BELAJAR OTODIDAK WINDOWS FORENSIC

Untuk semua versi Windows

Prof. Dr. Sarjon Defit, S.Kom, MSc.
Efvy Zamidra Zam, M.Kom., MPM

BELAJAR OTODIDAK WINDOWS FORENSIC

Sanksi Pelanggaran Pasal 113
Undang-Undang Nomor 28 Tahun 2014
tentang Hak Cipta

1. Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000 (seratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).
3. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
4. Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

BELAJAR OTODIDAK WINDOWS FORENSIC

Prof. Dr. Sarjon Defit, S.Kom, MSc.
dan
Efvy Zamidra Zam, M.Kom., MPM

PENERBIT PT ELEX MEDIA KOMPUTINDO
KOMPAS GRAMEDIA

Belajar Otodidak Windows Forensic

Prof. Dr. Sarjon Defit, S.Kom, MSc. dan Efvy Zamidra Zam, M.Kom., MPM

Diterbitkan pertama kali oleh
Penerbit PT Elex Media Komputindo
Kelompok Gramedia, Anggota IKAPI, Jakarta 2018

nadhia@elexmedia.id

ID 718051011

ISBN 978-602-04-7667-4 (Printed)

978-602-04-7668-1Digital)

Dicetak oleh Percetakan PT Gramedia, Jakarta

Isi di luar tanggung jawab percetakan

DAFTAR ISI

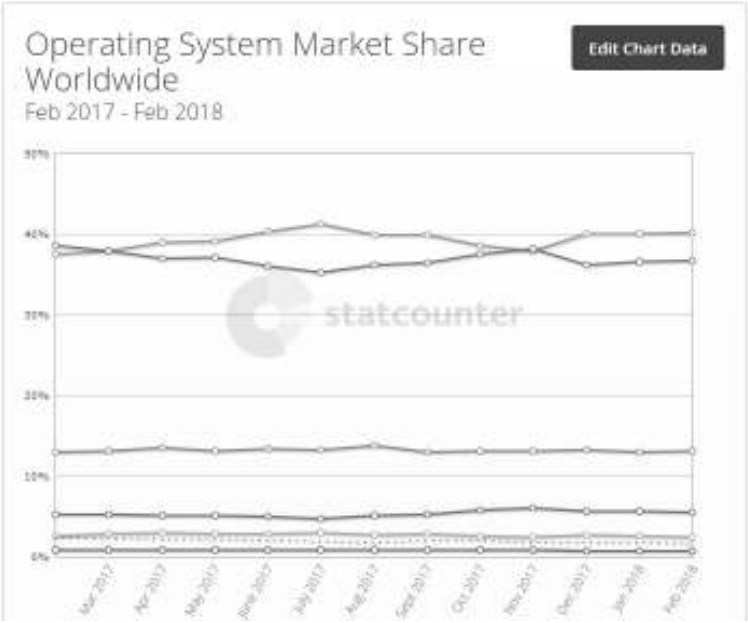
BAB 1
WINDOWS FORENSIC
Selayang Pandang

Sebelum menelaah lebih jauh, apa saja yang dapat dilakukan dengan Windows Forensic, ada baiknya terlebih dahulu kita mengenal istilah lainnya yang berkaitan. Pertama yang akan dibahas adalah Digital Forensic, yaitu identifikasi dan pengumpulan bukti digital dari media apapun, sambil tetap menjaga integritasnya. Dalam digital forensic media yang digunakan bisa berupa komputer/laptop, hp/smartphone, CCTV (video), handycam, gambar dan sebagainya. Selanjutnya, dipersempit lagi dengan istilah Computer Forensic, yaitu proses pembuktian tindak kejahatan yang menggunakan komputer, atau dikenal dengan istilah *computer crime*. Komputer forensik adalah aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan atau penyaringan, dan dokumentasi bukti komputer dalam kejahatan komputer.

Penggunaan *handphone*, PDA, dan banyak perangkat *mobile* saat ini juga digolongkan sebagai *Computer Forensic*. Hal ini dikenal dengan istilah *Embedded Computer Systems* karena perangkat seperti telepon bergerak (ponsel), *personal digital assistant* (PDA), *smart card*, dan perangkat-perangkat lain yang tidak dapat disebut komputer tapi memiliki sistem komputer dalam sistem kerjanya, dapat digolongkan dalam kategori ini karena bukti-bukti digitalnya dapat tersimpan di sini.

Dalam pemakaian komputer atau laptop saat ini salah satu sistem operasi yang banyak digunakan di dunia adalah sistem operasi Windows. Bisa dikatakan Windows Forensic merupakan bagian dari Computer Forensic maupun Digital Forensic yang fokusnya pada sistem operasi Windows. Hal itulah yang menjadi pokok pembahasan utama dalam buku ini. Walau demikian, apa yang dijelaskan pada Windows Forensic ini secara teoritis bisa diterapkan pada sistem operasi lainnya, hanya saja metode dan alat bantu (*tools*) yang digunakan berbeda.

