3 Acquire	32
4.3.1 Imaging Physical Disk	32
4.3.1.1 Write protect	32
4.3.1.2 Cloning dan Disk Imaging	34
4.3.1.3 Hashing	35
4.3.2 Imaging Virtual Disk	37
4.4 Analisis Kasus	39
4.4.1 Hasil Analisis oleh Teknisi	41
4.4.1.1 Instalasi VMWare	41
4.4.1.2 Membuat Konfigurasi <i>Virtual machine</i>	43
4.4.1.3 Penyelidikan pada Link Files.....	46
4.4.1.4 Penyelidikan pada prefetch folder	47

4.4.1.5 Hasil Pembahasan pada My Documents	48
4.4.1.6 Hasil dan Pembahasan Software terpasang.....	49
4.4.1.7 Hasil dan Pembahasan History Web Browser	50
4.4.1.8 Laporan Sederhana tentang Hasil Temuan	52
4.4.2 Hasil Analisis oleh <i>Forensic Examiner</i>	52
4.4.2.1 Known File Filter (KFF).....	58
4.4.2.2 Hasil Analisis Struktur file pada Virtual Machine.....	58
4.4.2.3 Hasil Analisis pada <i>Deleted Files</i>	59
4.4.2.4 Hasil dan Pembahasan pada Signature Analysis	60
4.4.2.5 Penyelidikan lebih lanjut dari Laporan Teknisi	62
4.5 Dokumentasi dan Presentasi.....	65
4.6 Rangkuman Hasil Analisis	68
BAB V	71
KESIMPULAN DAN SARAN	71
5.1 Kesimpulan.....	71
5.2 Saran.....	72
DAFTAR PUSTAKA.....	xvi
LAMPIRAN	xix

DAFTAR GAMBAR

Gambar 1. 1 Statistik Kejahatan Komputer	2
Gambar 2. 1 Tahapan umum dalam Komputer Forensik.....	9
Gambar 2. 2 Inti dari Penelitian digital forensik.....	10
Gambar 2. 3 Cloud Computing Service level	13
Gambar 2. 4 Arsitektur <i>Hosted Virtualization</i>	15
Gambar 2. 5 Proses I/O pada VMWare	16
Gambar 3. 1 Metode Penelitian Usulan	22
Gambar 3. 2 Langkah-langkah yang dilakukan teknisi komputer	25
Gambar 4. 1 Contoh Formulir Penerimaan Barang Bukti	31
Gambar 4. 2 Membuat Konfigurasi <i>Write protect</i>	33
Gambar 4. 3 Bukti <i>Write protect</i>	33
Gambar 4. 4 Proses Disk Imaging	34
Gambar 4. 5 Struktur file dalam Virtual Machine	35
Gambar 4. 6 Proses <i>hashing</i>	36
Gambar 4. 7 Hasil dari proses <i>hashing</i>	36
Gambar 4. 8 Membuat Image file dari Virtual Disk	37
Gambar 4. 9 Proses Imaging <i>virtual machine</i>	39
Gambar 4. 10 Tahapan Analisis Forensik.....	40
Gambar 4. 11 Instalasi <i>Virtual machine</i>	42
Gambar 4. 12 Tampilan awal <i>Virtual machine</i>	42
Gambar 4. 13 Tampilan Live View	43
Gambar 4. 14 Image File yang akan di-booting	44
Gambar 4. 15 Proses Booting pada VMWare Workstation	45
Gambar 4. 16 BIOS <i>virtual machine</i>	45
Gambar 4. 17 Tampilan desktop Windows XP Virtual Machine	46
Gambar 4. 18 General Properties pada salah satu link file	46
Gambar 4. 19 Isi dalam Folder Prefetch	47
Gambar 4. 20 Isi dalam Folder My Pictures	48

Gambar 4. 21 Dokumen yang dicurigai sebagai daftar narkoba.....	48
Gambar 4. 22 Salah satu dokumen corrupt.....	49
Gambar 4. 23 Software terpasang dilihat dari Control Panel	50
Gambar 4. 24 Yahoo Mail	51
Gambar 4. 25 Internet Banking.....	51
Gambar 4. 26 History situs Pornografi	52
Gambar 4. 27 Forensic Toolkit Interface	54
Gambar 4. 28 New Case Dialog.....	54
Gambar 4. 29 Informasi <i>Forensic examiner</i>	55
Gambar 4. 30 Case Log Options.....	56
Gambar 4. 31 Proses optional	57
Gambar 4. 32 Menentukan Lokasi Barang bukti	57
Gambar 4. 33 Struktur File Virtual Machine	58
Gambar 4. 34 Signature file JPG	60
Gambar 4. 35 Signature file GIF.....	60
Gambar 4. 36 Signature File PDF	60
Gambar 4. 37 Signature File Microsoft office DOCX.....	60
Gambar 4. 38 Bukti file signature.....	61
Gambar 4. 39 File gambar yang berisi nomor rekening tersembunyi.....	62
Gambar 4. 40 Pornografi Anak dilihat dari FTK.....	63
Gambar 4. 41 Pornografi anak dilihat dari FTK Imager.....	63
Gambar 4. 42 File jpg yang diganti ekstensi-nya	64
Gambar 4. 43 Data kontak pada profil gelatoz	65

DAFTAR TABEL

Tabel 2. 1 Tabel Keuntungan dan Kerugian <i>Cloud Computing</i>	14
Tabel 4. 1 <i>File Signature</i>	61
Tabel 4. 2 Perbandingan FTK dan FTK Imager	69

BAB I

PENDAHULUAN

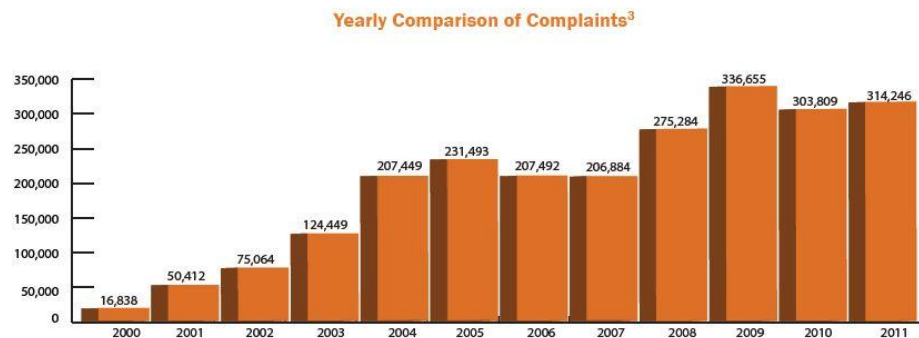
1.1 Latar Belakang

Perkembangan dunia teknologi informasi memang sangat pesat. Terhitung pada tahun 2011, jumlah total pengguna internet di dunia adalah sebanyak 2.267.233.742. Angka ini tentunya sangat besar, dibandingkan dengan tahun 2000, dimana pengguna internet hanya 360.985.492. Hal ini menunjukkan bahwa dalam kurun waktu 2000-2011, pertumbuhan pengguna internet di dunia adalah 528,1%. Pengguna internet di Indonesia adalah sebesar 22.4% atau sekitar 55.000.000 dari total populasi 245.613.043 (IWS, 2011).

Namun, seiring dengan pesatnya pertumbuhan jumlah pengguna internet di dunia, khususnya di Indonesia, juga mendorong pertumbuhan tindak kriminal yang menyalahgunakan teknologi komputer tersebut. Kasus yang paling sering ditemukan diantaranya adalah pencurian identitas, mengubah isi suatu website, pornografi, mengganggu jalur komunikasi internet, dan lain sebagainya.

Menurut FBI dalam laporan tahunannya, pada tahun 2011 terdapat 300.000 keluhan yang dilaporkan kepada Internet Crime Complaint Center (IC3). Angka ini menunjukkan peningkatan sebesar 3,4 persen dari tahun sebelumnya. Diperkirakan, kerugian berdasarkan keluhan yang ada, adalah sekitar \$485.300.000 atau setara dengan Rp4.755.940.000.000 (kurs Rp 9700). Kebanyakan dari korban yang melaporkan adalah korban penipuan, dan pencurian identitas. IC3 sendiri menerima dan memproses 26.000 keluhan tiap bulannya (IC3, 2011).

Pada gambar 1.1 berikut ini adalah grafik yang diambil dari *annual report* FBI.



Gambar 1. 1 Statistik Kejahatan Komputer
(Sumber: IC3, 2011)

Dari diagram diatas, dapat kita lihat bahwa jumlah tindakan kriminal meningkat dari tahun ke tahun. Jumlah yang paling tinggi ada di tahun 2009. Dengan demikian, keahlian penanganan kasus kejahatan dalam bidang komputer menjadi perhatian yang cukup serius.

Komputer forensik adalah metode yang digunakan untuk menyelidiki kasus, atau perkara kriminal yang memanfaatkan teknologi komputer, maupun barang bukti elektronik lain. Dengan memanfaatkan komputer forensik, *forensic examiner*, dapat mengetahui tindakan kejahatan apa saja yang telah dilakukan oleh pelaku kriminal. Oleh karena itu, sangat penting bagi penegak hukum, untuk memiliki ahli di bidang komputer forensik.

Virtual machine, adalah aplikasi yang memungkinkan pengguna-nya untuk dapat memasang lebih dari satu sistem operasi, di dalam satu komputer yang sama. Atau dengan kata lain, memasang sistem operasi lain di dalam sistem operasi. Sehingga pengguna dapat menjalankan beberapa sistem operasi sekaligus dalam waktu yang sama. Sistem operasi yang sebenarnya disebut sistem operasi "*host*". Dan sistem operasi virtual yang terpasang di dalam sistem operasi *host*, disebut sistem operasi "*guest*".

VMWare adalah salah satu perusahaan yang mengelola *cloud computing*. Para analis memperkirakan, sebanyak 80% virtualisasi berjalan pada teknologi dari VMWare. *Cloud computing* merupakan teknologi terkini dalam dunia teknologi informasi. Dalam *cloud computing*, data-data dari para *client* disimpan dalam server-server internet. *Client* atau *user* dapat mengubah, menyimpan serta

mengakses data-data mereka dimana-pun mereka berada dengan memanfaatkan perangkat elektronik seperti PC, *smartphone*, tablet, dan perangkat-perangkat lain yang memungkinkan pengguna untuk dapat mengakses internet. Dengan begitu, *cloud computing* dapat meningkatkan efisiensi dan kecepatan, serta membantu mengurangi resiko operasi dalam organisasi, namun tetap dengan menghemat sumber daya.

Digital forensik pada VMWare Workstation penting dilakukan, karena pengguna VMWare Workstation sangat beragam. Mulai dari developer, sistem engineer, pengajar dan pelajar, maupun oleh masyarakat umum. Karena sifatnya yang terisolasi dari sistem operasi yang sebenarnya, maka apabila terjadi kesalahan pada *virtual machine*, tidak akan mengganggu sistem operasi *host*. Oleh karena itu VMWare Workstation sangat mungkin digunakan oleh pihak yang tidak bertanggungjawab untuk membuat aplikasi pengganggu seperti malware, virus, dan aplikasi-aplikasi pengganggu lain.

Meski sistem operasi yang terpasang pada *virtual machine* sama dengan sistem operasi pada umumnya, tetap ada beberapa perbedaan seperti pada file konfigurasi, dan tempat penyimpanan pada *virtual machine*. Oleh sebab itu, penanganan digital forensik pada *virtual machine* sedikit berbeda dari penanganan digital forensik pada komputer fisik.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, penelitian ini dilakukan untuk menyelidiki barang bukti digital pada *virtual machine* agar dapat dijadikan barang bukti hukum yang sah.

1.3 Batasan masalah

Pembahasan secara terperinci dapat diperoleh ketika tersedianya suatu batasan masalah pada penyusunan Tugas Akhir ini. Dalam hal ini terdapat beberapa batasan masalah sebagai berikut:

1. Penelitian tidak mencakup pada keseluruhan isi hard disk fisik, melainkan pada *virtual disk*.
2. *Virtual machine* yang akan diteliti, tidak sedang dalam keadaan terkunci maupun terhapus.
3. *Guest operating system* pada *virtual machine* yang dianalisis adalah Windows XP, dan tidak menganalisis file sistem Windows secara keseluruhan.
4. Memanfaatkan *virtual machine* VMWare Workstation.
5. Menggunakan perangkat lunak FTK Imager untuk membuat file image.
6. Menggunakan software FTK dalam analisis.

1.4 Tujuan Penelitian

Tujuan dalam penelitian ini, adalah untuk membuktikan *virtual machine* sebagai barang bukti digital yang sah di pengadilan. Sehingga diharapkan dapat meningkatkan efektifitas serta kinerja *forensic examiner*.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini antara lain adalah:

1. Menemukan pendekatan baru dalam penanganan kasus digital forensik, sehingga dapat mempercepat proses analisis.
2. Menemukan manfaat serta peranan *virtual machine* dalam proses penyelidikan.
3. Mendemonstrasikan temuan yang didapat dari *virtual machine* kepada audiens yang tidak mengetahui masalah teknis.

1.6 Review Penelitian

Menurut dokumen yang diterbitkan SWGDE (2006) yang berjudul “*Best Practices for Computer Forensics*”. Menerangkan, bahwa ada beberapa tahapan yang harus dilakukan oleh penegak hukum, dalam penanganan barang bukti digital. Mulai dari penyitaan, penanganan, sampai ke tahap dokumentasi, dan laporan.

Penelitian yang berjudul “*Computer Forensic Analysis in a Virtual Environment*” (Bem & Huebner, 2007) dari University of Western Sydney, mengungkapkan sebuah pendekatan baru dalam penanganan *virtual machine* sebagai barang bukti. Selain menganalisa hasil image, mereka juga mencoba untuk membooting image *virtual machine* yang didapat, untuk mencoba mencari kemungkinan-kemungkinan yang ada. Sehingga dapat mempersingkat waktu.

Menurut penelitian yang berjudul “*Live Forensic Acquisition as Alternative to Traditional Forensic Processes*” (Lessing & Solms, 2008) menerangkan tentang metode akuisisi bukti digital pada komputer yang sedang dalam keadaan hidup. Meski metode penanganan komputer yang sedang menyala berbeda dengan penanganan pada komputer dalam keadaan mati, namun prinsip yang digunakan tetap sama seperti penanganan komputer dalam keadaan menyala, yaitu agar barang bukti digital yang asli jangan sampai rusak maupun berubah.

1.7 Metodologi Penelitian

Metodologi penelitian memuat tentang metode yang digunakan oleh penulis untuk mendukung penelitian. Adapun metode penelitian yang digunakan adalah sebagai berikut.

1.7.1 Studi dan Pengumpulan Data

Studi yang digunakan untuk mengumpulkan literatur dan data, adalah metode studi pustaka. Dengan metode ini, penulis mengumpulkan data-data, dan mencari referensi dari beberapa jurnal internasional, website, artikel, dan buku-buku yang berkaitan dengan digital forensik, serta pencarian referensi mengenai tata cara penanganan *virtual machine* sebagai barang bukti digital.

1.7.2 Analisis Data

Pada tahap analisis data, peneliti mencoba melakukan pengaksesan data serta melakukan akuisisi pada file *virtual machine*. Kemudian

melakukan *write protect*, *back up*, serta *imaging* pada *virtual machine* tersebut. Ada dua personel yang ditugaskan untuk menganalisis data. Yaitu *forensic examiner* dan teknisi. Peran teknisi adalah memanfaatkan lingkungan virtual untuk melakukan analisis sederhana. Sedangkan peran *forensic examiner* bertujuan untuk menganalisis data lebih lanjut.

1.7.3. Penyusunan Laporan

Merupakan tahap selanjutnya, setelah dilakukan analisis pada *virtual machine*. Laporan harus dibuat berdasarkan format yang telah ditetapkan. Laporan berisi dokumentasi barang bukti, cara penanganannya, serta hasil dan kesimpulan yang didapat dari analisis.

1.8 Sistematika Penulisan

Bab I Pendahuluan

Memuat latar belakang penulisan, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

Bab II Landasan Teori

Bab ini memuat landasan teori yang mendukung dalam penelitian. Dan berfungsi sebagai sumber atau referensi dalam memahami permasalahan yang terkait dengan analisis *virtual machine* sebagai barang bukti yang dapat dipertanggungjawabkan di pengadilan.

Bab III Metodologi

Bab ini berisi tentang literatur tentang virtual machine, tools forensik, serta langkah-langkah yang dilakukan untuk proses ujicoba dalam penanganan kasus digital forensik.

Bab IV Pengujian dan Pembahasan

Memuat langkah instalasi, serta hasil dari pengujian dan analisis yang dilakukan terhadap *virtual machine* yang diteliti, berikut pembahasan .

Bab V Kesimpulan dan Saran

Bab ini memuat kesimpulan dari seluruh rangkaian proses analisis *virtual machine* forensik, jenis data digital yang diteliti, beserta alat dan langkah-langkah penanganan *Virtual machine* sebagai bukti digital. Dalam bab ini, juga memuat saran yang dapat digunakan oleh pihak-pihak yang berkepentingan dalam penelitian ini.

BAB II

LANDASAN TEORI

2.1 Komputer Forensik

2.1.1 Definisi Komputer Forensik

Menurut US-CERT (2008) komputer forensik adalah disiplin yang menggabungkan unsur hukum dan ilmu komputer untuk mengumpulkan serta menganalisis data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan dengan tata cara yang dapat diterima sebagai bukti di pengadilan.

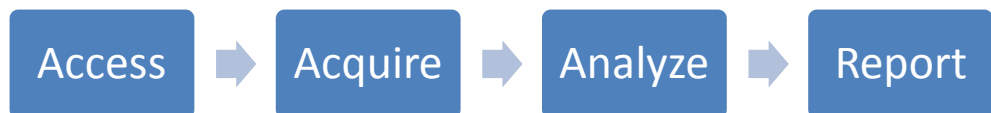
DFRWS (2001), mendefinisikan komputer forensik sebagai penggunaan metode ilmiah yang telah terbukti untuk dapat melakukan pemeliharaan, pengumpulan, validasi, identifikasi, analisis, interpretasi, dokumentasi dan presentasi bukti digital yang berasal dari sumber-sumber digital untuk tujuan memfasilitasi atau melanjutkan rekonstruksi kejadian pidana, atau membantu untuk mengantisipasi tindakan yang tidak sah yang terbukti mengganggu.

Komputer Forensik adalah pemeriksaan secara ilmiah, dan analisis data yang didapatkan atau diambil dari media penyimpanan komputer, sehingga informasi tersebut dapat dijadikan sebagai bukti di pengadilan (Nardoni, 2005).

Dari penjelasan diatas, dapat disimpulkan bahwa komputer forensik adalah suatu ilmu dan metode, untuk mengumpulkan, memelihara, mengidentifikasi, menganalisis barang bukti digital, untuk kemudian didokumentasikan dan dipresentasikan untuk membuktikan apakah seseorang terbukti melakukan tindak pidana, atau tidak.

2.1.2 Tahapan Komputer Forensik

Proses komputer forensik, terdiri dari sejumlah langkah. Dan secara luas, dapat dikemas dalam empat tahap utama. Tahapan tersebut dapat dilihat pada gambar dibawah ini.



Gambar 2. 1 Tahapan umum dalam Komputer Forensik

2.1.2.1 Access

Hal yang paling pertama dilakukan sebelum pemeriksaan, adalah mengumpulkan barang bukti elektronik yang ada di TKP. Lalu kemudian membawa barang bukti elektronik tersebut ke laboratorium untuk diserahkan kepada *forensic examiner*.

Prosedur penanganan awal barang bukti elektronik di TKP, disebut juga *Triage Forensic* yang merupakan panduan bagi penegak hukum. Hal ini berfungsi untuk mencegah terjadinya perubahan pada barang bukti yang mudah rusak, atau bersifat *volatile*. *Triage forensic* memiliki dua tujuan akhir, yaitu :

1. Menyelamatkan bukti digital yang bersifat *volatile*.
2. Menyerahkan bukti digital secara cepat kepada investigator dan *forensic examiner*.

2.1.2.2 Acquire

Adalah tahapan untuk mendapatkan data digital, dari barang bukti elektronik. Ada beberapa langkah yang harus dilakukan untuk mendapatkan data-data digital yang dimaksud. Diantaranya adalah melakukan *write protect*, *mem-back up* data, dan membuat file *image* dari perangkat digital tersebut.

2.1.2.3 Analyze

Merupakan tahapan inti dari proses digital forensik. Setelah data-data digital terkumpul, maka dilakukan analisis data-data tersebut. Hal ini dilakukan

untuk mencari bukti-bukti yang nantinya dapat menguatkan, atau melemahkan tuntutan kepada tersangka di pengadilan.

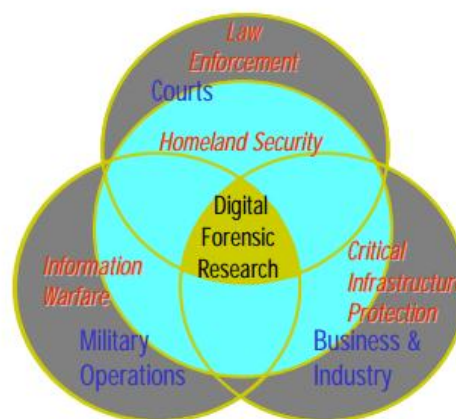
2.1.2.4 Report

Dokumentasi dan laporan adalah tahap terakhir dalam proses komputer forensik. Pada tahap ini, seorang *forensic examiner* mendokumentasikan hasil analisis-nya, membuat laporan tentang hasil temuan yang didapatkan, lalu kemudian mempresentasikan hasil tersebut.

2.1.3 Tujuan Komputer Forensik

Komputer forensik merupakan metode yang sangat penting untuk memecahkan masalah kriminal yang memanfaatkan komputer, maupun barang elektronik lain. Digital forensik juga menjadi alat yang sangat penting sebagai jaminan informasi, karena kemampuannya untuk merekonstruksi kembali barang bukti yang ditinggalkan oleh pelaku kejahatan.

Pada saat ini, mayoritas analisis komputer forensik difokuskan untuk membantu penegak hukum dalam mengungkap kasus kejahatan komputer. Namun, menurut *technical report* dari DFRWS, pemanfaatan digital forensik juga mencakup pada kepentingan lain seperti operasi militer, bisnis dan industri. Seperti yang diterangkan pada gambar 2.2 berikut ini.



Gambar 2. 2 Inti dari Penelitian digital forensik
(Sumber: DFRW, 2001)

Komputer forensik tidak hanya digunakan untuk kasus kejahatan komputer, tetapi teknik dan metodenya juga diadaptasi untuk keperluan non-investigasi. Sebagai contoh memasukkan pemetaan data untuk keamanan dan penaksiran resiko pribadi, dan pencarian kekayaan intelektual untuk mengamankan data. Komputer forensik merupakan transisi dari investigasi dan mekanisme tanggapan untuk salah satu dari pencegahan, penyesuaian dan jaminan.

Dengan memanfaatkan teknik pada komputer forensik, perusahaan dapat melindungi diri mereka dari ancaman dari luar seperti *hacker*, maupun ancaman dari karyawan mereka sendiri, dengan lebih baik.

Sebagai tambahan, skema pada komputer forensik dapat digunakan ketika data-data penting terhapus secara tidak sengaja, atau disebabkan karena kerusakan *hardware*. Dengan demikian ada beberapa aplikasi tambahan yang berkaitan dengan ilmu komputer forensik untuk memaksimalkan metode untuk menginvestigasi tindakan kejahatan yang berkaitan dengan komputer.

2.2 Virtual machine

2.2.1 Pengertian *Virtual machine*

Virtual machine (VM) bukanlah merupakan hal baru dalam dunia komputer, dan telah digunakan selama lebih dari setengah abad. *Virtual machine* ("*guest*") adalah sebuah mesin virtual yang berjalan mandiri di dalam sebuah mesin yang sebenarnya ("*host*"). Atau dengan kata lain, VM adalah sebuah komputer virtual yang berjalan di dalam komputer fisik. Dengan begitu, *virtual machine* memungkinkan penggunaanya untuk menjalankan beberapa sistem operasi yang berbeda, dalam satu komputer fisik, dan dalam satu waktu (Shavers, 2008).

Virtual machine sendiri telah banyak digunakan oleh individu, maupun oleh suatu organisasi. Dalam praktiknya, *virtual machine* biasa digunakan untuk menganalisis atau menguji suatu aplikasi, mencoba sistem operasi baru sebelum mulai menggunakannya, untuk mem-*backup* sistem, serta untuk menghemat

sumber daya (biasa digunakan oleh perusahaan atau organisasi). *Virtual system* dapat diisolasi atau dipisahkan dari sistem yang sebenarnya. Sehingga hasil pengujian dapat dilakukan dengan mudah, tanpa harus khawatir komputer terserang *malware* atau program jahat lainnya. Sedangkan untuk keperluan organisasi, *virtual machine* biasa digunakan untuk memaksimalkan sumber daya, dan berfungsi untuk mempercepat pemulihan bencana atau kesalahan (Shavers, 2008).

Ada dua jenis arsitektur utama dalam virtualisasi. Yaitu *hosted virtualization* dan *bare metal virtualization*. Setiap arsitektur memiliki kelebihan dan kekurangan-nya masing-masing.

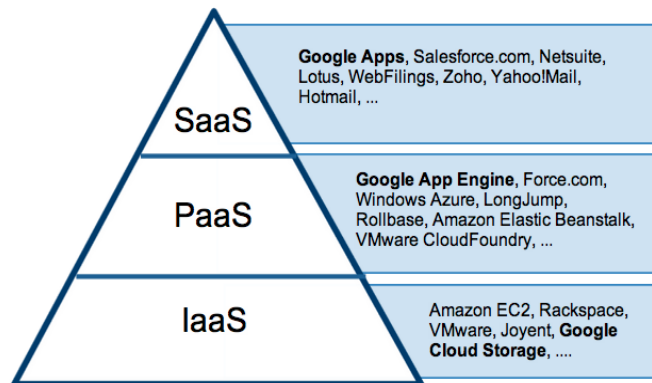
2.2.2 Cloud Computing

Cloud computing memiliki dua pengertian yang berbeda. Pengertian pertama, dan yang paling banyak diartikan secara umum, *cloud computing* adalah penggunaan layanan komersil yang dikirimkan melalui internet secara berkala dari penyimpanan ke aplikasi web. Sehingga informasi secara permanen tersimpan di dalam server internet, dan secara sementara tersimpan di komputer *client*. Sedangkan arti kedua mengacu pada arsitektur *cloud computing* yang sebenarnya dan teknologi yang diperlukan untuk memberikan layanan *cloud*.

Sedangkan menurut NIST (2011), *cloud computing is a shared collection of configurable networked resources (e.g., networks, servers, storage, applications and services) that can be reconfigured quickly with minimal effort*.

Jadi dapat disimpulkan bahwa cloud computing adalah layanan pembagian sumber daya yang terdapat dalam jaringan, yang mencakup, server, penyimpanan, aplikasi, dan layanan yang dapat dikonfigurasi dengan cepat, tanpa memerlukan usaha berlebih, dengan memanfaatkan jaringan internet.

Di dalam *cloud computing*, terdapat tiga layanan utama, yaitu Infrastructure-as-a-Service, Platform-as-a-Service, dan Software-as-a-Service. Masing-masing layanan memiliki keistimewaan tersendiri. Keterangan pada ketiga layanan utama tersebut dapat dilihat pada gambar 2.3 berikut ini.



Gambar 2. 3 Cloud Computing Service level
(Sumber: Chun, 2012)

Penjelasan dari tiga layanan utama yang ditawarkan kepada pengguna yaitu :

1. Infrastructure-as-a-Service

Memungkinkan klien untuk menggunakan semua sumber daya yang ada yang biasa digunakan pada departement IT, seperti data center, server, peralatan networking, dan *software*.

2. Platform-as-a-Service

Adalah layanan yang seringkali memanfaatkan sistem operasi dengan layanan yang terkait pada internet tanpa melakukan download maupun instalasi.

3. Software-as-a-Service

Pengiriman aplikasi yang berlisensi kepada *customer* melalui internet untuk penggunaan sebagai permintaan layanan. Vendor SaaS akan menghosting aplikasi dan membolehkan *customer* untuk mengunduh aplikasi dalam beberapa periode waktu tertentu, setelahnya aplikasi akan menjadi tidak aktif.

Gambaran kelebihan dan kekurangan *cloud computing* sendiri dapat dilihat pada tabel 2.1 berikut ini.

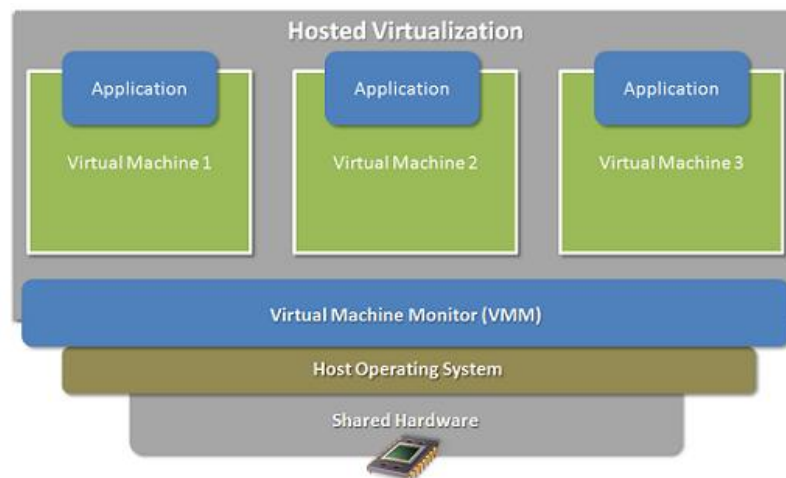
Tabel 2. 1 Tabel Keuntungan dan Kerugian *Cloud Computing*

Kelebihan	Kekurangan
1. Menghemat pengeluaran. 2. Akses dapat dilakukan dimanapun 3. Penyimpanan yang tak terbatas 4. Menjaga data dari kerusakan yang disebabkan karena <i>hardware failure</i> maupun bencana. 5. Tidak perlu mengupgrade <i>hardware</i> dan <i>software</i> 6. Efisien	1. Keamanan dan kerahasiaan. 2. Kurangnya kontrol 3. Kehandalan 4. Captivity : Pengguna tidak dapat bermigrasi ke penyedia layanan lain 5. Komputer menjadi lambat jika jaringan internet bermasalah, maupun jika komputer <i>overloaded</i> .

2.2.3 Hosted Architecture Virtualization

Dalam arsitektur ini, sistem operasi dasar (*host*) dipasang di dalam komputer terlebih dahulu. Kemudian sebuah *software* yang disebut hypervisor atau *virtual machine* monitor (VMM), dipasang di dalam sistem operasi *host*, dan memungkinkan pengguna untuk menjalankan berbagai sistem operasi *guest* dalam jendela aplikasi mereka sendiri. Produk yang terkenal menggunakan arsitektur ini adalah VMWare Workstation.

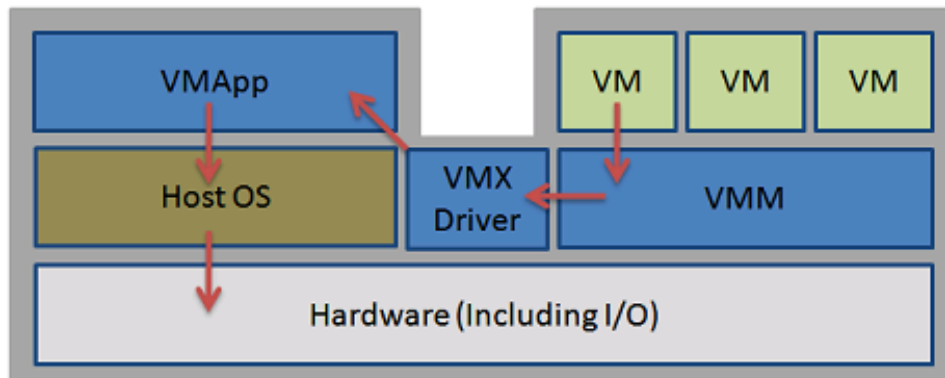
Sebagai tambahan, untuk menghubungkan *virtual machine* kedalam *network adapters*, CD-ROM, hard disk, dan perangkat USB. VMWare Workstation juga menyediakan kemampuan untuk meniru *hardware* tambahan tersebut. Sebagai contoh, VMWare Workstation dapat *me-mounting* file ISO sebagai CD-ROM, dan file *.vmdk* sebagai hard disk. Juga dapat mengkonfigurasi virtual network adapter untuk menggunakan *network address translation* (NAT) melalui *host machine*, daripada menetapkan alamat IP untuk setiap mesin virtual (National Instruments, 2009).



Gambar 2. 4 Arsitektur *Hosted Virtualization*
(Sumber: National Instruments)

Pada arsitektur virtualisasi, setiap *virtual machine* (sistem operasi *guest*) umumnya hanya memiliki akses yang terbatas pada peralatan *Input Output* I/O. Sistem operasi *host* mempertahankan kepemilikan fisik I/O yang terhubung ke sebuah komputer, dan *virtual machine* monitor (VMM) meniru *hardware* yang sebenarnya (jika memungkinkan) kepada tiap-tiap *virtual machine*. Karena VMM tidak bisa mendeteksi tentang perangkat I/O yang tidak umum seperti PCI card, yang tidak disertakan oleh perangkat-perangkat emulasi ke VM. Hanya perangkat umum seperti kartu jaringan dan CD ROM yang dapat ditiru. Namun ada pula beberapa virtualisasi yang mendukung USB port. Fitur ini memungkinkan pengguna untuk mengakses perangkat USB dari *virtual machine* secara langsung .

Pada kenyataannya, beberapa komponen perangkat lunak bekerja sama untuk membuat I/O dalam arsitektur virtualisasi *host*. Sebagai contoh, produk Workstation VMWare mengarahkan permintaan I/O dari mesin virtual melalui komponen VMM tingkat rendah, kemudian melalui *driver*, dan akhirnya ke komponen aplikasi *user-level* yang disebut VMAApp. Lalu, komponen VMAApp melewati permintaan I/O melalui sistem operasi *host*. Kuncinya adalah bahwa permintaan I/O melewati host OS dalam sebuah arsitektur virtualisasi *host*. Sebuah diagram dari proses ini ditunjukkan pada gambar 2.3 di bawah ini.



Gambar 2. 5 Proses I/O pada VMWare
(Sumber: National Instruments)

2.2.4 Virtual Machine VMWare

VM dikembangkan oleh IBM pada tahun 1960. Pada tahun itu, IBM memiliki range system yang amat luas, dimana setiap generasi dari *virtual machine* berbeda dengan generasi lainnya. Hal ini cukup menyulitkan pelanggan untuk selalu mengikuti perkembangan suatu sistem dan *hardware* yang dibutuhkan untuk menjalankannya. Lagipula, pada waktu itu, komputer hanya dapat melakukan satu tugas, dalam satu waktu.

Pada bulan Januari 1987, Insignia Solution medemonstrasikan *software* emulator yang disebut SoftPC. SoftPC memungkinkan penggunaanya untuk menjalankan aplikasi Dos, pada sistem operasi Unix mereka. Terinspirasi dari SoftPC, perusahaan lain mulai muncul dan berkembang. Pada 1997, Apple membuat program yang disebut Virtual PC dan menjualnya melalui perusahaan yang disebut Connectix. Pada 1998, sebuah perusahaan yang bernama VMWare berdiri, dan setahun setelahnya mereka menjual produk yang hampir sama dengan Virtual PC yang disebut VMWare Workstation. Pada awalnya, VMWare Workstation hanya berjalan pada sistem operasi Windows. Dan pada saat ini, VMWare menjadi *market leader* di bidang virtualisasi (Conroy, 2010).

File-file yang umumnya terkait dengan *virtual machine*, diantaranya adalah sebagai berikut:

1. .Log file : Pencatatan aktifitas pada *virtual machine*.

2. .VMDK (*Virtual Machine Disk*) adalah media penyimpanan pada sistem operasi virtual.
3. .VMX merupakan file konfigurasi dari sebuah mesin virtual. Seperti sitem operasi, *information disk*, dsb
4. .NVRAM merupakan file yang menyimpan informasi BIOS pada *virtual machine*.
5. .VMSD merupakan file yang berisi metadata *snapshot*
6. .VMXF apabila sebuah mesin virtual dihapus , maka akan ada sisa dari file konfigurasi ini.

2.2.5 VMWare Workstation

VMWare Workstation memberikan dukungan platform yang luas untuk menjalankan sistem operasi yang berbeda pada saat yang sama, pada satu *personal computer* (PC). VMWare Workstation mendukung lebih dari 200 sistem operasi, termasuk Windows 7, Windows Server 2008 R2, dan versi Windows yang lain. Kemudian juga mendukung Redhat, Ubuntu, OpenSuse dan 26 versi Linux lainnya. VMWare Workstation dapat menjalankan VMWare vSphere dan VMWare ESXi untuk pengujian atau untuk tujuan demonstrasi pada PC.

Software virtualisasi VMWare memetakan sumber daya dari perangkat keras untuk *virtual machine*. Sehingga setiap *virtual machine* dilengkapi dengan CPU, RAM, harddisk, dan NIC-nya sendiri. Tidak perlu melakukan reboot pada komputer, maupun partisi harddisk untuk beralih dari satu mesin virtual ke mesin virtual lainnya. *Virtual machine* setara dengan sistem x86 standar, dan mampu menjalankan sistem operasi Windows, Linux, dan sistem operasi desktop serta server lainnya .

Dalam aplikasi VMWare, terdapat rangkaian peralatan yang bernama VMWare Tools yang berfungsi untuk meningkatkan performa sebuah VM yang dipasang di dalam komputer. Rangkaian ini bekerja seperti layaknya *driver* pada sistem operasi host. Beberapa fitur yang tersedia bila VMWare Tool dipasang diantaranya adalah meningkatkan tampilan grafis, meningkatkan performa

mouse, serta dapat menyalin dan menyisipkan teks, grafik, dan file antara mesin virtual dan desktop host (VMWare Workstation Documentation, 2012) .

2.3 *Virtual Forensic*

Dalam kasus komputer forensik, semua barang elektronik yang ada di TKP harus diselidiki. Yang termasuk dalam golongan barang elektronik adalah PC, handphone/*smartphone*, flashdisk, harddisk external, dan barang elektronik lain yang dilengkapi dengan media penyimpanan, yang kemungkinan besar dapat menyimpan data-data digital, yang nantinya diperlukan untuk keperluan analisis.

Virtual machine adalah suatu aplikasi yang memungkinkan penggunaanya dapat memasang lebih dari satu sistem operasi dalam satu PC, tanpa harus membuat partisi baru, dan tanpa harus me-restart PC untuk beralih dari satu mesin virtual, ke mesin virtual lain-nya. Kebanyakan orang menggunakan *virtual machine* untuk mencoba aplikasi baru, dan sistem operasi lain, sebelum memasangnya kedalam PC.

Sebuah *virtual machine* yang terpasang di dalam komputer, benar-benar merupakan sebuah mesin yang independen. Karena kemampuan-nya tersebut yang sama dengan sistem operasi sebenarnya, maka *virtual machine* tidak dapat dilupakan dari penyelidikan forensik.

2.4 **Hashing**

Proses hashing atau dikenal juga sebagai digital fingerprint, adalah metode untuk melihat derajat kesamaan antara barang bukti aseli, dengan file image. Ada dua algoritma yang umum digunakan dalam proses hashing, yaitu MD5 dan SHA1.

MD5 (Message-Digest algorithm 5) merupakan algoritma yang dibuat pada tahun 1991 oleh Profesor Ronald Rivest, untuk menggantikan algoritma sebelumnya, yaitu MD4. Merupakan kriptografi yang paling banyak digunakan. MD5 menggunakan nomor hexadesimal, dengan panjang 32 digit dengan 128 bit *message digest (hash value)*. Message digest ini diklaim sebagai image file yang unik seperti sidik jari pada manusia. Dan menurut Internet Engineering Task

Force (IETF) “hal yang tidak mungkin secara komputasi” bahwa dua input data memiliki message digest yang sama.

SHA1 (Secure Hash Algorithm 1) adalah algoritma hashing kedua yang paling banyak digunakan. Algoritma ini pada dasarnya menganut prinsip yang mirip seperti yang digunakan pada MD4, pendahulu dari MD5 yang memproduksi 160-bit message digest ketika sebuah file image berukuran lebih kecil dari 2^{64} bit diberikan sebagai input kepada algoritma. SHA1 disebut-sebut sebagai algoritma yang aman, karena seperti algoritma MD5, yang dapat dengan mudah untuk menemukan data yang cocok dengan message digest yang diberikan atau untuk menemukan dua data yang berbeda yang memproduksi message digest yang sama.

2.5 *Software Pendukung*

Dibutuhkan FTK (Forensic Toolkit) adalah *software* forensik yang dikembangkan oleh Access Data, yang berguna untuk mencari berbagai informasi dari berbagai data digital. Memungkinkan *forensic examiner* untuk untuk melihat semua file pada perangkat penyimpanan.

Lalu dibutuhkan juga FTK Imager untuk membuat file image dari *virtual machine* yang akan dianalisis. File image ini sangat penting dalam penyelidikan forensik, karena barang bukti asli tidak dapat langsung dianalisis dikarenakan sifatnya yang mudah berubah.

Agar dapat mem-booting sebuah file image kedalam lingkungan virtual, dibutuhkan *software* yang dapat membuat file konfigurasi dari *virtual machine*. *Software* itu bernama Live View. Adalah aplikasi *freeware* berbasis Java yang didesain untuk menjalankan image disk (DD file) kedalam lingkungan virtual. Hal ini memungkinkan penguji untuk dapat mem-*booting* image, dan dapat menggali informasi yang ada di dalam sistem tersebut.

BAB III

METODOLOGI PENELITIAN

3.1 Studi dan Pengumpulan Data

Pengumpulan data merupakan hal yang berperan penting dalam kelancaran dan keberhasilan dalam suatu penelitian. Dalam penelitian ini metode pengumpulan data yang digunakan adalah studi pustaka. Studi pustaka ini dilakukan untuk mengetahui hal-hal yang terkait dengan masalah yang sedang dikaji dan sebagai bahan untuk menganalisis masalah.

Dengan menggunakan *virtual machine*, memungkinkan pengguna-nya untuk memasang sistem operasi lain dalam komputer yang sama. Oleh karena itu, kemampuan *virtual machine* bisa dipastikan hampir sama dengan sistem operasi *host*. Tergantung seberapa banyak sumber daya yang dialokasikan, dan sistem operasi yang dipasang di dalamnya. Idealnya, masing-masing *virtual machine* bersifat seperti sebuah komputer yang independen dengan sistem operasinya sendiri, dan dengan perangkat keras-nya sendiri. Pengguna juga dapat mengontrol tiap-tiap lingkungan virtual tersebut.

Seperti hal-nya barang bukti elektronik maupun barang bukti digital lainnya, *virtual machine* juga tidak dapat dianalisis secara langsung. Karena data-data di dalamnya sangat riskan dari perubahan. Karena *virtual machine* terpasang di dalam sebuah komputer, hal yang paling mungkin dilakukan adalah dengan membuat *back up* harddisk komputer, mengkloning-nya dengan byte per byte, serta membuat file image dari komputer yang disita dari Tempat Kejadian Perkara (TKP).

Namun masalahnya, karena virtual disk dari VMWare tidak dapat dianalisa jika masih berada di dalam media penyimpanan, maka *examiner* perlu membuat file image dari media penyimpanan pada *virtual machine*, atau yang biasa disebut *virtual machine disk*. File image dari virtual disk tersebut yang nantinya diselidiki menggunakan *tools* forensik, yaitu FTK Imager dan FTK.

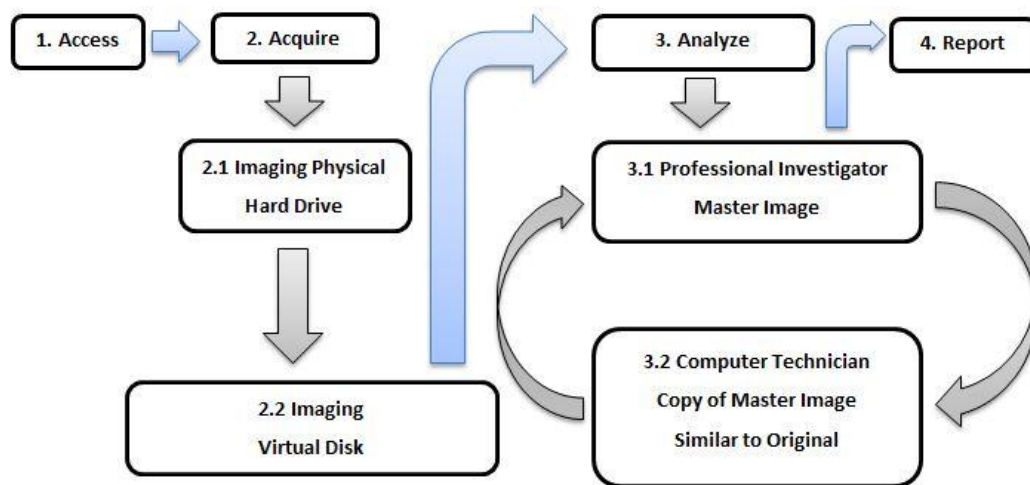
3.2 Metode Penelitian

Metodologi usulan yang digunakan oleh peneliti mencakup segala aspek dalam tahapan komputer forensik secara umum. Namun dalam penelitian ini, digunakan metode penelitian yang sedikit berbeda dari metode penelitian komputer forensik pada umumnya. Perbedaan tersebut terletak pada proses *acquire* (akuisisi) dan pada proses analisis.

Setelah kita mendapatkan barang bukti elektronik dari tempat kejadian perkara, yang harus dilakukan kemudian adalah membuat *back up* serta file image dari barang bukti tersebut, sehingga didapatkan barang bukti elektronik. Namun file image dari harddisk fisik yang diperoleh belum dapat digunakan untuk melihat dan menganalisis data-data pada *virtual machine disk*. Oleh karena itu dalam proses akuisisi, setelah memback-up semua data dalam harddisk fisik, langkah selanjutnya adalah melakukan *file imaging* dari *virtual disk*. Sehingga *examiner* dapat melihat isi dan struktur file yang ada pada virtual disk.

Kemudian dalam proses analisis dalam penelitian ini juga berbeda. Dalam penelitian ini diperlukan peran teknisi komputer (bukan *forensic examiner*) untuk melakukan booting sebuah *virtual machine* kedalam lingkungan virtual. Hal ini dilakukan untuk dapat memberi gambaran tentang kondisi pada *virtual machine* yang terpasang.

Ketika masuk ke tahap analisis, barang bukti digital dibuat dalam dua file yang berbeda. File image pertama diserahkan kepada *forensic examiner*, dan yang kedua diserahkan kepada teknisi komputer. Kemudian teknisi komputer mencoba untuk membooting file image tersebut, dan mencari data-data yang ada di dalamnya dengan menggunakan *virtual machine* VMWare Workstation dan Live View. Dari gambar 3.1 berikut ini, dijelaskan mengenai metodologi yang dipakai dalam penelitian ini.



Gambar 3. 1 Metode Penelitian Usulan

Setelah seorang teknisi mendapatkan data-data yang dicurigai dapat berisi file-file penting dalam proses penyelidikan, lalu ia membuat laporan sederhana kepada *forensic examiner* tentang data-data yang ia temukan ketika mencoba membooting file *virtual machine* tersebut. Hal ini dimaksudkan, agar *forensic examiner* dapat memiliki gambaran tentang apa yang terjadi, serta dengan cepat dapat langsung memeriksa file mencurigakan yang dilaporkan oleh teknisi komputer.

3.2.1 Skenario Kasus

Asumsi telah dilakukan penggerebekan terhadap sebuah rumah mewah di kawasan Jakarta Selatan, yang diduga digunakan sebagai tempat pesta narkoba. Dari rumah tersebut polisi menemukan beberapa barang bukti, diantaranya adalah beberapa sejumlah obat-obatan terlarang, dan satu buah notebook dalam keadaan mati. Kemudian polisi membawa notebook tersebut ke laboratorium untuk dilakukan pemeriksaan secara menyeluruh.

Kemudian untuk memastikan apakah pemilik notebook tersebut terlibat dalam kasus kriminal, maka diperlukan penanganan komputer menurut langkah-langkah yang telah ditetapkan sebagai standar dalam penanganan kasus kejahatan komputer.

Setelah dilakukan penyelidikan terhadap notebook tersebut, ternyata terdapat aplikasi *virtual machine* VMWare. Dalam *virtual machine* tersebut ada sistem operasi Windows XP yang terpasang. Di dalam virtual disk tersebut juga ditemukan beberapa file mencurigakan. Diantaranya adalah adanya file-file yang mengindikasikan pornografi anak, dan jaringan narkoba. Dalam sub-bab selanjutnya akan dijelaskan mengenai tata cara penanganan barang bukti elektronik dan barang bukti digital.

3.2.2 Access

Atau pengumpulan barang bukti elektronik dari tempat kejadian perkara. Merupakan langkah paling awal dalam prosedur penanganan barang bukti elektronik. Barang elektronik yang ditemukan dalam kasus ini adalah sebuah notebook dalam keadaan mati. Barang bukti elektronik ini kemudian dilaporkan dan disimpan ke laboratorium, untuk kemudian diperiksa oleh ahli forensik.

Sebelum beranjak ke tahap akuisisi, dalam tahap ini, seorang *forensic examiner* perlu meninjau ulang tiga hal berikut ini:

1. Mengetahui kewenangan hukum untuk permintaan pemeriksaan forensik.
2. Memastikan bahwa form permintaan untuk melakukan analisis telah diisi dengan benar.
3. Melengkapi dokumentasi *Chain of Custody*, atau yang disebut pula dokumentasi kronologi dari penyitaan, penahanan, kontrol, transfer, analisis, dan pengaturan dari sebuah bukti fisik maupun digital.

Setelah menentukan apakah kasus tersebut layak untuk ditindaklanjuti, maka penanganan selanjutnya terhadap barang bukti yang bersangkutan meliputi data-data sebagai berikut:

1. Fokus kepada barang bukti, dengan melihat dimana barang bukti tersebut ditemukan dan kelayakan sebuah media untuk dianalisis.
2. Menetapkan bagaimana sebuah barang bukti didokumentasi (mengambil foto barang bukti, membuat sketsa, maupun dengan menggunakan catatan).
3. Mengevaluasi lokasi penyimpanan dari gangguan elektromagnetik.

4. Memastikan kondisi barang bukti masih tetap seperti sediakala meskipun telah melalui pengemasan, transportasi, dan penyimpanan.

3.2.3 Acquire

Proses ini membutuhkan ekstra kehati-hatian, karena seperti sudah dijelaskan bahwa data digital sangat mudah sekali berubah. Ada beberapa hal yang harus dilakukan untuk mendapatkan data-data digital dari sebuah barang bukti elektronik. Diantaranya adalah melakukan *write protect*, *imaging*, dan *hashing* (Al Azhar, 2012). Berikut penjelasan dalam proses acquire atau akuisisi.

3.2.3.1 Write Protect

Write protect atau biasa juga disebut dengan *write blocking* adalah teknik untuk mempertahankan keaslian data pada saat pemeriksaan. *Write protect* dilakukan untuk mencegah adanya perubahan data, baik yang disengaja maupun tidak. Perubahan data sangat mungkin terjadi karena setiap sebuah sistem komputer dinyalakan, maka sebuah data baru akan ditulis. *Write protect* juga berguna untuk menutup akses penulisan data pada media penyimpanan yang terhubung melalui USB (*Universal Serial Bus*).

3.2.3.2 Back Up

Langkah selanjutnya setelah berhasil melakukan *write protect* adalah melakukan *back up* pada media penyimpanana atau barang bukti elektronik. Mem-*back up* data pada media penyimpanan penting dilakukan, agar apabila dikemudian hari data tersebut dibutuhkan, tidak perlu lagi mengambil dari barang bukti aseli, cukup mengambil dari file *back up* yang ada. Sehingga dapat meminimalisir terjadinya perubahan pada barang bukti aseli, karena terlalu sering diakses.

3.2.3.3 Imaging

Kemudian melakukan *forensic imaging*, pada harddisk laptop yang dimaksud. *Forensic imaging* adalah penggandaan harddisk secara *byte-per-byte*. Hal ini dilakukan agar harddisk yang asli bisa disimpan, dan proses analisis akan dilakukan pada *image* hard disk tersebut. Dan langkah terakhir adalah melakukan

hashing, untuk membuktikan keaslian data digital. Hal ini dilakukan dengan melihat derajat kesamaan antara barang bukti elektronik yang asli, dengan data digital hasil dari proses *imaging*.

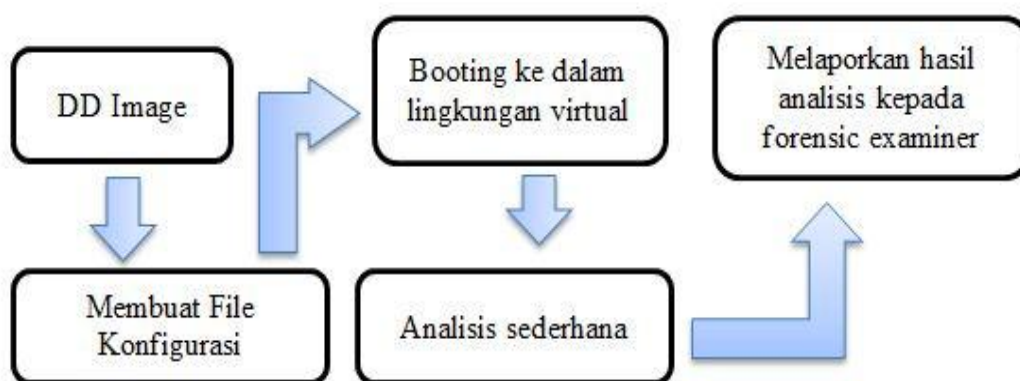
Namun file image dari harddisk fisik yang diperoleh belum dapat digunakan untuk melihat dan menganalisis data-data pada *virtual machine disk*. Oleh karena itu langkah selanjutnya adalah membuat file image dari *virtual disk*.

3.2.4 Analyze

Dalam proses analisis ini, memanfaatkan dua orang yang berbeda. Yaitu teknisi komputer dan *forensic examiner*. Setelah seorang *forensic examiner* melakukan akuisisi pada barang bukti elektronik, hasil image dari barang bukti tersebut kemudian dibuat salinan yang lain, sehingga baik teknisi komputer maupun forensic examiner masing-masing memegang satu salinan tersebut. Hal ini dilakukan untuk mencegah perubahan dan kerusakan data.

3.2.4.1 Analisis oleh Teknisi

Pada tahap ini, seorang *forensic examiner* menyerahkan sebuah copy dari DD image barang bukti yang sama dengan aslinya kepada teknisi komputer yang belum berpengalaman dalam bidang komputer forensik. Hal ini ditujukan agar seorang teknisi dapat melakukan booting, dan analisis sederhana pada file image tersebut. Kemudian dari hasil analisis sederhana tersebut, teknisi memberikan laporan sederhana kepada *forensic examiner*. Berikut adalah alur tahapan yang harus dilakukan oleh teknisi.



Gambar 3. 2 Langkah-langkah yang dilakukan teknisi komputer

3.2.4.2 Analisis oleh *Forensic Examiner*

Dari hasil analisis sederhana yang dilakukan oleh teknisi komputer, diharapkan dapat memberikan gambaran mengenai kondisi *virtual machine* tersebut. Sehingga *forensic examiner* dapat dengan cepat menentukan langkah yang harus diambil selanjutnya. Dapat langsung menuju ke inti dari penelitian tersebut. Dengan metode ini juga diharapkan dapat menghemat waktu yang diperlukan oleh *forensic examiner* dalam menganalisis *virtual machine*.

3.2.5 Report

Report adalah tahap terakhir dari proses komputer forensik. Dimana seorang *forensic examiner* membuat laporan tertulis dan mendokumentasikan hasil penelitian yang didapat untuk kemudian dipresentasikan.

Meskipun dalam tool forensik seperti FTK dapat secara otomatis membuat file dokumentasi, perlu dibuat laporan dengan format resmi untuk memudahkan penegak hukum dalam mengambil kesimpulan dan keputusan.

Dokumentasi harus sejalan dengan pemeriksaan dan penyimpanan catatan harus bersesuaian dengan kebijaksanaan antar departemen. Hal berikut ini adalah beberapa hal yang umum diperhatikan dalam proses dokumentasi menurut National Institut of Justice:

1. Melakukan pencatatan ketika berkonsultasi dengan pihak kepolisian yang menangani kasus.
2. Memelihara dan menjaga salinan wewenang penyelidikan serta catatan kasus.
3. Menyimpan paraf dan identitas dari pihak yang meminta bantuan dengan file-file kasus.
4. Memelihara salinan dari dokumentasi penahanan.
5. Mencatat tanggal, *notes*, waktu, deskripsi, serta langkah-langkah yang dilakukan.
6. Mendokumentasi sistem operasi dan *software* yang relevan serta patch yang terpasang.

Laporan dari hasil penyelidikan merupakan catatan-catatan yang dibuat oleh investigator. Semua data-data mengenai barang bukti, mulai dari proses pengumpulan barang bukti, akuisisi, serta hasil analisis yang didapat. Laporan penyelidikan ini dapat dilihat pada lampiran. Berikut ini adalah catatan yang harus disertakan dalam penulisan laporan:

1. Mengidentifikasi agen yang melapor dan menyerahkan barang bukti.
2. Nomor kasus
3. Pihak yang menangani kasus
4. Identitas pihak yang menyerahkan barang bukti
5. Tanggal penerimaan
6. Tanggal laporan
7. Deskripsi dari barang yang diberikan untuk diteliti. Seperti nomor serial, pembuatan, dan model.
8. Identitas dan tanda tangan examiner atau penyidik.
9. Keterangan dan deskripsi singkat mengenai langkah-langkah yang diambil selama penyidikan.
10. Hasil dan Kesimpulan.

Setelah selesai menyusun laporan, tahap akhir pada proses report adalah melakukan presentasi. Dimana presentasi ini menjelaskan semua hasil penyelidikan secara garis besar dan tidak memihak.

3.3 Analisis dan Pengadaan Perangkat Keras

Kebutuhan akan perangkat keras tidak dapat dilepaskan dari sebuah penelitian komputer forensik. Tahap ini merupakan tahap pengadaan perangkat keras yang dibutuhkan untuk melakukan pemasangan dan menjalankan aplikasi untuk kepentingan penelitian. Diperlukan perangkat keras yang memiliki kemampuan yang baik.

Dalam pengujian ini, menggunakan notebook Asus A43SJ, dengan spesifikasi sebagai berikut:

1. Processor intel Core i3

2. 2GB RAM
3. Harddisk 500GB

3.4 Analisis dan Pengadaan Perangkat Lunak

Merupakan kebutuhan perangkat lunak yang digunakan untuk keperluan analisis barang bukti digital yang telah didapatkan. Tanpa adanya perangkat lunak yang dimaksud, maka penelitian tidak akan dapat dijalankan. Karena baik perangkat keras maupun perangkat lunak, saling membutuhkan. Sehingga keduanya tidak dapat dipisahkan dari penelitian ini. Perangkat lunak yang digunakan dalam penelitian ini adalah:

1. VMWare Workstation 7
2. FTK Imager
3. FTK
4. Live View

3.5 Instalasi dan Konfigurasi Perangkat Lunak

Adalah tahapan untuk melakukan pemasangan perangkat lunak yang dibutuhkan dalam proses penelitian dan analisis. Adapun perangkat lunak yang nantinya akan digunakan dalam penelitian ini adalah FTK Imager. FTK Imager berfungsi untuk membuat file image dari sebuah media penyimpanan yang akan dianalisis. FTK Imager juga berfungsi untuk melakukan *hashing* atau melihat derajat kesamaan antara media asli, dan hasil dari file image.

Kemudian perangkat lunak lainnya yang dibutuhkan, adalah VMWare Workstation. VMWare Workstation digunakan untuk melakukan *booting* sebuah file image yang dihasilkan kedalam lingkungan virtual. Dengan memanfaatkan metode ini, penyidik dapat melakukan pencarian sederhana pada *virtual machine* yang dijadikan barang bukti.

LiveView digunakan untuk membuat konfigurasi pada file DD yang akan di-*booting* kedalam lingkungan virtual. Namun agar LiveView dapat dipasang di dalam komputer, diperlukan *software* pendukung. Diantaranya adalah Java 1.5 atau yang lebih tinggi, serta Virtual Disk Development Kit (VDDK). Tanpa kedua perangkat lunak ini, LiveView tidak dapat dipasang di dalam komputer.

Setelah itu, diperlukan *software* FTK, untuk menganalisis seluruh isi dari file-file *virtual machine*. Dengan menggunakan FTK, bukti-bukti dapat ditemukan, sehingga dapat membantu jalannya keputusan di persidangan, dan menentukan apakah seseorang benar-benar bersalah atau tidak.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Skenario Kasus

Telah dilakukan penggerebekan di sebuah rumah kontrakan, di kawasan Jakarta Barat, yang diduga digunakan oleh seorang pengedar obat-obatan terlarang bernama Supriyanto. Namun, ketika diperiksa, ternyata rumah tersebut telah ditinggalkan penghuninya. Dari dalam rumah, polisi menemukan beberapa barang bukti, diantaranya adalah berupa sejumlah obat-obatan terlarang, dan sebuah notebook.

Untuk penyelidikan lebih lanjut, maka polisi membawa serta notebook tersebut ke laboratorium forensik. Namun ternyata polisi menemukan sebuah aplikasi *virtual machine* yang terpasang di dalam notebook tersebut. Oleh karena itu, selain membuat *back up* dari isi harddisk secara keseluruhan, polisi juga membuat file image dari *virtual machine* yang terpasang.

Dengan skenario kasus tersebut, akan dilakukan penyelidikan menyeluruh pada file *virtual machine* yang tersimpan pada harddisk tersebut. Hal ini dilakukan untuk membuktikan apakah kelompok tersebut benar-benar bersalah atau tidak, sekaligus untuk mengetahui data-data apa saja yang ada, dan aplikasi apa yang telah terpasang dalam *virtual machine* tersebut.

Untuk melakukan pembuktian, selain menyelidiki dengan menggunakan *software* forensik, penyidik juga memanfaatkan teknisi untuk mem-*booting* *virtual machine* tersebut, dengan tujuan untuk dapat menemukan petunjuk, serta dapat memperlihatkan secara jelas data-data apa saja yang ada di dalam *virtual machine* tersebut.

4.2 Access

Adalah tahap mengakses, atau mendapatkan, serta mengumpulkan barang bukti elektronik dari tempat kejadian perkara. Barang elektronik yang ditemukan dalam kasus ini adalah sebuah notebook dalam keadaan mati. Barang bukti elektronik ini kemudian dilaporkan dan disimpan ke laboratorium, untuk kemudian diperiksa oleh ahli forensik.

Hal yang perlu dilakukan dalam tahap ini, adalah :

1. Mencatat spesifikasi teknis dari barang bukti elektronik yang berupa notebook tersebut, seperti : merek, model, dan *serial number* (S/N) atau *product name* (PN).
2. Melakukan fotografi forensik. Fotografi forensik ini mencakup foto yang menggambarkan TKP secara keseluruhan
3. Membungkus barang bukti, dan beri label pada bagian luar untuk menandakan jenis barang bukti elektronik yang ada di dalamnya.
4. Bawa barang bukti tersebut, beserta catatan dan foto-foto yang didapat ke laboratorium untuk analisis lebih lanjut.

Single Evidence Form	
Case No.	Evidence No.
PLEASE COMPLETE FORM IN UPPERCASE	
Section B: Evidence Collection	
Date/Time Collected	Collected by
Site Address	
Section C: Evidence Details	
Date/Time Stored	
Storage Location	
Device Type	Capacity
Manufacturer	Model
Serial No.	
MDS Sum	
SHA-1 Sum	
Additional Information...	
☐ No any damage, marks and scratches ☐ Digital Image Taken ☐ Yes ☐ No	
Section D: Image Details	
Date/Time Imaged	Imaged by
Storage Location	
Image Filename	Image Size (in MB)
Additional Information...	
This form is to be used when collecting a hardware device containing data that may be of interest in a case. Guidelines: • Ensure that this form only refers to one item of evidence and that one is completed for each item of evidence • This form must be accompanied by Chain of Custody forms which detail the individuals that have handled the evidence • Further remarks can be noted overleaf in Section E: Remarks • It is important that these forms are kept with the evidence at all times • Upon handover or disposal please complete Section F: Evidence Handover	

Gambar 4. 1 Contoh Formulir Penerimaan Barang Bukti
(Sumber: <http://technoid.net>)

Formulir penerimaan barang bukti yang dibuat untuk keperluan penelitian ini, dapat dilihat pada lampiran.

4.3 Acquire

Acquire atau mengumpulkan data-data digital dari barang bukti elektronik berupa harddisk, merupakan tahapan selanjutnya setelah proses akses data selesai dilakukan. Dalam hal ini, hal-hal teknis yang harus dilakukan diantaranya adalah melakukan *write protect*, *imaging*, dan *hashing*.

4.3.1 Imaging Physical Disk

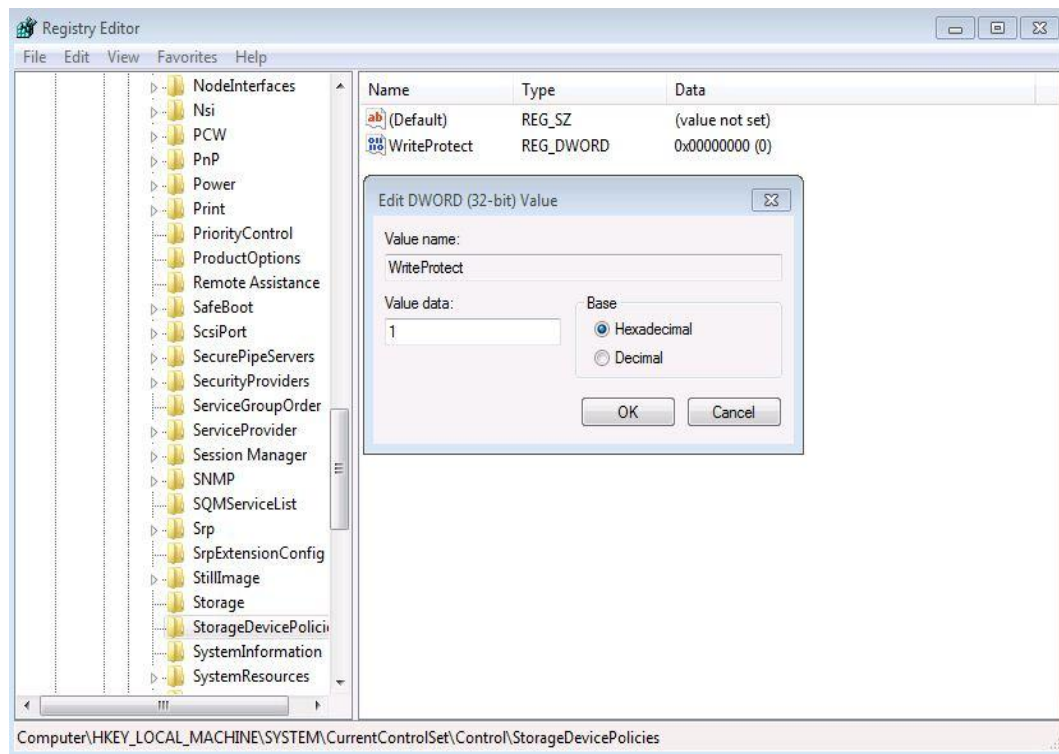
Sebelum melakukan *imaging* terhadap *virtual disk*, maka perlu dilakukan *imaging* pada harddisk fisik, untuk keperluan dokumentasi dan analisis lebih lanjut.

4.3.1.1 Write protect

Untuk melakukan *write protect* pada harddisk, dapat dilakukan dengan memanfaatkan Registry sebagai berikut:

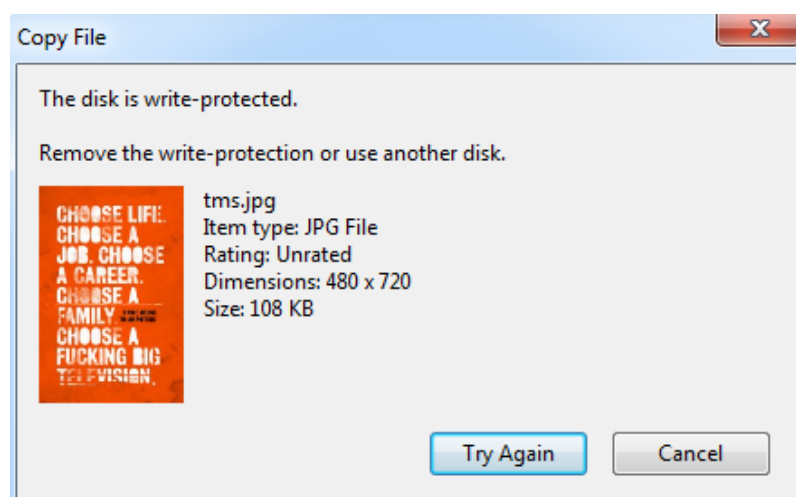
1. Buka Registry
2. Lalu cari Registry key berikut:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
3. Buat Key Baru dengan nama *StorageDevicePolicies*.
4. Lalu klik kanan pada *StorageDevicePolicies* lalu pilih New->DWORD (32-bit) Value namakan sebagai *WriteProtect*.
5. Double-click pada *WriteProtect* dan atur Value data menjadi “1”.

Tanpa me-*restart* komputer, *user* tidak akan dapat meng-copy file, dari dan ke dalam harddisk. Pada gambar 4.3 adalah tampilan, ketika dilakukan percobaan untuk meng-copy sebuah file gambar kedalam media penyimpanan eksternal.



Gambar 4. 2 Membuat Konfigurasi *Write protect*

Langkah diatas merupakan langkah paling sederhana dalam melakukan *write protect*. Ada pula beberapa langkah lain, yang menggunakan *hardware* khusus untuk melakukan *write protect* dari media penyimpanan.



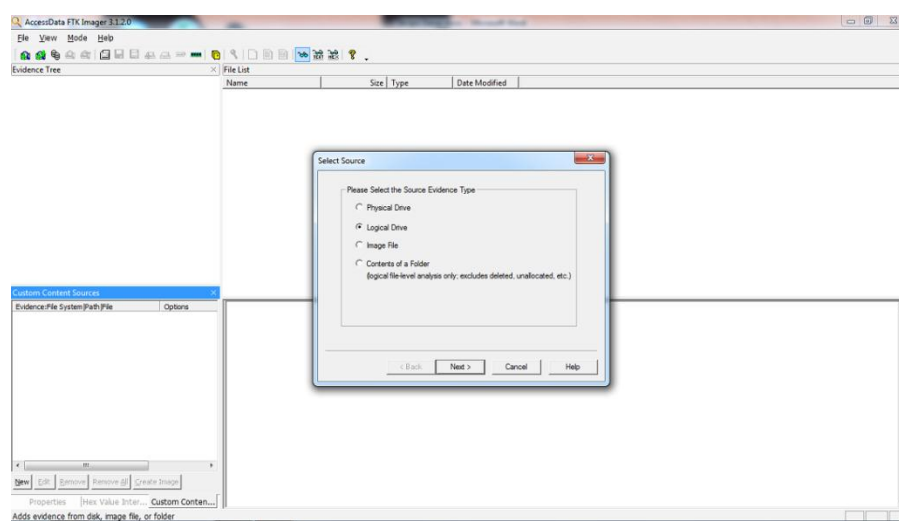
Gambar 4. 3 Bukti *Write protect*

Untuk menghapus *Write protect*, cukup mengganti value pada file registry yang bernama *WriteProtect* menjadi “0”. Maka user akan dapat mengirim dan menerima file dari berbagai media eksternal.

4.3.1.2 Cloning dan Disk Imaging

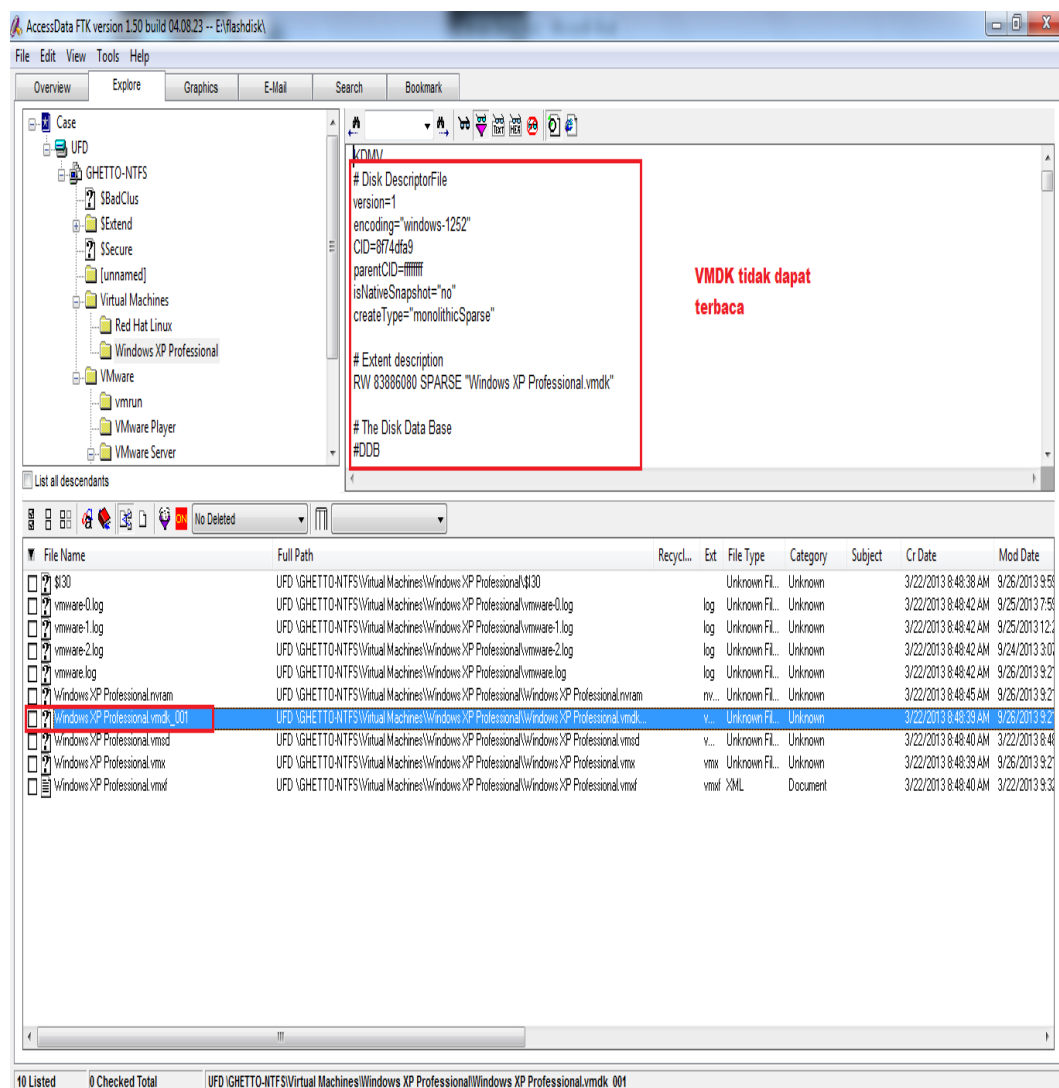
Cloning atau *back up* perangkat digital merupakan langkah yang harus dilakukan dalam penyelidikan forensik. Dalam melakukan *cloning* ini, seorang ahli forensik harus menggandakan perangkat elektronik yang bersangkutan. *Cloning* dapat dilakukan antara *device to device*, yang artinya apabila ada barang bukti berupa harddisk, maka harddisk tersebut di-*cloning* ke harddisk lain, yang memiliki spesifikasi sama. Namun, *cloning* juga dapat dilakukan dengan membuat disk image dari perangkat yang akan di-*cloning* tersebut.

Dalam melakukan disk imaging, dibutuhkan *software* bernama FTK Imager. Selain digunakan sebagai alat akuisisi, FTK Imager juga dapat digunakan untuk melihat sekilas barang bukti yang telah diakuisisi. Apabila bukti digital yang ada memerlukan investigasi lebih lanjut, maka perlu dibuat image dari bukti digital tersebut. Untuk menghindari perubahan atau perbedaan data, FTK Imager membuat duplikat dengan bit-per-bit. Maka *forensic image* akan sama dengan bukti asli, termasuk di dalamnya terdapat *file slack* serta *unallocated space*.



Gambar 4. 4 Proses Disk Imaging

Dalam kasus imaging pada *virtual machine*, yang perlu dilakukan adalah membuat file image dari file VMDK, atau *virtual machine* disk untuk keperluan analisis. Jika file vmdk tidak dibuat file image sendiri, maka FTK tidak akan dapat membaca file yang tersimpan di dalamnya. Hal tersebut dikarenakan FTK hanya dapat membaca file image menurut format yang telah dibuatnya.

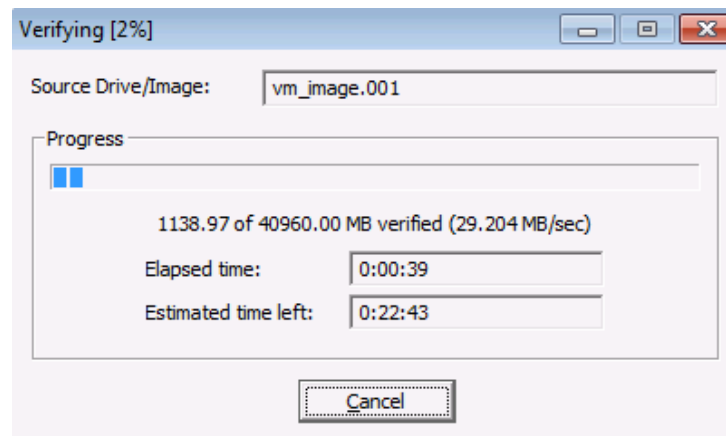


Gambar 4. 5 Struktur file dalam Virtual Machine

4.3.1.3 Hashing

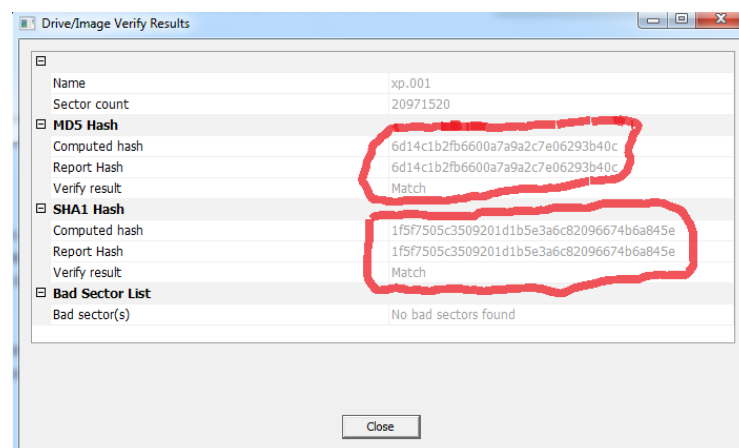
Proses *hashing* berguna untuk melihat derajat kesamaan antara barang bukti asli, dan barang bukti hasil kloning. Proses ini juga dikenal sebagai *digital*

fingerprint. Cara ini dapat dilakukan pada FTK Imager, dengan mencentang opsi “*verify image after they are created*” sebelum membuat image file. Pada gambar 4.6 berikut ini, dapat dilihat proses *image verification*.



Gambar 4. 6 Proses *hashing*

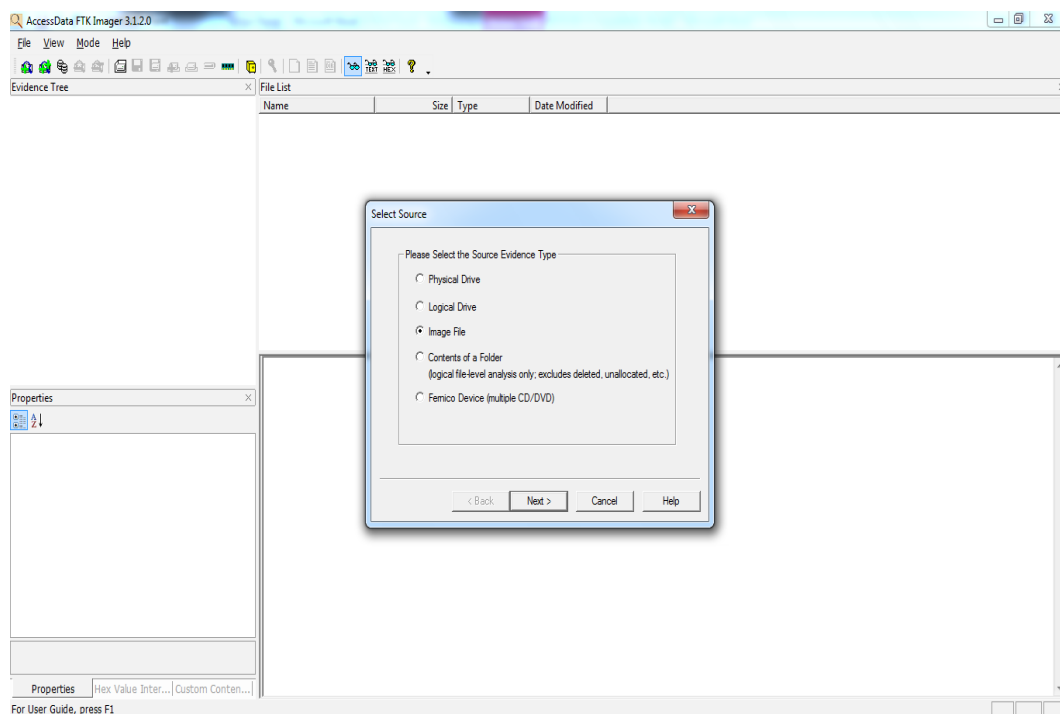
Pada gambar 4.7 dapat dilihat bahwa hasil dari *hashing* menunjukkan derajat yang sama. Baik dengan menggunakan algoritma MD5 maupun SHA1. Hal ini menunjukkan bahwa antara file asli, dan file image sama. Tidak ada yang berubah diantara keduanya.



Gambar 4. 7 Hasil dari proses *hashing*

4.3.2 Imaging Virtual Disk

Membuat file image dari virtual disk, tidak jauh berbeda dengan melakukan *imaging* pada hardisk fisik.

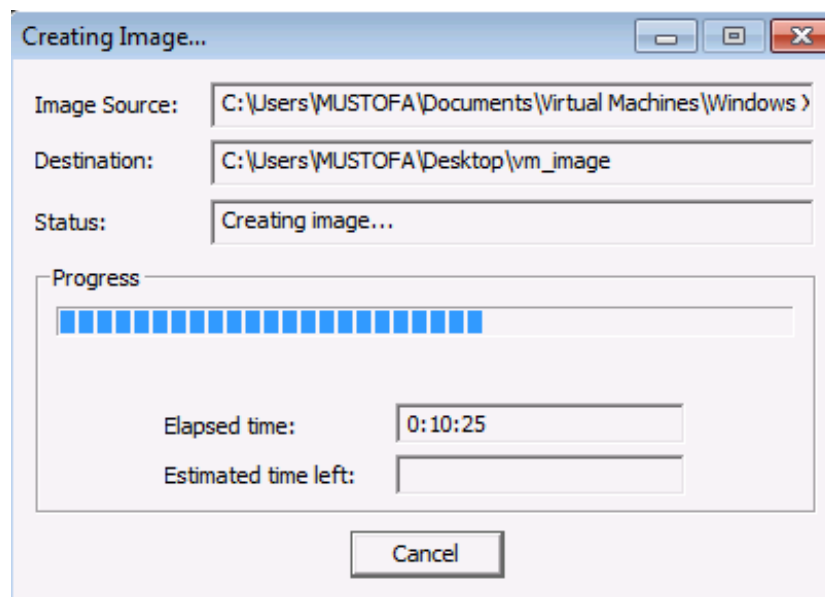


Gambar 4. 8 Membuat Image file dari Virtual Disk

Untuk melakukan *forensic imaging* pada *virtual disk*, dapat menggunakan tools seperti EnCase, maupun Forensik Tool Kit (FTK) Imager. Adapun langkah-langkah *forensic imaging* dengan menggunakan FTK Imager secara langsung adalah sebagai berikut:

1. Klik menu file
2. Pilih “*Create Disk Image*”.
3. Lalu pilih “*Image file*”.Kemudian pilih lokasi dimana file VMDK berada.
4. Pilih tipe image yang diinginkan (dalam penelitian ini, menggunakan DD image/raw).
5. Kemudian, akan tampil window untuk mengisi informasi serta keterangan dari barang bukti. Informasi tersebut antara lain :

- i. *Case Number* untuk memberikan nomor pada barang bukti. Sebaiknya menggunakan tahun, bulan, tanggal, serta jumlah masuknya kasus pada hari itu. Pada kasus ini akan diberi nomor 012345.
 - ii. *Evidence Number* adalah nomor barang bukti yang akan disidik. Dalam kasus ini, diberi nomor “01”
 - iii. *Unique Description* adalah deskripsi yang membedakan barang bukti lain yang satu dengan yang lainnya. Bisa dituliskan *Serial Number* dari barang bukti yang akan disidik. Atau dapat pula diberi keterangan lain.
 - iv. *Examiner* digunakan untuk mengisi nama orang yang menganalisis barang bukti digital, atau biasa disebut *forensic examiner*. Dalam kasus ini, seorang *forensic examiner*-nya bernama Mustofa.
 - v. *Notes* adalah catatan-catatan lain yang diperlukan untuk mengidentifikasi barang bukti.
6. Kemudian, tentukan lokasi yang akan digunakan untuk menyimpan file image pada *Image Destination Folder*. Lalu isikan pula nama dari file image tersebut pada kolom *Image Filename* tanpa menggunakan ekstensi. Untuk kasus ini, kita gunakan nama “winxp_vm”. Lalu klik *Finish*.
 7. Setelah selesai, maka akan muncul keterangan *image destination*. Lalu centang opsi *verify image after they are created* agar setelah selesai membuat file image, FTK secara otomatis dapat mencocokkan derajat kesamaan antara file asli, dan file hasil *cloning*. Pada gambar 4.9 berikut ini adalah proses imaging dari file *virtual machine*.



Gambar 4. 9 Proses Imaging *virtual machine*

Carvey (2009) dalam “*Windows Forensic Analysis*” menyebutkan bahwa DD adalah nama yang diberikan kepada aplikasi yang efektif dari dunia UNIX yang memiliki berbagai macam kegunaan, baik untuk menyalin file maupun harddisk secara keseluruhan. Format DD dipilih, karena telah lama dianggap sebagai standar untuk pembuatan image forensik. Dan banyak dari *tools* forensik yang mendukung format DD.

Dapat dilihat bahwa file vmdk image dipisahkan menjadi 28 file yang berbeda. Hal itu dikarenakan virtual disk memiliki kapasitas 40960MB, dan FTK Imager membuat file image secara default dengan membagi-nya per 1536MB.

Setelah proses imaging pada virtual disk selesai, maka secara otomatis proses *hashing* akan dilakukan, seperti pada proses akuisisi harddisk fisik. Kemudian langkah selanjutnya adalah melakukan analisis.

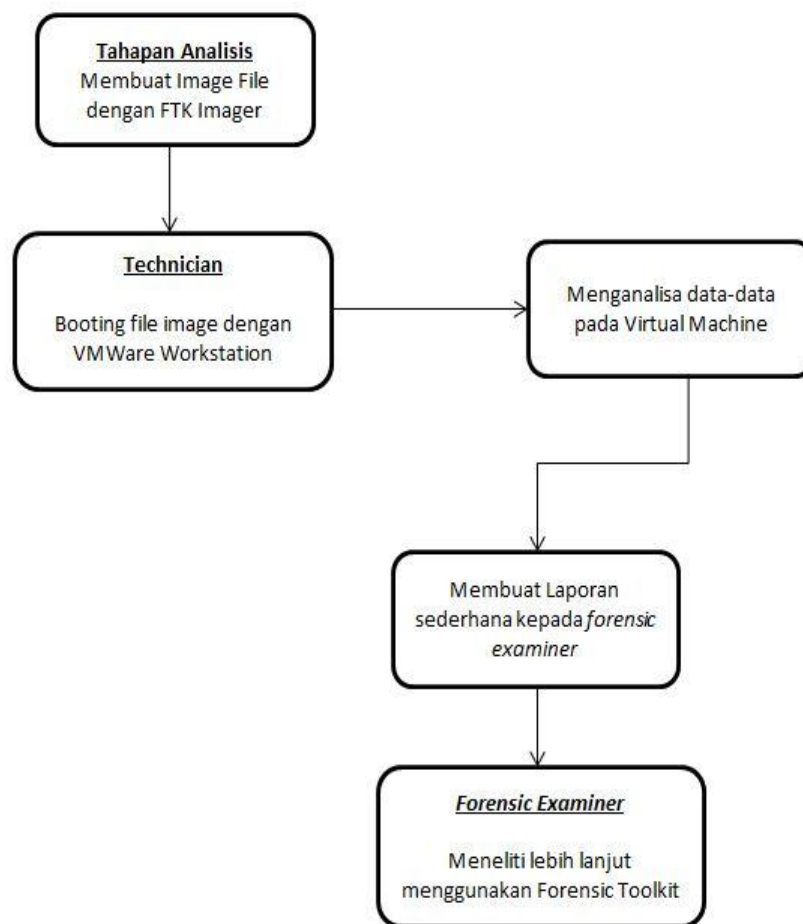
4.4 Analisis Kasus

Adalah proses analisis pada barang bukti digital. Dalam tahap analisis ini, kita membutuhkan *software* analisis Forensic Toolkit. Perbedaan antara FTK Imager dan FTK terletak pada kemampuannya menganalisis sebuah file image. Pada dasarnya FTK Imager digunakan untuk membuat file image, melakukan

hashing, dan melakukan analisis sederhana. Sedangkan FTK digunakan untuk melakukan analisis file secara menyeluruh.

Namun meski demikian, FTK Imager dan FTK merupakan dua perangkat yang saling melengkapi. Dalam penelitian ini, kedua tools tersebut digunakan baik dalam melakukan melakukan akuisisi maupun analisis.

Kemudian pada tahap analisis ini, penulis menggunakan beberapa sub-tahap, untuk mendapatkan hasil yang diinginkan. Gambar 4.10 berikut merupakan alur yang menggambarkan proses analisis dalam penelitian ini.



Gambar 4. 10 Tahapan Analisis Forensik

4.4.1 Hasil Analisis oleh Teknisi

Pada tahap ini, sebuah image file dari *virtual machine* Windows XP, akan di-booting dalam lingkungan virtual. Dengan teknik seperti ini, akan dapat memberi gambaran pada *forensic examiner* tentang lingkungan sistem operasi yang dipakai oleh pelaku tindak kriminal.

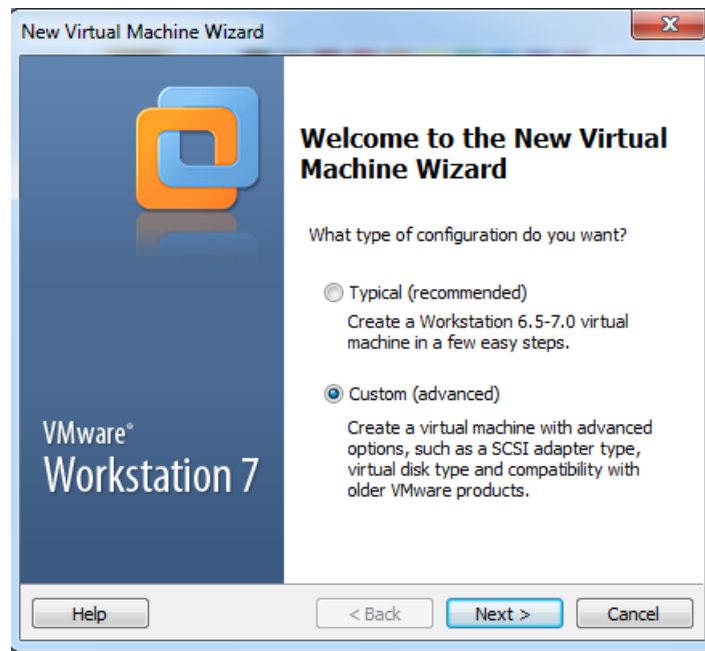
Sebelum dapat membooting file image kedalam lingkungan virtual, maka perlu dilakukan persiapan-persiapan seperti memasang VMWare Workstation dan Live View.

4.4.1.1 Instalasi VMWare

Sebelum melakukan booting ke lingkungan virtual, langkah yang paling utama adalah memasang *virtual machine* terlebih dahulu. Dalam penelitian ini, digunakan VMWare Workstation untuk meneliti *virtual machine* ke dalam lingkungan virtual. Telah disebutkan dalam bab sebelumnya bahwa VMWare digunakan untuk membooting *virtual machine* kedalam lingkungan virtual.

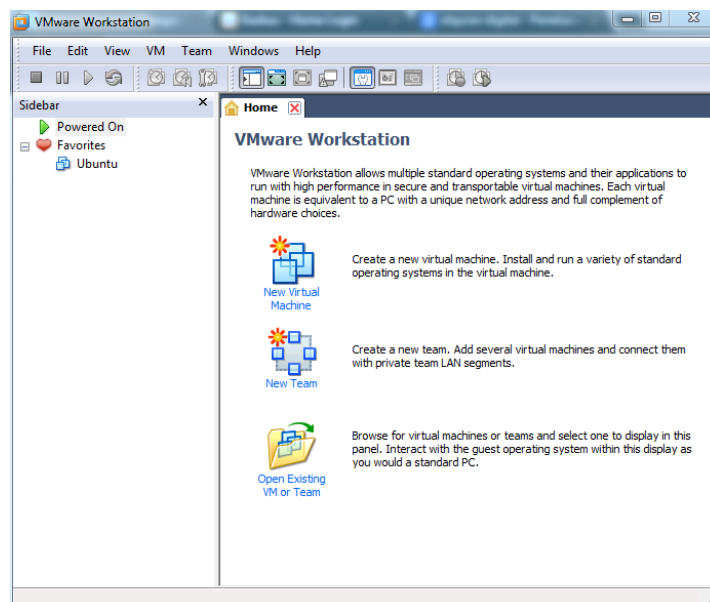
Apabila kita telah menentukan semua disk penyimpanan harus diletakkan pada satu buah file, Workstation menggunakan nama file yang telah disediakan untuk membuat file sebesar 40GB. Dan bila dalam pembuatan telah ditentukan bahwa lokasi disk harus ditempatkan dalam beberapa file, Workstation akan membuat nama file selanjutnya dengan menggunakan nama file yang telah diberikan.

Apabila kita telah menentukan bahwa sebuah file bersifat dinamis dan dapat bertambah besar, maka nama file berikutnya dibedakan dengan menggunakan penomoran pada file tersebut. Contohnya Windows XP-s001.vmdk. Dan apabila kita telah menentukan bahwa semua tempat penyimpanan dialokasikan ketika virtual disk dibuat, maka nama file berikutnya akan ditambah huruf “f” pada nomor file. Sebagai contoh Windows XP-f001.vmdk.



Gambar 4. 11 Instalasi *Virtual machine*

Setelah proses pemasangan VMWare selesai, maka akan tampil halaman VMWare seperti pada gambar 4.12 berikut ini.

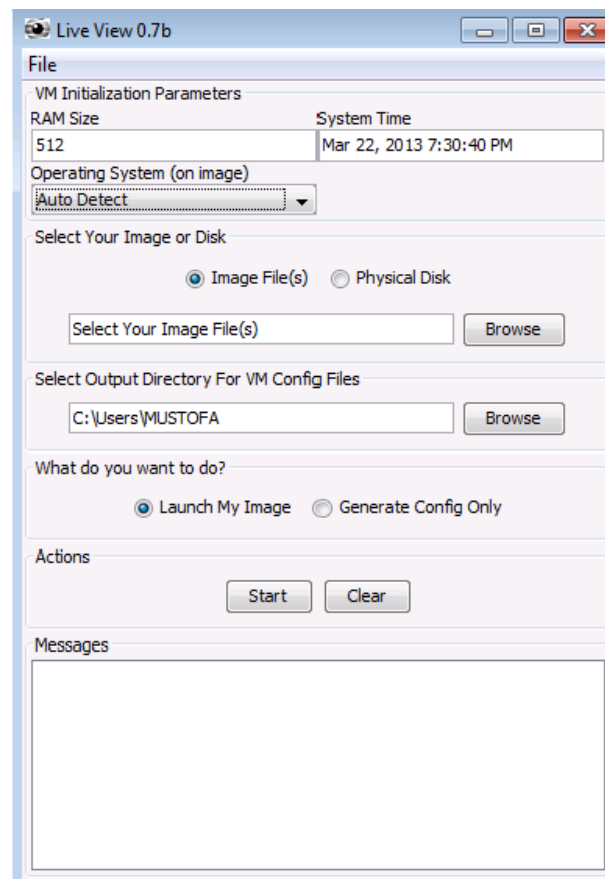


Gambar 4. 12 Tampilan awal *Virtual machine*

4.4.1.2 Membuat Konfigurasi *Virtual machine*

Dengan memanfaatkan LiveView, kita dapat membuat konfigurasi dari file image *virtual machine* yang akan dianalisis. Kemudian dengan konfigurasi tersebut, dapat dengan mudah dilakukan booting *virtual machine* kedalam lingkungan virtual.

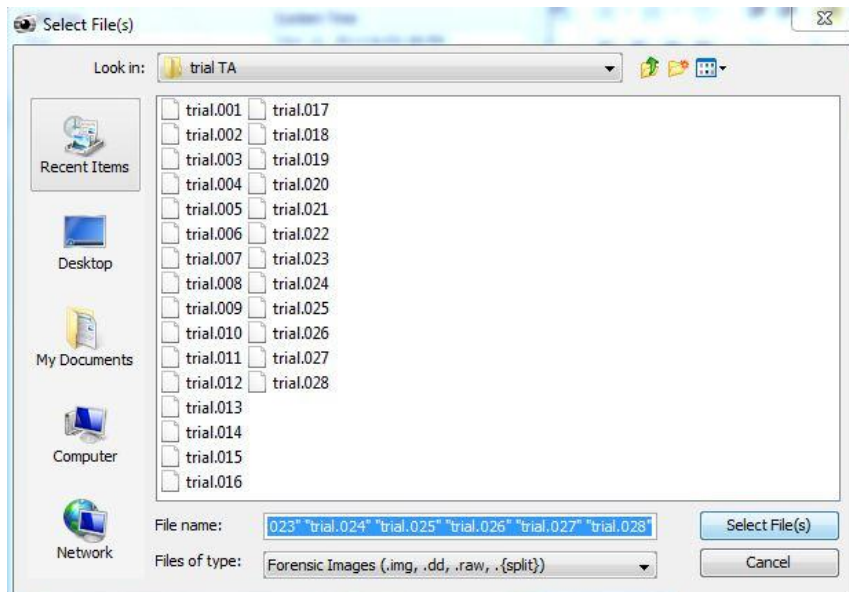
Namun sebelum dapat memasang LiveView ke dalam komputer, dibutuhkan aplikasi tambahan, yaitu Virtual Disk Development Kit (VDDK) serta Java. Apabila kedua aplikasi ini belum terpasang di dalam komputer, maka pemasangan LiveView tidak dapat dilanjutkan.



Gambar 4. 13 Tampilan Live View

Setelah LiveView selesai dipasang, langkah selanjutnya adalah membuat konfigurasi dari file image yang telah dibuat. Caranya yaitu dengan menjalankan LiveView, kemudian pilih image file pada pilihan yang tersedia, kemudian cari

folder yang berisi image file. Bila image file terdiri dari beberapa file, maka pilih semua image file tersebut. Kemudian pilih juga tempat untuk menyimpan hasil output dari konfigurasi tersebut. Dalam kasus ini, file konfigurasi akan disimpan dalam folder *C:\Users\Mustofa*.



Gambar 4. 14 Image File yang akan di-booting

Kemudian pada menu pilihan dibawah, ada dua opsi. Yaitu “*Launch My Image*” dan “*Generate Config Only*”. pada pilihan *Launch My Image*, LiveView akan membuat file konfigurasi dan secara otomatis membooting file konfigurasi yang telah dibuat, kedalam lingkungan virtual.

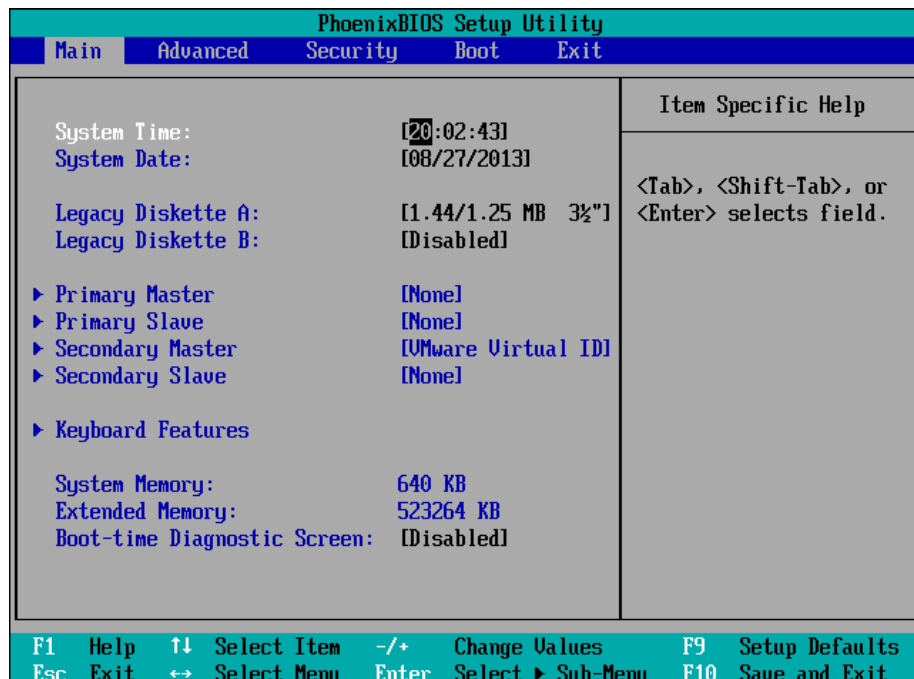
Setelah image di-booting melalui Live View, secara otomatis kita akan diarahkan kedalam lingkungan virtual dari *virtual machine*. Disini, kita dapat melakukan penyelidikan menyeluruh terhadap sistem operasi yang terpasang pada *virtual machine*. Hal yang bisa diteliti ketika sebuah sistem operasi sudah berjalan adalah file registry, link file, serta file log.

Untuk masuk kedalam BIOS (*Basic Input Output System*) dari *virtual machine*, kita dapat menekan tombol F2 pada keyboard ketika proses booting dimulai.



Gambar 4. 15 Proses Booting pada VMWare Workstation

Setelah itu, akan ditampilkan informasi BIOS dari *virtual machine* yang ada. Diantarany seperti tanggal, waktu, informasi memory. Seperti terlihat dalam gambar 4.15 berikut ini.



Gambar 4. 16 BIOS *virtual machine*



Gambar 4. 17 Tampilan desktop Windows XP Virtual Machine

4.4.1.3 Penyelidikan pada Link Files

Link Files merupakan bagian yang penting dalam proses penyelidikan. Karena setiap link file memiliki tanggal yang pembuatan, tanggal pengubahan, dan tanggal akses yang berbeda. Oleh karena itu, setiap link file dibuat, diubah, dan diakses termasuk kedalam file target. Dan apabila file target masih berada dalam media penyimpanan, maka file tersebut memiliki tiga tanggal berbeda.

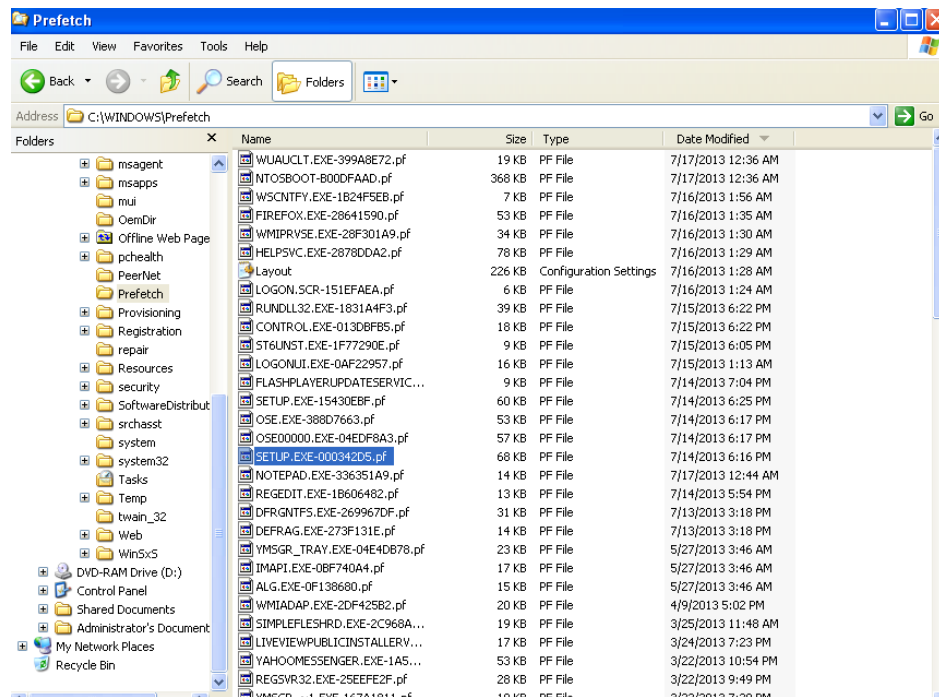
Name	Folder locker 1.0 (2).LNK
File Class	Regular File
File Size	755
Physical Size	4,096
Start Cluster	5,400,869
Date Accessed	6/5/2013 11:00:37 PM
Date Created	3/22/2013 11:47:09 PM
Date Modified	3/22/2013 11:47:09 PM
Encrypted	False
Compressed	False

Gambar 4. 18 General Properties pada salah satu link file

4.4.1.4 Penyelidikan pada prefetch folder

Fungsi dari prefetch folder adalah mengumpulkan berbagai informasi dari program yang dibutuhkan saat booting. Kemudian informasi tersebut disimpan dalam \Windows\Prefetch folder, sehingga ketika suatu saat ketika komputer dinyalakan lagi, maka program akan berjalan dengan lebih cepat. Windows XP menggunakan informasi dalam Prefetch folder untuk menyiapkan bagian program tersebut kedalam memori sebelum mereka benar-benar dibutuhkan sehingga ketika program-program tersebut dibutuhkan dalam proses loading, maka Windows akan berjalan dengan lebih cepat. Prefetch data dilewatkan kedalam layout.ini yang berlokasi pada direktori yang sama dengan prefetch file.

File layout.ini digunakan oleh peralatan defragmentasi untuk mengoptimasi layout file-file tersebut kedalam harddisk. Dalam prefetch folder juga dapat dilihat kapan user terakhir kali mengakses suatu program.

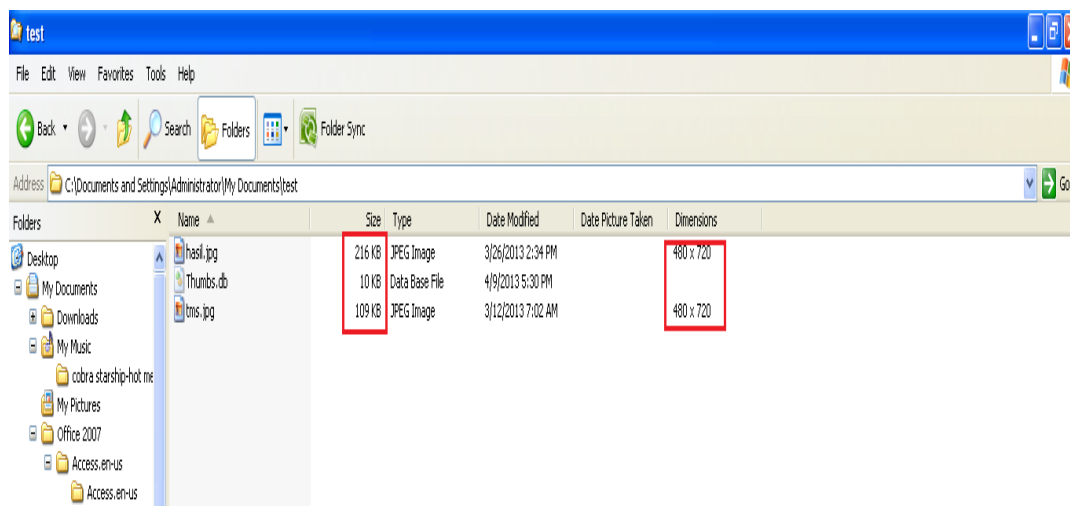


Gambar 4. 19 Isi dalam Folder Prefetch

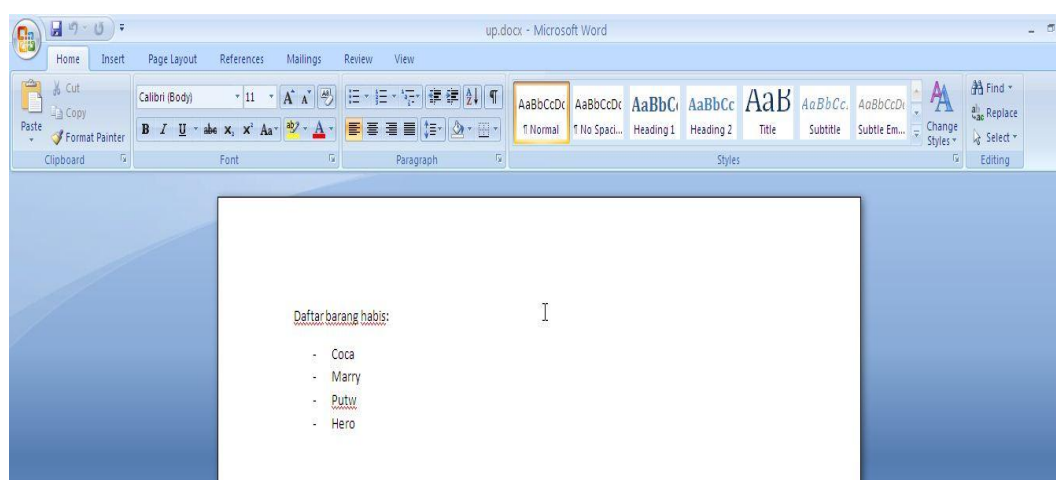
4.4.1.5 Hasil Pembahasan pada My Documents

Dalam folder *My Document* terdapat beberapa gambar, dimana ada dua gambar yang sama, dan dengan ukuran sama, namun memiliki besar file yang berbeda. Yaitu gambar dengan nama “tms.jpg” dan “hasil.jpg”.

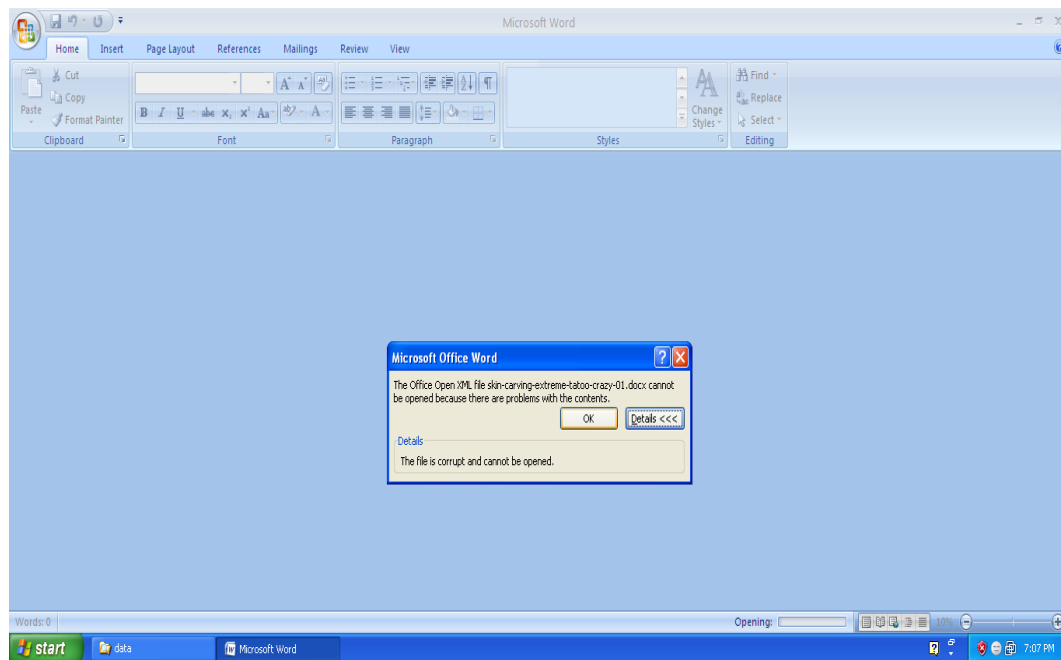
Kedua gambar tersebut sama-sama berukuran 480 x 720 piksel, dan sama-sama berformat .JPEG. Namun “hasil.jpg” memiliki ukuran file sebesar 109kb dan “tms 2.jpg” berukuran 216kb. Hasil dari temuan ini dapat dilaporkan kepada *forensic examiner* untuk penelitian lebih lanjut.



Gambar 4. 20 Isi dalam Folder My Pictures



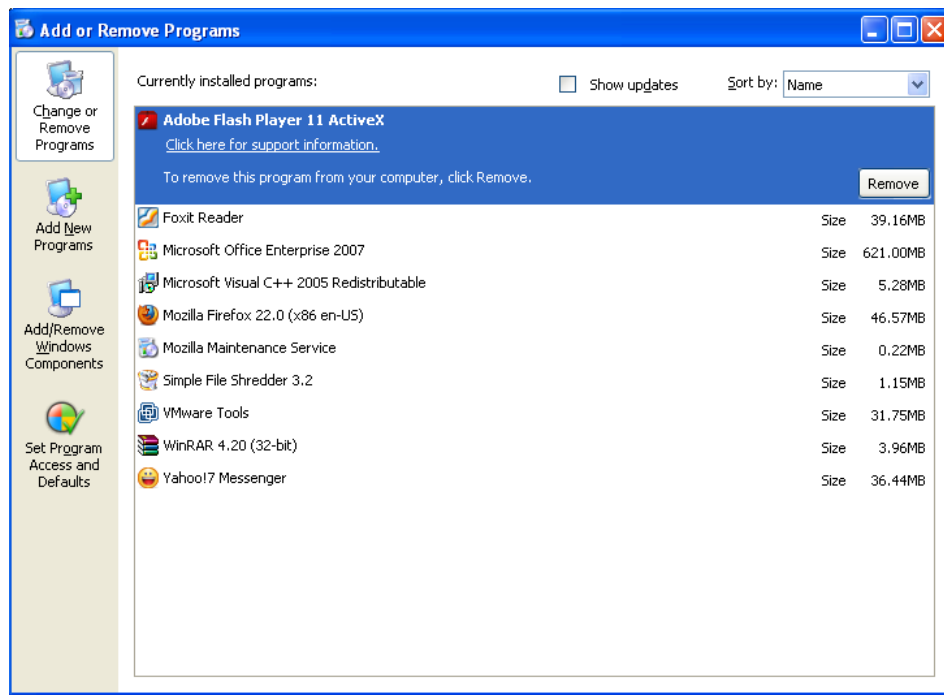
Gambar 4. 21 Dokumen yang dicurigai sebagai daftar narkoba



Gambar 4. 22 Salah satu dokumen corrupt

4.4.1.6 Hasil dan Pembahasan Software terpasang

Kemudian, teknisi komputer meneliti *software* yang terpasang di dalam *virtual machine* dengan melihat *control panel*. Ditemukan beberapa program yang terpasang pada mesin virtual Windows XP, diantaranya adalah browser Mozilla, Yahoo Messenger, dan File Shredder. Berikut adalah *screenshot* dari *control panel* pada *virtual machine* Windows XP.

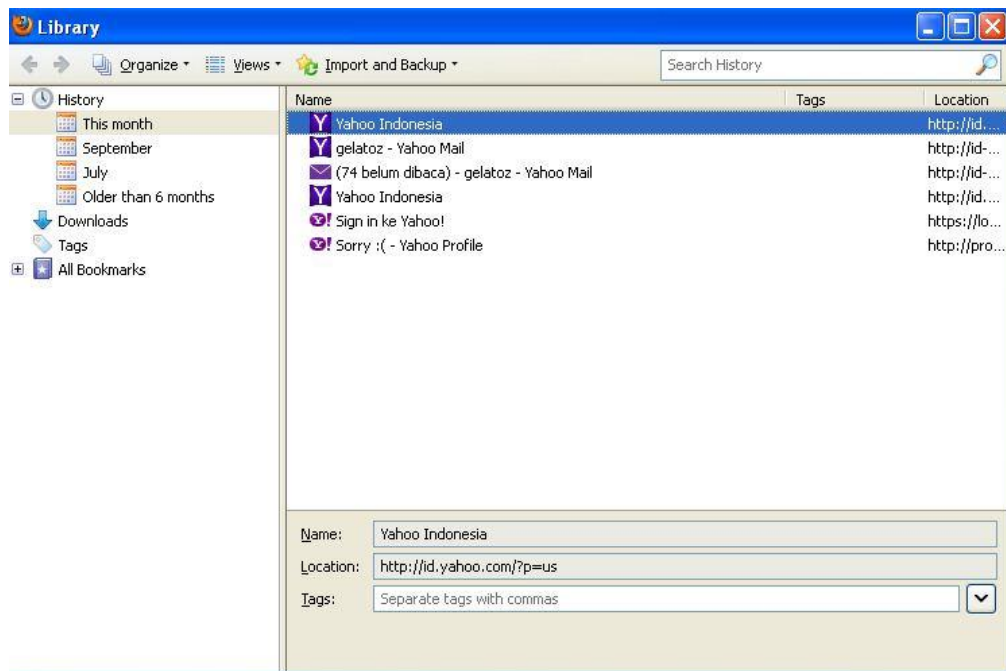


Gambar 4. 23 Software terpasang dilihat dari Control Panel

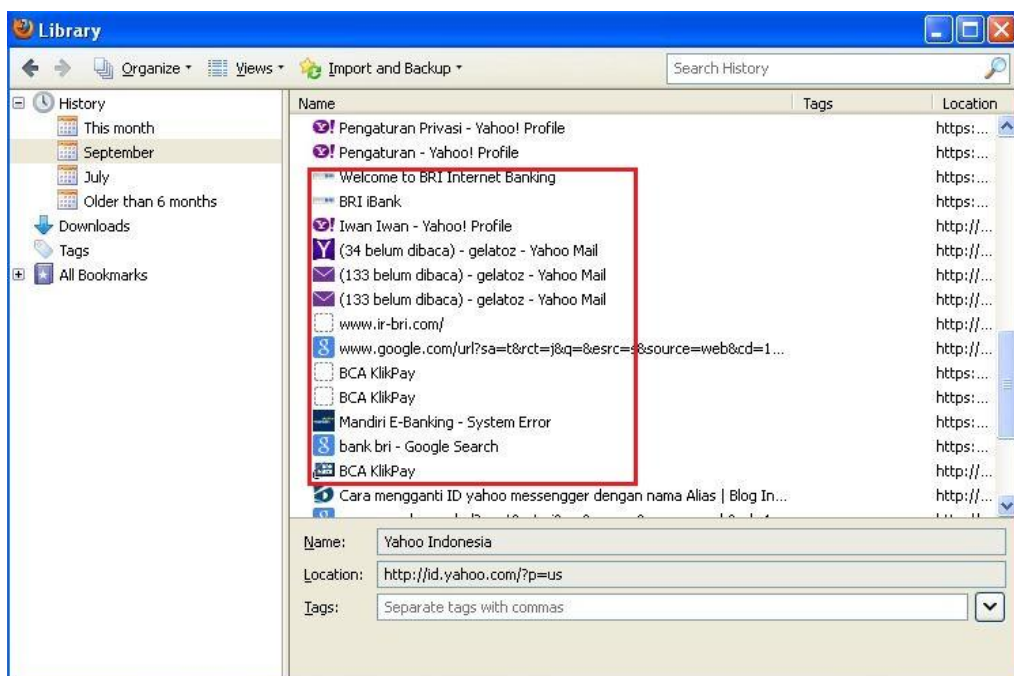
4.4.1.7 Hasil dan Pembahasan History Web Browser

Dalam history pada web browser Mozilla, teknisi menemukan beberapa halaman mencurigakan yang telah dikunjungi oleh tersangka. Diantaranya ialah history yang merujuk pada website Yahoo, *internet banking*, serta history yang merujuk pada situs-situs pornografi.

Pada gambar 4.24 dibawah ini, history mozilla menunjukkan bahwa tersangka memiliki akun email Yahoo yang bernama gelatoz. Dengan adanya temuan ini, dapat ditelusuri lebih lanjut tentang akun-akun yang pernah berhubungan dengan gelatoz.

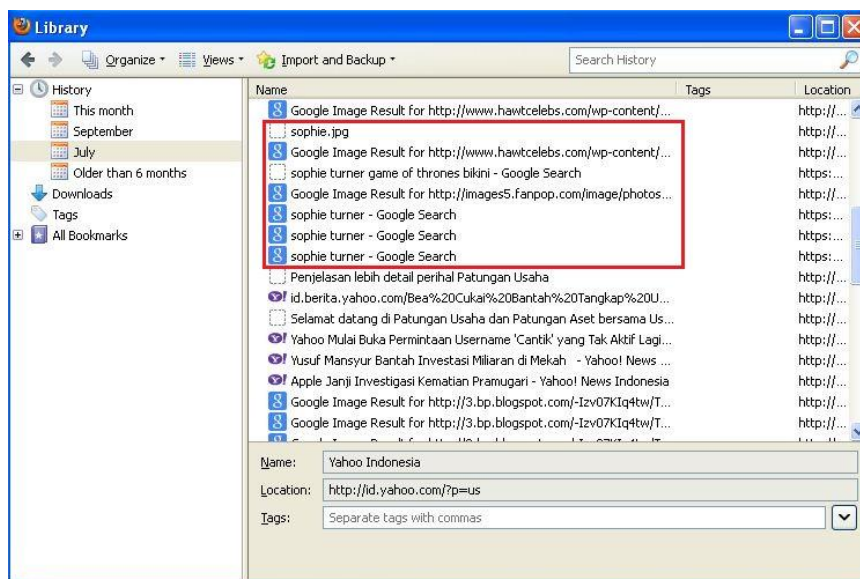


Gambar 4. 24 Yahoo Mail



Gambar 4. 25 Internet Banking

Gambar 4.25 diatas mengindikasikan adanya aktifitas internet banking pada beberapa bank berbeda. Diantaranya adalah BRI Internet Banking, Mandiri e-banking, dan BCA klikPay. Sedangkan pada gambar 4.26 ditemukan adanya history web browser yang merujuk pada situs pornografi.



Gambar 4. 26 History situs Pornografi

4.4.1.8 Laporan Sederhana tentang Hasil Temuan

Dari hasil temuan yang didapatkan oleh teknisi komputer diatas, maka kemudian dibuatlah sebuah laporan sederhana yang nantinya diserahkan kepada *forensic examiner* untuk analisis lebih lanjut. Laporan dapat berupa memo, ataupun catatan kecil mengenai hasil temuan.

4.4.2 Hasil Analisis oleh *Forensic Examiner*

Analisis pada tahap ini dilakukan oleh forensic examiner yang sudah ahli di bidangnya. Forensic examiner umumnya menggunakan tools forensik dalam melakukan tugasnya. Tool forensik yang digunakan dalam penelitian ini adalah Forensic Toolkit.

Pada tool FTK terdapat enam buah window. Yaitu window Overview, Explore, Graphics, E-mail, Search, dan Bookmark. Berikut akan dijelaskan kegunaan dan file yang dapat dilihat pada masing-masing window.

1. Overview

Jendela Overview menyediakan gambar kasus umum. Dari sisni dapat dilihat keseluruhan item dari hasil analisis. Di dalam jendela overview juga ditampilkan status file, dan kategori file.

2. Explore

Dalam jendela Explore kita dapat melihat struktur file yang tersimpan dalam berbagai folder, layaknya seperti dalam explorer di Windows. Pada jendela ini, examiner dapat melihat secara detail file serta data yang ada pada media penyimpanan.

3. Graphics

Jendela Graphics memungkinkan kita untuk melihat kasus dalam bentuk album gambar. Setiap file grafis disajikan dalam bentuk thumbnail.

4. E-mail

Pada jendela e-mail, diperlihatkan email dan pesan-pesan serta lampiran yang terkait dengannya. Namun tidak semua file email disimpan di dalam disk komputer.

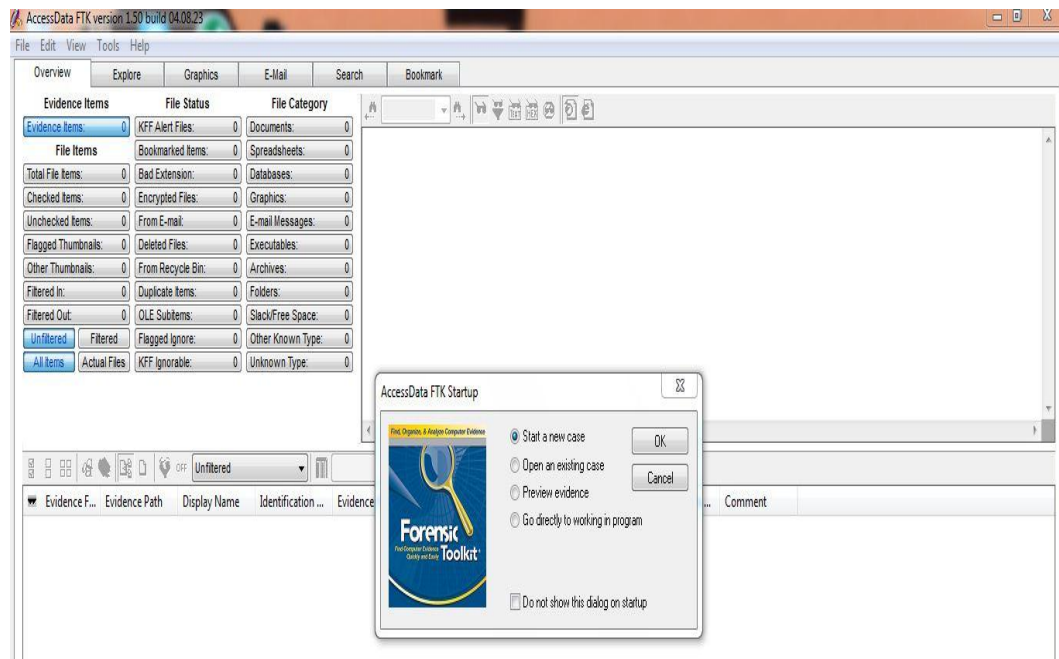
5. Search

Melalui jendela Search dapat menuntun kita pada pencarian yang merujuk pada pencarian index. Sehingga dapat mempercepat kinerja dalam proses penyelidikan.

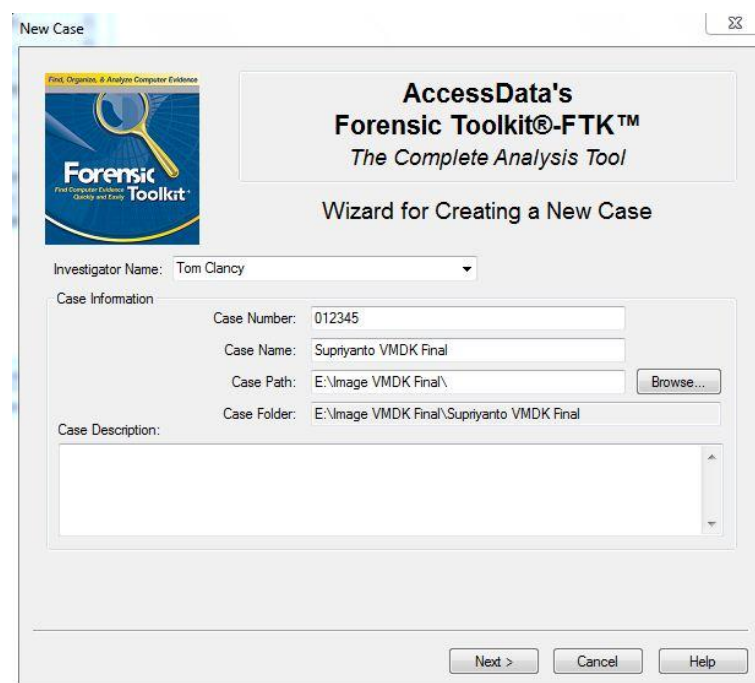
6. Bookmark

Jendela Bookmark memungkinkan kita untuk dapat melihat file yang telah kita tandai sebagai file penting dalam proses analisis.

Untuk mendapatkan data yang lebih akurat secara menyeluruh, diperlukan peran *forensic examiner*. Pada tahap ini dibutuhkan *software* FTK. Untuk memulai, jalankan *software* FTK, kemudian pilih “Start New Case”. Seperti terlihat pada gambar 4.27 dibawah ini.



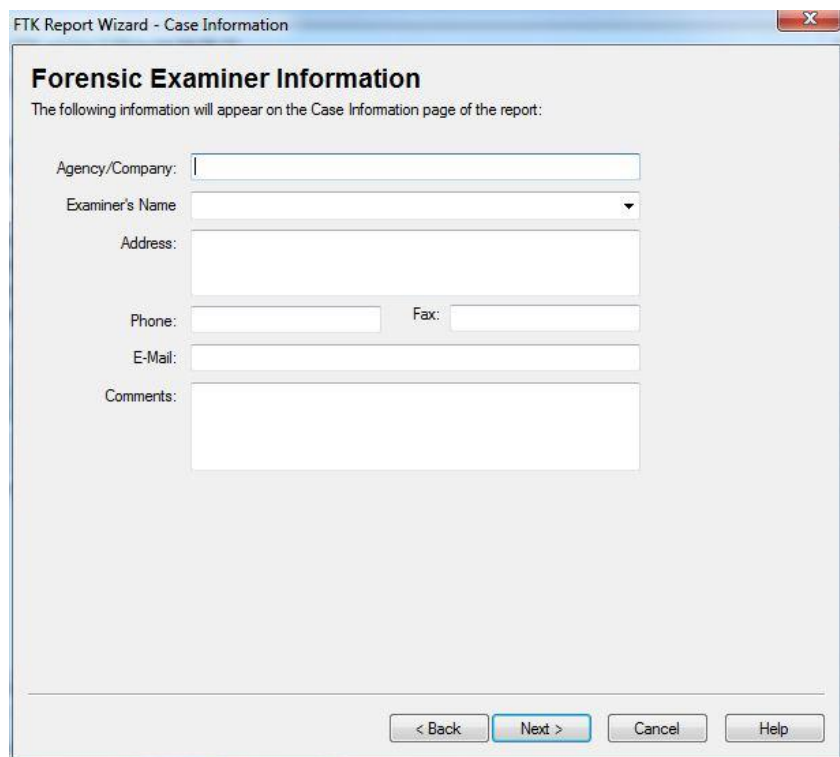
Gambar 4. 27 Forensic Toolkit Interface



Gambar 4. 28 New Case Dialog

Pada kotak dialog diatas, terdapat beberapa kolom harus diisi. Hal ini dilakukan untuk mendokumentasikan kasus yang sedang ditangani. Berikut penjelasan dari screenshot gambar 4.28:

1. Pada kolom Investigator Name, diisi dengan nama penyidik kasus (bukan *forensic examiner*).
2. Pada kolom Case Number diisi dengan Nomor Kasus
3. Kolom Case Name diisi dengan nama kasus
4. Case Path adalah kolom lokasi drive yang akan dianalisis
5. Case Folder adalah nama folder yang akan dianalisis
6. Case Description diisi dengan deskripsi kasus yang sedang ditangani (optional).
7. Setelah itu, klik next, maka akan muncul tampilan seperti pada gambar 4.29 berikut ini.



FTK Report Wizard - Case Information

Forensic Examiner Information

The following information will appear on the Case Information page of the report:

Agency/Company:

Examiner's Name:

Address:

Phone: Fax:

E-Mail:

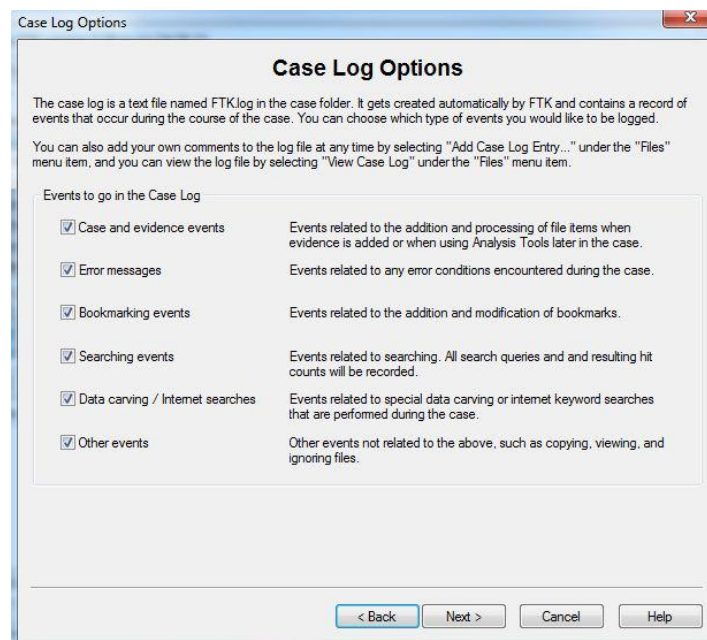
Comments:

< Back Next > Cancel Help

Gambar 4. 29 Informasi *Forensic examiner*

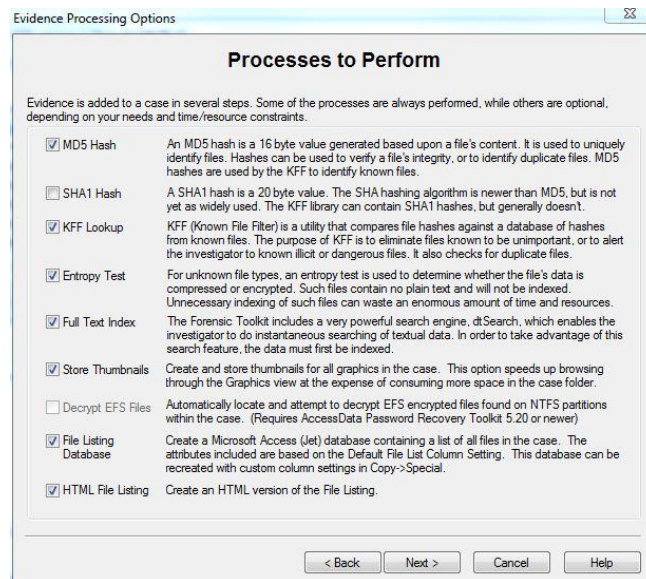
Pada gambar 4.29, adalah kotak dialog yang harus diisi mengenai data seorang *forensic examiner*. Berisi nama instansi, nama lengkap examiner, alamat, nomor telepon, e-mail, serta catatan atau komentar mengenai data digital yang akan dianalisis.

Setelah selesai mengisi data pada form *forensic examiner*, kemudian klik next, maka akan tampil halaman “*Case Log Options*”. Halaman ini memungkinkan kita untuk dapat menyimpan file log dari hasil analisis yang kita kehendaki. Pilihan yang ada, dapat dilihat pada gambar 4.30 berikut ini.



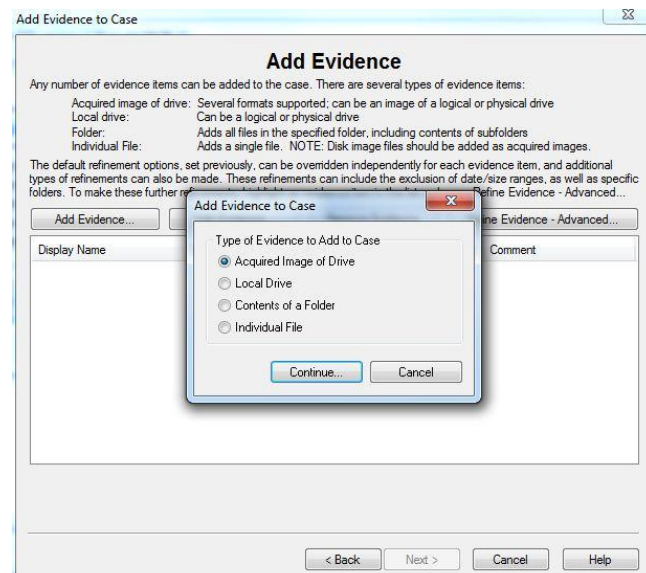
Gambar 4. 30 Case Log Options

Setelah itu, akan muncul kotak dialog “*Processess to Perform*” yang memungkinkan kita untuk memilih proses yang akan dilakukan seperti hashing, full text indexing. Langkah ini merupakan optional. Untuk menghemat waktu, kita juga dapat menyaring data yang tidak relevan dengan proses analisis. Opsi ini dapat dilakukan pada menu “*Refine Case*”.



Gambar 4. 31 Proses optional

Kemudian setelah semua proses optional dilakukan, maka akan muncul kotak dialog “Add Evidence”. Klik “Add Evidence” kemudian pilih “Acquired Image of Drive”. Klik “Continue” lalu pilih lokasi dimana file image berada. Lali klik “next” kemudian klik “finish”



Gambar 4. 32 Menentukan Lokasi Barang bukti

4.4.2.1 Known File Filter (KFF)

KFF adalah utility FTK yang berfungsi untuk membandingkan hash sebuah file terhadap database dari file-file yang telah diketahui. Tujuan utama KFF adalah untuk mengeliminasi file yang dapat diabaikan, sebagai contoh seperti *system file* maupun *program file*. Atau bisa juga berfungsi sebagai peringatan terhadap file yang berbahaya. KFF juga dapat mengecek file duplikat. Mengecek file yang berisi file lain, seperti Zip serta file email yang berisi *attachment*. File-file ini disebut sebagai *container file*.

Ketika KFF mengidentifikasi sebuah *container file* sebagai *ignorable file* (file yang dapat diabaikan), FTK tidak akan mengekstrak komponen dari file tersebut. Kemudian, ketika KFF digunakan, barang bukti akan dipisahkan kedalam dua kategori berbeda, yaitu file yang diabaikan (seperti sistem file) dan barang bukti yang akan dianalisis lebih lanjut.

Secara umum, database KFF (ADKFFLibrary.hdb) dipasang kedalam program folder FTK. Yaitu *AccessData\AccessData Forensic Toolkit\Program*. Apabila database KFF dipasang ke lokasi yang berbeda, maka examiner harus menunjukkan dimana letak database KFF tersebut.

4.4.2.2 Hasil Analisis Struktur file pada Virtual Machine

Name	Size	Type
Windows XP Professional.vmx.lck	1	Directory
\$I30	4	NTFS Index All...
vmware-0.log	88	Regular File
vmware-1.log	89	Regular File
vmware-1.log.FileSlack	4	File Slack
vmware-2.log	90	Regular File
vmware-2.log.FileSlack	3	File Slack
vmware.log	98	Regular File
vmware.log.FileSlack	3	File Slack
Windows XP Professional.nvram	9	Regular File
Windows XP Professional.nvram.FileSlack	4	File Slack
Windows XP Professional.vmdk	6,192,384	Regular File
Windows XP Professional.vmsd	0	Regular File
Windows XP Professional.vmx	3	Regular File
Windows XP Professional.vmx.FileSlack	2	File Slack
Windows XP Professional.vmx.f	2	Regular File
Windows XP Professional.vmx.f.FileSlack	3	File Slack

Gambar 4. 33 Struktur File Virtual Machine

File-file yang umumnya terkait dengan *virtual machine*, diantaranya adalah sebagai berikut:

1. Log file : Pencatatan aktifitas pada *virtual machine*.
2. .VMDK (*Virtual machine Disk*) adalah media penyimpanan pada sistem operasi virtual.
3. .VMX merupakan file konfigurasi dari sebuah mesin virtual. Seperti informasi sistem operasi, *information disk*, dsb.
4. .NVRAM merupakan file yang menyimpan informasi BIOS pada *virtual machine*.
5. .VMSD merupakan file yang berisi metadata *snapshot*
6. .VMXF apabila sebuah mesin virtual dihapus, maka akan ada sisa dari file konfigurasi ini.

4.4.2.3 Hasil Analisis pada *Deleted Files*

Menurut keterangan pada website resmi Microsoft, ada tiga kemungkinan yang terjadi pada file-file yang terhapus. Yaitu:

1. File yang terhapus akan dipindah ke Recycled/Recycler Bin.
2. Rincian berikut ini direkam di dalam file INFO2 pada setiap file yang dihapus:
 - a. Index
 - b. Waktu dan tanggal ketika file dihapus
 - c. Lokasi drive dari file yang dihapus
 - d. Full *path*
 - e. Ukuran file
3. File yang terhapus diberi nama kembali, menggunakan syntax berikut ini:
D<drive original dari sebuah file> <#>. <original extension>

Keterangan pada <#> adalah perintah dimana sebuah file diletakkan di dalam Bin. Apabila user menghapus isi Recycle Bin, yang dapat kita adalah dengan melihat dan menganalisa file INFO2. Dengan memanfaatkan file INFO2,

examiner dapat melihat tanggal dan waktu ketika sebuah file dihapus, pada drive mana file tersebut dihapus, original path file, dan ukuran file.

4.4.2.4 Hasil dan Pembahasan pada Signature Analysis

Signature analysis merupakan prosedur otomatis untuk mengidentifikasi bukti-bukti potensial. Sebuah file *signature* merupakan header atau footer (atau keduanya) di dalam file yang mengindikasikan sebuah aplikasi berhubungan dengan tipe-tipe file tertentu (Craig, 2005). Kita dapat melihat perbedaan jenis *file signature* pada gambar 4.34 sampai gambar 4.37 berikut ini.

vbuletin_lightbox.js	13	Regular File	11/18/2010 2:5	original-brand09.jpg	211	Regular File	7/27/2012 3:48:...
polafrekwensi.jpg	20	Regular File	11/18/2010 2:5	original-brand10.jpg	204	Regular File	7/27/2012 3:49:...
vbuletin_global.js	26	Regular File	11/18/2010 2:5	original-brand11.jpg	211	Regular File	7/27/2012 3:50:...

0000 FF D8 FF E0 00 10 4A 46-49 46 00 01 01 01 00 48	y0yã··JFIF·····H	000000 FF D8 FF E0 00 10 4A 46-49 46 00 01 02 00 00 64	y0yã··JFIF·····H
0010 00 48 00 00 FF DB 00 43-00 1E 14 16 1A 16 13 1E	·H··yü·C·······	000100 00 64 00 00 FF EC 00 11-44 75 63 6B 79 00 01 00	·d··yi··Ducky··
0020 1A 18 1A 21 1F 1E 23 2C-4A 30 2C 29 29 2C 5B 41	···!··#·J0·)·)·[A	000200 04 00 00 00 14 00 00 FF-EE 00 0E 41 64 6F 62 65	·······yi··Adobe
0030 44 36 4A 68 5F 71 6F 69-5F 68 66 76 85 8A 90 76	D6T7·nni·hfv···v	000300 00 64 C0 00 00 00 01 FF-DB 00 04 00 12 0E 0E 0E	·dã···yü······

Gambar 4. 34 Signature file JPG

firstnew.gif	1	Regular File	7/14/2011 6:09:...	firstnew.gif	1	Regular File	7/14/2011 6:09:...
follow_button.htm	33	Regular File	7/14/2011 6:09:...	follow_button.htm	33	Regular File	7/14/2011 6:09:...
ga.js	30	Regular File	7/14/2011 6:09:...	ga.js	30	Regular File	7/14/2011 6:09:...
hansip.gif	2	Regular File	7/14/2011 6:09:...	hansip.gif	2	Regular File	7/14/2011 6:09:...

0001 47 49 46 38 39 61 0C 00-0C 00 E6 00 00 FF FF FF	GIF89a·····e·yüü	0001 47 49 46 38 39 61 52 00-19 00 E6 7F 00 D5 D6 D6	GIF89aR·····e·öÖ
0100 50 59 8A 51 5A 8B BB DF-E2 CF D0 D3 A5 C5 E4 82	PY·Q2··ääIDöyÄä	0100 C2 C5 C6 DC EC BF E5 F0-D3 7F C0 26 37 7E 3D 59	ÄÄEÜi·äöÖ·Äe7~·Y
0200 94 AC 80 8D E4 50 58 8B-7B 88 DE 82 8A AB 52 5B	····aPX·{·P·e[R	0200 98 68 C0 DD 88 E3 E3 E4-B5 B5 B5 BF D4 C4 AE AE	·hÄY·äääpupuz·öÄö
0300 87 83 9B C7 69 76 AD 88-9B F9 AA CB F4 8B 97 B8	····Çiv~···ü·Eö··	0300 AE 89 CB 3F 67 BE 44 F7-F1 FE 75 B9 3C 53 B9 49	···EzgzD·äpu·+S·I

Gambar 4. 35 Signature file GIF

Sportindo_com_-_The...	6,743	Regular File	7/13/2013 3:05:...	Sportindo_com_-_The...	6,743	Regular File	7/13/2013 3:05:...
TheMagz-2012-12.pdf	5,186	Regular File	7/13/2013 3:04:...	TheMagz-2012-12.pdf	5,186	Regular File	7/13/2013 3:04:...
TheMagz-2013-07.pdf	6,412	Regular File	7/13/2013 3:04:...	TheMagz-2013-07.pdf	6,412	Regular File	7/13/2013 3:04:...
Thumbs.db	56	Regular File	11/5/2011 11:4:...	Thumbs.db	56	Regular File	11/5/2011 11:4:...

000000 25 50 44 46 2D 31 2E 37-0D 25 E2 E3 CF D3 0D 0A	\$PDF-1.7·\$·00000000	000000 25 50 44 46 2D 31 2E 37-0D 25 E2 E3 CF D3 0D 0A	\$PDF-1.7·\$·ääIÖ··
000010 31 31 38 39 20 30 20 6F-62 6A 0D 3C 3C 2F 4C 69	1189 0 obj 000010	000010 39 35 35 20 30 20 6F 62-6A 0D 3C 3C 2F 4C 69 6E	955 0 obj <</Lin
000020 6E 65 61 72 69 7A 65 64-20 31 2F 4C 20 36 35 36	nearized 1 000020	000020 65 61 72 69 7A 65 64 20-31 2F 4C 20 36 39 30 34	earized 1/L 6904
000030 35 31 36 37 2F 4F 20 31-31 39 31 2F 45 20 31 30	5167/O 119 000030	000030 35 32 32 2F 4F 20 39 35-37 2F 45 20 31 33 32 34	522/O 957/E 1324

Gambar 4. 36 Signature File PDF

Latihan yg benar.docx	31	Regular File	8/18/2011 5:16:...	Latihan yg benar.docx	31	Regular File	8/18/2011 5:16:...
Six Pack.docx	39	Regular File	8/27/2011 11:3:...	Six Pack.docx	39	Regular File	8/27/2011 11:3:...
tabel-nutrisi.htm	115	Regular File	1/18/2012 2:12:...	tabel-nutrisi.htm	115	Regular File	1/18/2012 2:12:...

0000 50 4B 03 04 14 00 06 00-08 00 00 00 21 00 2F B2	PK······!·!·/4	0000 50 4B 03 04 14 00 06 00-08 00 00 00 21 00 1E 19	PK······!·!·
0010 A8 74 81 01 00 00 D9 05-00 00 13 00 08 02 5B 43	·t····ü······[C	0010 EF 75 73 01 00 00 54 05-00 00 13 00 08 02 5B 43	iua···T······[C
0020 6F 6E 74 65 6E 74 5F 54-79 70 65 73 5D 2E 78 6D	ontent_Types].xm	0020 6F 6E 74 65 6E 74 5F 54-79 70 65 73 5D 2E 78 6D	ontent_Types].xm
0030 6C 20 A2 04 02 28 A0 00-02 00 00 00 00 00 00 00	l·e··{······	0030 6C 20 A2 04 02 28 A0 00-02 00 00 00 00 00 00 00	l·e··{······

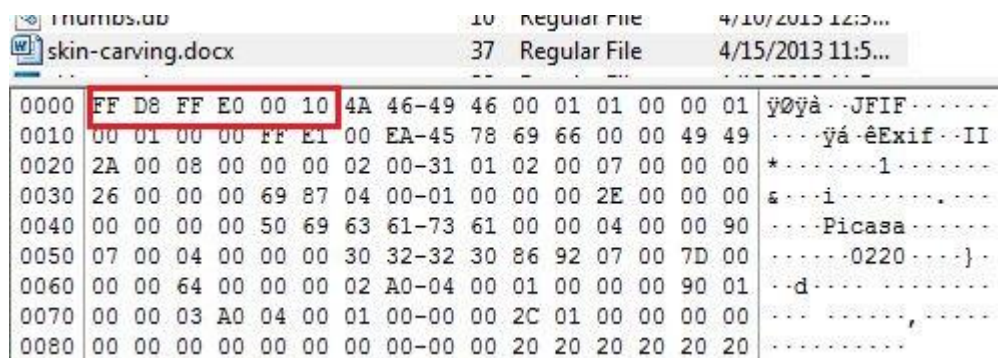
Gambar 4. 37 Signature File Microsoft office DOCX

Dari beberapa gambar diatas, dapat dilihat bahwa setiap jenis file ekstensi memiliki *signature file* yang berbeda. Rangkuman perbedaan *file signature* dari ke-empat *screenshot* diatas dapat dilihat pada tabel 4.1 dibawah ini.

Tabel 4. 1 *File Signature*

Typ File	File Signature
PDF	25 50 44 46 2D
JPG	FF D8 FF E0
GIF	47 49 46 38
DOCX	50 4B 03 04 14

Signature file tidak akan berubah meskipun ekstensi dari sebuah file telah diganti. Sehingga berguna untuk melihat file yang sengaja disembunyikan. Bukti bahwa *signature file* tidak akan berubah meski ekstensi dari sebuah file telah diubah, dapat dilihat pada gambar 4.38 berikut.



Gambar 4. 38 Bukti file signature

Dari gambar diatas, dapat kita lihat bahwa file dokumen yang bernama “*skin-carving.docx*” memiliki *file signature* FF D8 FF E0, yang menandakan *file signature* tersebut merupakan *file signature* dari file JPG. Maka dari bukti yang ada tersebut, dapat dipastikan bahwa file “*skin-carving.docx*” merupakan file gambar berformat .jpg dan pemilik komputer telah mengganti ekstensi dari file gambar tersebut menjadi .docx.

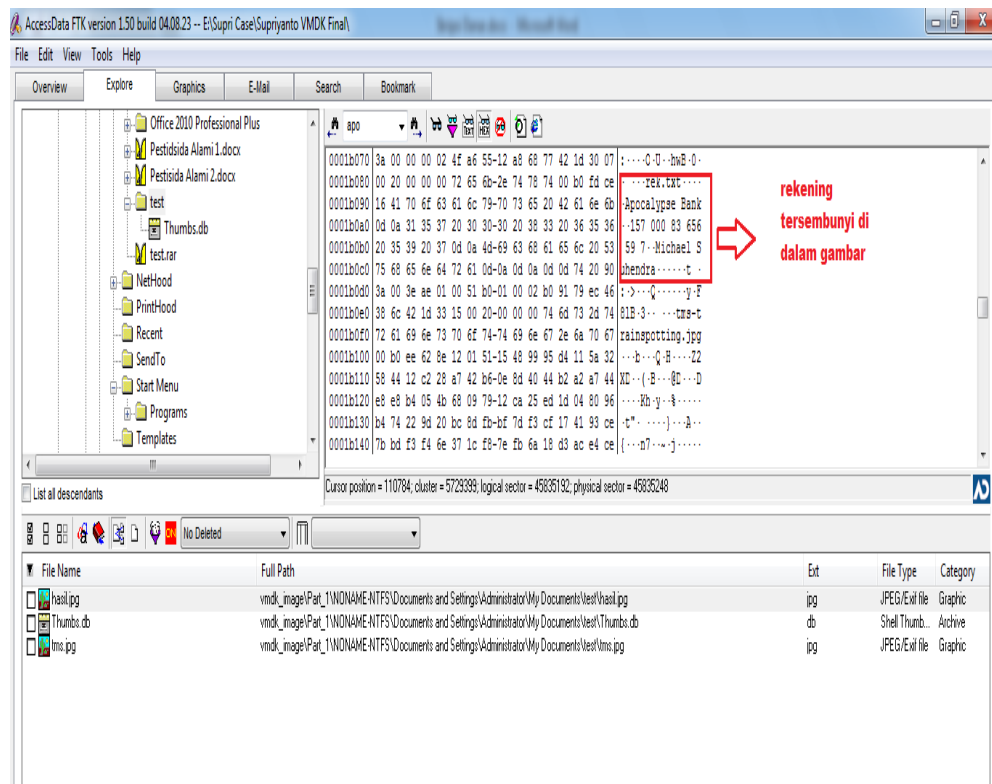
4.4.2.5 Penyelidikan lebih lanjut dari Laporan Teknisi

Dari laporan dan penjelasan yang diberikan oleh teknisi, maka *examiner* bertugas menyelidiki lebih lanjut hasil temuan teknisi tersebut. Lalu memeriksa image file yang ada, untuk kemudian dicocokkan dengan hasil analisis dari teknisi.

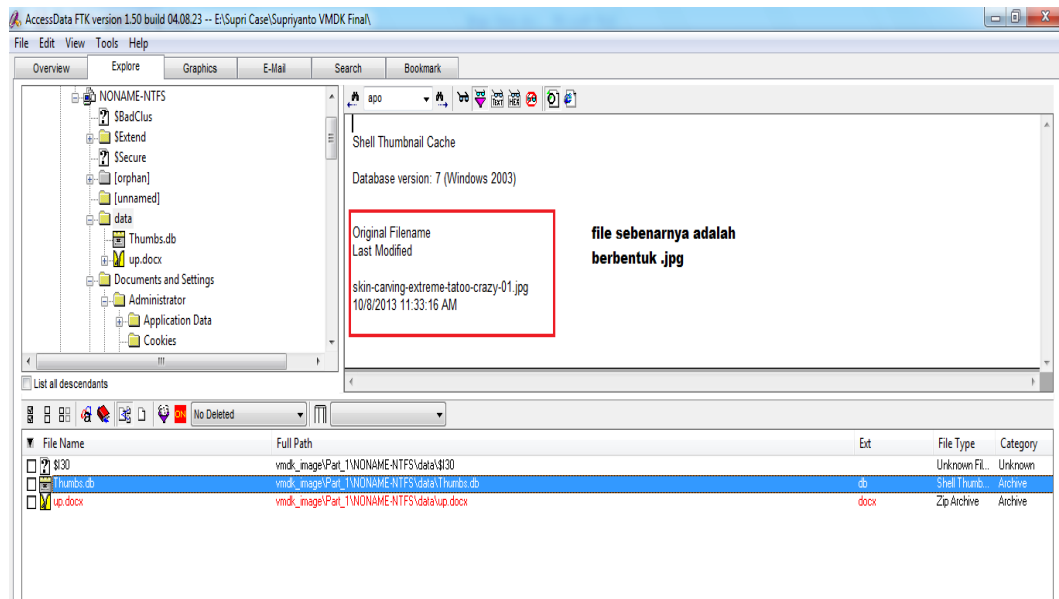
a. Hasil dan Pembahasan pada Graphics

Berdasarkan laporan dari teknisi tentang adanya dua file gambar yang memiliki ukuran berbeda, maka dilakukan penelitian tentang gambar tersebut yang ternyata di dalamnya terdapat file rahasia yang berisi nomor rekening beserta nama pemilik dan bank-nya.

Tercatat disana bahwa nama pemilik rekening adalah Michael Suhendra dengan memiliki rekening di Apocalypse Bank dengan nomor rekening 157 000 83 656 83 656 59 7.



Gambar 4. 39 File gambar yang berisi nomor rekening tersembunyi

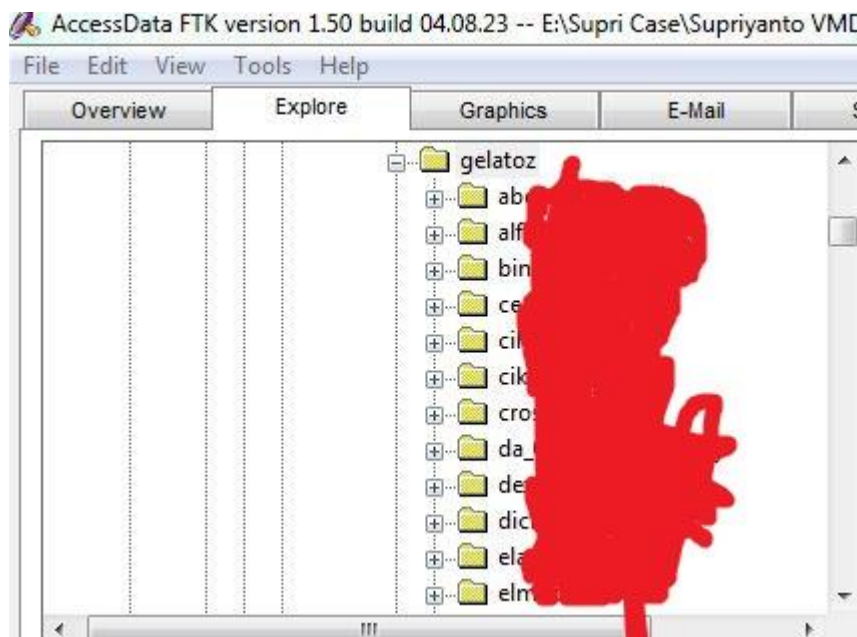


Gambar 4. 42 File jpg yang diganti ekstensi-nya

Dari file docx yang tidak dapat dibuka karena corrupt, examiner menemukan bahwa ternyata file docx tersebut merupakan file jpg yang telah diganti ekstensinya.

b. Hasil dan Pembahasan pada Yahoo Messenger

Akun Yahoo Messenger yang bernama gelatoz memiliki beberapa kontak terlihat pada gambar 4.43 berikut. Folder tersebut dapat dilihat di *Documents and Settings\Administrator\Application Data\Yahoo!\Messenger\gelatoz*.



Gambar 4. 43 Data kontak pada profil gelatoz

Namun sayangnya, *history* percakapan Yahoo Messenger tersebut tidak disimpan di dalam harddisk komputer, melainkan di dalam server Yahoo. Sehingga *examiner* tidak dapat melihat dan meneliti apa yang telah dibicarakan oleh tersangka dengan para lawan *chatting*-nya tersebut.

4.5 Dokumentasi dan Presentasi

Ditemukan barang bukti berupa sebuah netbook di rumah kontrakan Supriyanto, seorang tersangka pengedar obat-obatan terlarang. Kemudian netbook tersebut ditangani secara profesional menurut standar penanganan barang bukti elektronik yang berlaku. Setelah melalui proses akuisisi dan telah dibuat file image dari barang bukti tersebut, ternyata di dalamnya terdapat *virtual machine* yang terpasang. Kemudian *forensic examiner* bekerja sama dengan teknisi komputer untuk menyelidiki *virtual machine* tersebut. Dimana teknisi komputer melakukan *booting* pada file image *virtual machine*, lalu melaporkan hasil temuannya untuk kemudian diselidiki lebih lanjut oleh *forensic examiner*.

Setelah dilakukan analisis pada *virtual machine*, polisi menemukan adanya kecurigaan bahwa tersangka merupakan pengedar obat-obatan terlarang. Namun bukti yang ada belum cukup kuat. *Examiner* menemukan aplikasi Yahoo

Messenger yang terpasang, dan menemukan akun yang bernama “gelatoz” yang pernah terhubung dengan beberapa akun Yahoo lainnya. Tapi sayangnya history percakapan Yahoo Messenger tersebut tidak tersimpan di dalam harddisk komputer. Aplikasi ini dicurigai sebagai alat untuk berkomunikasi dengan sindikat jaringan narkoba.

Dengan adanya dugaan yang kuat tersebut, maka penyidik melakukan kerja sama dengan penyedia layanan *e-mail*, dan bank-bank terkait untuk memblokir aktifitas dari pemilik akun gelatoz, dan pemilik nomor rekening Michael Suhendra.

Examiner juga menemukan gambar-gambar serta video yang melanggar hak-hak perlindungan anak. Selain itu, ditemukan pula *history* pada web browser yang merujuk pada aktifitas internet banking pada beberapa bank berbeda.

Berikut ini adalah dokumentasi dan laporan singkat mengenai barang bukti digital yang ditemukan. Laporan selengkapnya mengenai temuan barang bukti dapat dilihat pada lampiran.

Objective: Untuk menentukan dan memastikan bahwa tersangka terlibat dalam pengedaran obat-obatan terlarang, dan pornografi anak. Juga dilakukan untuk melacak produsen dan jaringan narkoba yang lebih besar

Type Media: VMWare Virtual Machine

Sistem Operasi: Windows XP

Offense: Obat-obatan terlarang, dan pornografi anak.

Case agent: Tom Clancy (Investigator)

Evidence Number: 012345

Chain of Custody: Lihat lampiran

Where examination took place: Laboratorium Komputer Forensik

Tools used: Perlengkapan untuk mengakuisisi hard disk, disk imager, disk examiner, vmware *virtual machine*, perangkat lunak untuk membuat file konfigurasi.

Processing

Access :

Mengulas kembali permintaan layanan dari kasus yang ditangani investigator. Investigator tertarik untuk menemukan semua informasi yang berhubungan dengan pengedaran obat-obat terlarang, dan pornografi anak. Dan seluruh peralatan yang dibutuhkan tersedia di laboratorium komputer forensik.

Acquire:

Konfigurasi *hardware* telah didokumentasi dan duplikat dari hard disk telah dibuat dengan tata cara standar yang telah ditetapkan untuk penanganan barang bukti elektronik, agar tidak merusak maupun mengubah barang bukti asli.

Analyze:

Direktori struktur file, termasuk waktu dan tanggal telah didokumentasi. Pencarian file header dilakukan untuk menemukan seluruh gambar grafik. File image telah diperiksa kembali, dan file-file yang berhubungan dengan kasus pengedaran obat-obat terlarang belum ditemukan, namun dicurigai adanya aktifitas chatting yang mengacu pada transaksi narkoba. Ditemukan pula file-file yang mengacu pada pornografi anak serta history pada browser Mozilla yang dicurigai sebagai alat untuk melakukan internet banking.

Documenting & Reporting:

Investigator telah diberikan sebuah laporan yang menggambarkan temuan dari hasil analisis. Setelah itu investigator memutuskan untuk melakukan wawancara serta kerjasama dengan pihak-pihak terkait untuk meminta keterangan lebih detail mengenai tersangka.

Langkah selanjutnya:

Bekerja sama dengan penyedia layanan Yahoo, untuk mendapatkan history percakapan serta file-file e-mail dari akun Yahoo bernama “gelatoz” yang tersimpan di dalam server Yahoo. Sehingga didapatkan data valid yang nantinya dapat diajukan ke pengadilan sebagai bukti.

Kemudian menyelidiki kasus pelanggaran pelecehan terhadap anak dibawah umur. Lalu melakukan investigasi lebih lanjut mengenai kepemilikan rekening atas nama Michael Suhendra di Apocalypse Bank. Melakukan

penyelidikan terhadap beberapa rekening pada bank lain yang telah diakses melalui komputer tersangka untuk melakukan transaksi *internet banking*, serta hubungannya dengan perdagangan obat-obatan terlarang. Jika memang benar terbukti bersalah, maka dapat dikenakan pasal berlapis yang dapat dilihat pada lampiran.

Presentasi merupakan tahap terakhir dalam proses digital forensik. Dalam melakukan presentasi, cukup menggunakan penjelasan sederhana, dan tidak perlu terlalu menyinggung masalah teknis. Cukup dijelaskan file apa saja yang ada di dalam *virtual machine*, kemudian dijelaskan pula hubungan-nya dengan tindak kriminal yang dilakukan oleh tersangka. Dalam hal ini, dengan melakukan booting image *virtual machine* dapat membantu jalannya presentasi. Sebagai catatan, data serta file yang ditemukan dalam barang bukti digital yang dianalisis bisa meringankan atau memberatkan hukuman bagi tersangka pelaku kejahatan.

4.6 Rangkuman Hasil Analisis

Setelah dilakukan penyelidikan terhadap *virtual machine* secara menyeluruh, baik dengan cara mem-booting *virtual machine* maupun dengan menggunakan *software* FTK, maka dapat disimpulkan beberapa beberapa temuan diantara keduanya. Ada beberapa file *log* maupun file *history* yang tidak tersimpan di dalam harrdisk komputer, melainkan tersimpan di dalam server internet. Seperti contohnya file log dalam Yahoo Messenger. Oleh karena itu, melakukan booting pada *virtual machine* sangat diperlukan guna mencari data-data yang diinginkan.

Dari pembahasan pada sub-bab sebelumnya, penulis juga menemukan adanya perbedaan pada tools yang digunakan. Sebagai contoh, analisis menggunakan FTK dan FTK Imager akan menghasilkan hasil yang berbeda. Kedua *software* tersebut memiliki kekurangan dan kelebihan-nya masing-masing. Disamping itu, keduanya juga memiliki kelemahan yang sama, yaitu tidak maksimal pada tugas *me-recovery data*. Hal tersebut dapat dilihat pada temuan yang telah dirangkum dalam tabel 4.2 dibawah ini.

Tabel 4. 2 Perbandingan FTK dan FTK Imager

Features	FTK Imager	Forensic Toolkit
File (Data) Discovery	●	○
File (Data) Recovery	○	○
Reveal File Contents	●	○
File (Data) Access & Analysis	○	●
Imaging	●	○
MD5	●	●
SHA1	●	●

Keterangan : ● Efektif ○ Kurang Efektif

Dari skenario yang disajikan dalam penelitian diatas, dapat diperoleh hasil bahwa formulir barang bukti dapat bermanfaat sebagai petunjuk dalam memprioritaskan suatu kasus. Sehingga *examiner* tahu kasus mana yang harus dikerjakan lebih dulu. Sehingga, kasus yang sedang ditangani dapat selesai tepat waktu sebelum persidangan dilakukan.

Kemudian kerjasama antara dua personel yang dilengkapi dengan peralatan dan keahlian yang berbeda, dapat menghasilkan hasil yang lebih cepat. Serta dapat mengurangi beban kerja dari *forensic examiner* profesional. Meskipun tanpa bantuan teknisi dan tanpa menggunakan lingkungan virtual, seorang *forensic examiner* profesional tetap dapat menemukan hasil yang sama. Namun, dengan menggunakan metode konvensional dan virtual tersebut, *forensic*

examiner dapat menghemat waktu dan kesempatan menemukan bukti-bukti penting menjadi lebih besar.

Selain itu, dengan menggunakan metode tersebut juga dapat bermanfaat untuk melatih teknisi yang belum berpengalaman agar dapat menjadi lebih mengerti akan bidang komputer forensik, sehingga teknisi dapat mengerti konsep dan prosedur dalam komputer forensik sebelum terjun langsung menjadi professional *forensic examiner*.

Membooting virtual machine juga dapat bermanfaat untuk keperluan presentasi di pengadilan. Sehingga orang awam yang tidak mengerti tentang komputer, dapat melihat bagaimana *virtual machine* bekerja, dan dapat melihat rekonstruksi kejadian bagaimana seorang pelaku kriminal melakukan tindak kejahatan.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian dan analisis yang telah dilakukan oleh *forensic examiner*, maka dapat didapatkan kesimpulan sebagai berikut:

1. Meskipun *virtual machine* sangat identik dengan sistem komputer yang sebenarnya, namun tetap ada beberapa perbedaan struktur file yang harus diwaspadai oleh *forensic examiner*. Salah satunya adalah karakteristik pada *virtual disk* dan cara kerjanya.
2. *Virtual Disk* tidak dapat dianalisis dari file image harddisk fisik. Perlu melakukan export pada virtual disk, selanjutnya membuat file image dari virtual disk tersebut.
3. Sebelum dilakukan analisis menyeluruh, pihak berwajib dapat memanfaatkan teknisi komputer untuk menjalankan *virtual machine*. Ditujukan untuk mencari data-data yang berpotensi dimanfaatkan sebagai alat kejahatan, sehingga dapat meningkatkan efektifitas, dan menghemat waktu yang diperlukan dalam proses analisis oleh *forensic examiner*.
4. *Virtual machine* dapat di-booting untuk memperlihatkan bukti-bukti digital yang ada dihadapan pengadilan, dengan tujuan untuk memberikan keterangan serta untuk mempresentasikan bukti-bukti yg ada di dalam *virtual machine* tersebut.
5. Tidak semua file tersimpan di dalam media penyimpanan komputer, namun dapat juga tersimpan dalam server penyedia layanan. Seperti file log pada Yahoo Messenger. Sehingga tidak dapat dianalisis menggunakan Forensic Toolkit. Oleh karena itu, penyidik perlu melakukan kerja sama dengan penyedia layanan. Sehingga analisis barang bukti digital tetap

dapat dilakukan secara konvensional, karena itu merupakan standar baku dalam penanganan barang bukti digital.

5.2 Saran

Karena keterbatasan yang dimiliki penulis dalam melakukan penelitian ini, maka ada penulis menyarankan beberapa hal untuk keperluan pengembangan penelitian dimasa yang akan datang, yaitu sebagai berikut:

1. Semua cara dan teknik penyelidikan yang dimuat dalam laporan ini, hanya merupakan salah satu dari sekian banyak teknik yang ada. Oleh karena itu, demi perbaikan dan perkembangan dalam penelitian selanjutnya, tidak menutup kemungkinan menggunakan teknik serta perangkat lunak selain yang dimuat dalam penelitian ini, namun tetap dengan menerapkan standar komputer forensik yang sudah ada.

DAFTAR PUSTAKA

- Internet World Stats. (2011). *Usage and Population Statistic*. Retrived October 15, 2012, from <http://www.internetworldstats.com/stats.htm>
- IC3. (2011). Internet Crime Complaint Center. Retrived October 23, 2012, from http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf
- Nardoni, D. (2005). David Nardoni. *Introduction to Computer Forensic*. Retrived November 10, 2012, from <http://www-scf.usc.edu/~itp499cf/Lectures/USC.Computer.Forensics-Computers.and.Networks.pdf>
- US-CERT. (2008). *Computer Forensics*. Retrived November 19, 2012, from <http://www.us-cert.gov/sites/default/files/publications/forensics.pdf>
- Huth, A ., Cebula, J. (2011). *The Basic of Cloud Computing*. United States Computer Emergency Readiness Team
- DFRWS. (2001). *A Road Map for Digital Forensics Research Workshop*. Retrived November 23, 2012, from <http://www.dfrws.org/2001/dfrws-rm-final.pdf>
- Shavers, B. (2008). *Virtual Forensics, A discussion of Virtual Machines Related to Forensics Analysis*. From <http://www.forensicfocus.com/downloads/virtual-machines-forensics-analysis.pdf>
- Conroy, Sean P. (2010). *History of Virtualization*. Retrived October 3, 2012, from <http://www.everythingvm.com/content/history-virtualization>
- Bilal, A. *Plus and Minus of Cloud Computing*. Retrived April 20, 2013, from <http://www.techmaish.com/plus-and-minus-of-cloud-computing>
- Webmaster Indonesia. (2011). *Komputasi Awan (Cloud Computing)*. Retrived 25 August, 2013, from <http://ewawan.com/topics/arti-cloud-computing>
- ICO. (2012). *Guidance on the use of Cloud Computing*. From http://www.ico.org.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Practical_application/cloud_computing_guidance_for_organisations.ashx

- P. Mell and T. Grance, The NIST Definition of Cloud Computing (Draft), Special Publication 800-145 (Draft), National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.
- Bem, D., Huebner, E. (2007). Computer Forensik Analysis in a Virtual Environment. *International Journal of Digital Evidence*, 6(2).
- Praveen. (2011). Analysis of Performance in the Virtual Machines Environment. *International Journal of Advanced Science and Technology*, 32.
- Al Azhar, M N. (2012). *Panduan Praktis Investigasi Komputer*, Jakarta : Salemba Infotek
- Hack, D. (2012). Great Way to write-protect USB flash drive. Retrived January 22, 2013, from <http://www.hackdonor.com/2012/03/great-way-to-write-protect-usb-flash.html>
- Zulfariansyah, M. (2012). *Forensik iPod Touch*. Univesitas Islam Indonesia.
- Williams , P. (2013). *Computer Forensic Form*. Retrived February, 4, 2013, from <http://technoid.net/uni/fit/single-form.pdf>
- National Instruments. (2009). *Virtualization Technology Under the Hood*. Retrived October, 2012, from <http://www.ni.com/white-paper/8709/en>
- VMWare Workstation Documentation. (2012). *Installing and Configuring VMware Tools*. Retrived February, 12, 2013, from <http://www.vmware.com/pdf/vmware-tools-installation-configuration.pdf>
- VMWare .(2007). *VMWare Virtual Networking Concepts*. Palo Alto, USA: VMWare Inc
- Chun, W. (2012). *What is Cloud Computing*. Retrived August 2013 from <https://developers.google.com/appengine/training/intro/whatiscc>
- Cloud Indonesia. Apa itu Cloud Computing. Retrived August 2013 from <http://www.cloudindonesia.or.id/apa-itu-cloud-computing.html>
- Mell, P., Grance T. (2011). *The Definition of Cloud Computing*. National Institute of Standards and Technology.
- Austin, R. (2013). Forensic Procedures Manual version 3.5. Price Software Company. Departement of Information Tecnology. Southern Politechnic State University

- Barrett, D., Kipper, G. (2010). *Virtualization and Forensic, A Digital Forensic Investigator's Guide to Virtual Environments*, Burlington : Elsevier.
- Carvey, H. (2009). *Windows Forensic Analysis, DVD Toolkit 2E*, Burlington : Elsevier
- Forensic Analysis using FTK Imager. Retrieved June 2013 from <http://cse.spsu.edu/raustin2/CourseFiles/forensics/UsingFTK.pdf>
- Analysis using FTK. Retrieved June, 2013 from <http://cse.spsu.edu/raustin2/CourseFiles/forensics/Lab3.pdf>
- Parsonage, H. (2010). *The Meaning of Linkfiles in Forensic Examinations*. Retrieved June, 04, 2013, from <http://computerforensics.parsonage.co.uk/downloads/TheMeaningofLIFE.pdf>
- US Department of Justice . (2004). *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* . Washington: National Institute of Justice
- Craig, J. Philip. (2005). *Computer Forensics Procedures and Methods*. University of Central Florida.
- Access Data. (2004). *User Guide Forensic Toolkit, Find Computer Evidence Quickly and Easily*. Utah, USA : AccessData Corp.
- Horvat, M. (2005). *Disk Cloning*. Sentinel Data Security. From <http://sentinelsecurity.net>
- Hirwani, M., Pan, Y., Stackpole, B., & Johnson, D. *Forensic Acquisition and Analysis of VMWare Virtual Hard Disk*. Rochester Institute of Technology

LAMPIRAN

Created By AccessData® FTK® Imager 3.1.2.0

Case Information:

Acquired using: ADI3.1.2.0

Case Number: 012345

Evidence Number: 2013

Unique description: vmdk image file

Examiner: Danar Mustofa

Notes:

Information for E:\Image VMDK final\vmdk_image:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 5,874

Heads: 255

Sectors per Track: 56

Bytes per Sector: 512

Sector Count: 83,886,080

[Physical Drive Information]

Drive Interface Type: buslogic

[Image]

Image Type: VMWare Virtual Disk

Source data size: 40960 MB

Sector count: 83886080

[Computed Hashes]

MD5 checksum: 83a6777031afb8a456d812849db6416c

SHA1 checksum: daf897ff65b0922a7bb79bffc96f63e765fc9ea4

Image Information:

Acquisition started: Thu Oct 10 07:55:31 2013

Acquisition finished: Thu Oct 10 08:21:54 2013

Segment list:

E:\Image VMDK final\vmrk_image.001
E:\Image VMDK final\vmrk_image.002
E:\Image VMDK final\vmrk_image.003
E:\Image VMDK final\vmrk_image.004
E:\Image VMDK final\vmrk_image.005
E:\Image VMDK final\vmrk_image.006
E:\Image VMDK final\vmrk_image.007
E:\Image VMDK final\vmrk_image.008
E:\Image VMDK final\vmrk_image.009
E:\Image VMDK final\vmrk_image.010
E:\Image VMDK final\vmrk_image.011
E:\Image VMDK final\vmrk_image.012
E:\Image VMDK final\vmrk_image.013
E:\Image VMDK final\vmrk_image.014
E:\Image VMDK final\vmrk_image.015
E:\Image VMDK final\vmrk_image.016
E:\Image VMDK final\vmrk_image.017
E:\Image VMDK final\vmrk_image.018
E:\Image VMDK final\vmrk_image.019
E:\Image VMDK final\vmrk_image.020
E:\Image VMDK final\vmrk_image.021
E:\Image VMDK final\vmrk_image.022
E:\Image VMDK final\vmrk_image.023
E:\Image VMDK final\vmrk_image.024
E:\Image VMDK final\vmrk_image.025
E:\Image VMDK final\vmrk_image.026
E:\Image VMDK final\vmrk_image.027

E:\Image VMDK final\vmdk_image.028

Image Verification Results:

Verification started: Thu Oct 10 08:21:58 2013

Verification finished: Thu Oct 10 08:42:19 2013

MD5 checksum: 83a6777031afb8a456d812849db6416c : verified

SHA1 checksum: daf897ff65b0922a7bb79bffc96f63e765fc9ea4 : verified

DATA FILE FORENSIC LABORATORY

REPORT OF MEDIA ANALYSIS

MEMORANDUM FOR : Kepolisian Republik Indonesia
Investigator Tom Clancy
Jakarta Barat, Indonesia 01234

SUBJECT : Laporan Forensik Analisis Media
SUBJECT: SUPRIYANTO
Case Number: 012345

1. Status: Closed.

2. Summary of Findings:

- Ditemukannya sebuah aplikasi *virtual machine* VMWare yang didalamnya terpasang sebuah sistem operasi Microsoft Windows XP.
- Ditemukannya 1 buah file gambar yang dicurigai sebagai media untuk menyimpan pesan rahasia.
- Ditemukannya beberapa file gambar berisi konten pornografi anak.
- History pada web browser yang digunakan untuk mengakses internet banking.

3. Items Analyzed:

TAG NUMBER:	ITEM DESCRIPTION:
012345	One Generic laptop, Serial # 123456789

4. Action Taken:

- Melakukan *back up* terhadap keseluruhan isi hard drive.
- Melakukan imaging pada virtual disk.
- Menyerahkan salinan file image kepada teknisi untuk analisis sederhana.
- Meneliti lebih lanjut tentang hasil temuan yang dilakukan oleh teknisi.

5. Details of Findings:

Berikut ini adalah detail hasil temuan yang ditemukan oleh kami, beserta tim.

- 1) Terdapat Virtual Machine VMWare yang terpasang dengan virtual disk berformat VMDK.
- 2) Sistem operasi di dalam VMWare merupakan Windows XP SP 1
- 3) Tiga buah file gambar pada folder *C:\Administrator\My Document\Download*. Mengindikasikan adanya pornografi anak.
- 4) Dua buah file gambar pada folder *C:\Documents and Settings\Administrator\My Documents\test*. Memiliki size yang berbeda.
- 5) Dua buah gambar pornografi pada folder *C:\Documents and Settings\Administrator\My Documents\My Pictures*
- 6) Satu buah file dokumen corrupt pada folder *C:\data*.
- 7) Sebuah File document yang berisi inisial dan nama-nama narkoba pada folder *C:\data*.
- 8) Aplikasi Yahoo Messenger yang terpasang. Dengan akun Yahoo bernama gelatoz yang pernah log-in melalui *virtual machine* tersebut
- 9) Aplikasi web browser Mozilla Firefox yang terpasang.
- 10) Aplikasi Simple File Shredder yang terpasang.
- 11) History browser yang mengacu pada pemilik akun e-mail Yahoo bernama gelatoz.
- 12) History pada browser Mozilla Firefox yang mengindikasikan pemilik komputer kerap melakukan internet banking pada beberapa bank berbeda.

6. Glossary:

- Shortcut File: Ikon yang dibuat sebagai jalan pintas untuk mengakses suatu program, maupun file.
- Virtual Machine : Mesin virtual
- Registry : Editor untuk database yang menyimpan segala informasi mengenai komputer
- Log: Catatan yang merekam segala aktifitas pada suatu aplikasi yang dijalankan.

- Steganography: Seni menyembunyikan pesan.

7. Items Provided:

Sebagai dokumentasi dari laporan *hard* copy maka disertakan pula compact disk (CD) dengan salinan digital pada laporan ini.

Released by_____

Danar Mustofa

Computer Forensic Examiner

PASAL – PASAL TERKAIT

Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Pasal 27

- (1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan.
- (2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.

Pasal 45

- (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Undang-undang Nomor 35 Tahun 2009 Tentang Narkotika

Pasal 73

Penyidikan, penuntutan, dan pemeriksaan di sidang pengadilan terhadap penyalahgunaan dan peredaran gelap Narkotika dan Prekursor Narkotika dilakukan berdasarkan peraturan perundang-undangan, kecuali ditentukan lain dalam Undang-Undang ini.

Pasal 74

- (1) Perkara penyalahgunaan dan peredaran gelap Narkotika dan Prekursor Narkotika, termasuk perkara yang didahulukan dari perkara lain untuk diajukan ke pengadilan guna penyelesaian secepatnya.
- (2) Proses pemeriksaan perkara tindak pidana Narkotika dan tindak pidana Prekursor Narkotika pada tingkat banding, tingkat kasasi, peninjauan kembali, dan eksekusi pidana mati, serta proses pemberian grasi, pelaksanaannya harus dipercepat sesuai dengan peraturan perundang-undangan.

Undang-undang Nomor 23 Tahun 2003 Tentang Perlindungan Anak

Pasal 78

Setiap orang yang mengetahui dan sengaja membiarkan anak dalam situasi darurat sebagaimana dimaksud dalam Pasal 60, anak yang berhadapan dengan hukum, anak dari kelompok minoritas dan terisolasi, anak yang tereksplorasi secara ekonomi dan/atau seksual, anak yang diperdagangkan, anak yang menjadi korban penyalahgunaan narkotika, alkohol, psikotropika, dan zat adiktif lainnya (napza), anak korban penculikan, anak korban perdagangan, atau anak korban kekerasan sebagaimana dimaksud dalam Pasal 59, padahal anak tersebut memerlukan pertolongan dan harus dibantu, dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 100.000.000,00 (seratus juta rupiah).

Pasal 79

Setiap orang yang melakukan pengangkatan anak yang bertentangan dengan ketentuan sebagaimana dimaksud dalam Pasal 39 ayat (1), ayat (2), dan ayat (4), dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 100.000.000,00 (seratus juta rupiah).

Pasal 80

(1) Setiap orang yang melakukan kekejaman, kekerasan atau ancaman kekerasan, atau penganiayaan terhadap anak, dipidana dengan pidana penjara paling lama 3 (tiga) tahun 6 (enam) bulan dan/atau denda paling banyak Rp 72.000.000,00 (tujuh puluh dua juta rupiah).

(2) Dalam hal anak sebagaimana dimaksud dalam ayat (1) luka berat, maka pelaku dipidana dengan pidana penjara paling lama 5 (lima) tahun dan/atau denda paling banyak Rp 100.000.000,00 (seratus juta rupiah).

(3) Dalam hal anak sebagaimana dimaksud dalam ayat (2) mati, maka pelaku dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 200.000.000,00 (dua ratus juta rupiah).

(4) Pidana ditambah sepertiga dari ketentuan sebagaimana dimaksud dalam ayat (1), ayat (2), dan ayat

(3) apabila yang melakukan penganiayaan tersebut orang tuanya.

Pasal 81

(1) Setiap orang yang dengan sengaja melakukan kekerasan atau ancaman kekerasan memaksa anak melakukan persetubuhan dengannya atau dengan orang lain, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun dan paling singkat 3 (tiga) tahun dan denda paling banyak Rp 300.000.000,00 (tiga ratus juta rupiah) dan paling sedikit Rp 60.000.000,00 (enam puluh juta rupiah).

(2) Ketentuan pidana sebagaimana dimaksud dalam ayat (1) berlaku pula bagi setiap orang yang dengan sengaja melakukan tipu muslihat, serangkaian kebohongan, atau membujuk anak melakukan persetubuhan dengannya atau dengan orang lain.

Pasal 82

Setiap orang yang dengan sengaja melakukan kekerasan atau ancaman kekerasan, memaksa, melakukan tipu muslihat, serangkaian kebohongan, atau membujuk anak untuk melakukan atau membiarkan dilakukan perbuatan cabul, dipidana dengan pidana penjara paling lama 15 (lima belas) tahun dan paling singkat 3 (tiga) tahun dan denda paling banyak Rp 300.000.000,00 (tiga ratus juta rupiah) dan paling sedikit Rp 60.000.000,00 (enam puluh juta rupiah).

Pasal 88

Setiap orang yang mengeksploitasi ekonomi atau seksual anak dengan maksud untuk menguntungkan diri sendiri atau orang lain, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp 200.000.000,00 (dua ratus juta rupiah).