Berdasarkan data dari http://gs.statcounter.com/os-market-share diketahui bahwa *market share* penggunaan sistem operasi Windows adalah 36,58%.

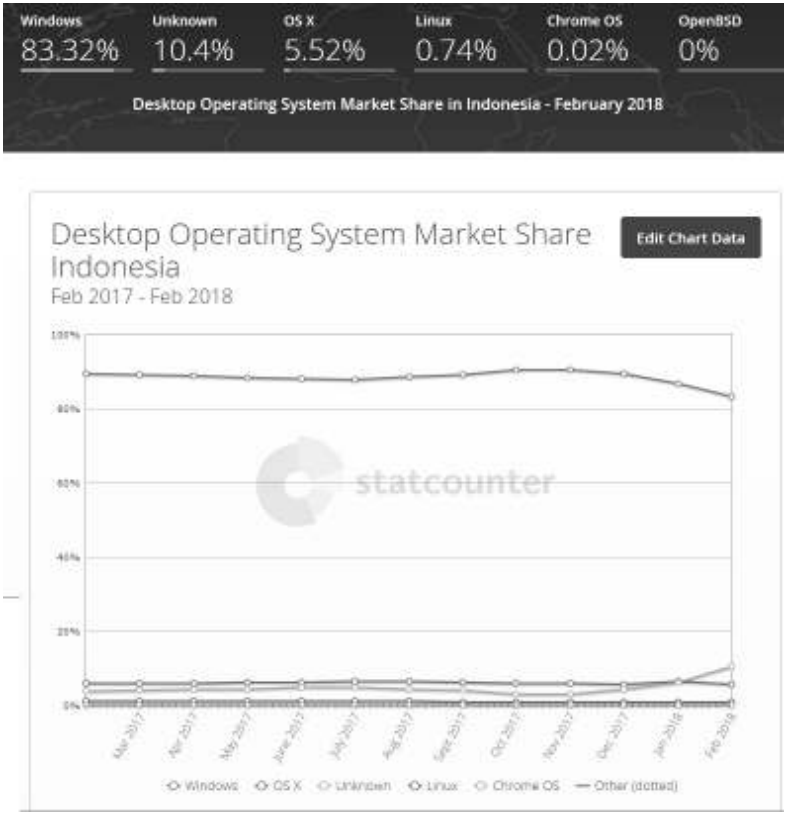


Gambar 1.1 Market share sistem operasi

Sedangkan, versi Windows yang paling banyak digunakan hingga Februari 2018 adalah Windows 10 (43,54%) yang disusul oleh Windows 7 (41,55%).

Gambar 1.2 Market share sistem operasi Windows

Masih dari http://gs.statcounter.com, di Indonesia sendiri pengguna komputer desktop paling banyak (83,32%) didominasi oleh Windows.



Gambar 1.3 Market share sistem operasi di Indonesia

Apabila dirunut secara *historis*, penggunaan komputer untuk kepentingan pembuktian hukum (*pro justice*) telah ada sejak lama. Sehubungan dengan keberadaan *computer evidence*, telah dilakukan berbagai konferensi, antara lain:

1. Tahun 1993; diselenggarakan konferensi internasional pertama berkenaan bukti komputer (*computer evidence*)

2. Tahun 1995; dibentuk International Organization Computer Evidence (IOCE)
3. Tahun 1997; G8 dan IOCE secara independen mengembangkan standar berkenaan bukti komputer.
4. Tahun 1998; banyak organisasi lain yang ikut berpartisipasi, seperti SWG-DE, ACPO, FCG, ENSFI, dan INTERPOL
5. Tahun 1999; ACPO, IOCE, FCG, dan ENSFI membahas mengenai standar komputer forensik di Eropa.

Selanjutnya, yang perlu kita ketahui adalah orang yang melakukan kegiatan Computer Forensic atau Windows Forensic disebut sebagai investigator atau analis forensik.

Data

Sebelum memasuki bab berikutnya yang akan menjelaskan langkah-langkah detail untuk melakukan Windows Forensic, terdapat beberapa hal mendasar yang perlu kita ketahui terlebih dahulu supaya mempermudah pemahaman kita dalam melakukan Windows Forensic. Hal yang pertama dan utama adalah data; karena memang hal inilah yang menjadi target operasi dari sebuah kegiatan Windows Forensic.

Proses pengumpulan dan analisa data dari sumber daya komputer, berasal dari:

- Sistem komputer
- Jaringan komputer
- Jalur komunikasi

- Media penyimpanan
- Aplikasi komputer

Sebelum melakukan Windows Forensic ada baiknya Anda mengenal tiga jenis data, beserta karaktertistiknya:

Active Data

- Data yang bisa digunakan oleh user maupun sistem operasi, user juga dapat "melihat" dan menggunakannya
- File dan folder yang tampak di Windows Explorer
- Berada di ruang yang dialokasikan
- Dapat diambil dengan cara menyalin file

Latent Data

- Data yang telah dihapus atau sebagian sudah ditimpa
- Tidak terlihat melalui sistem operasi
- Tidak muncul dalam Windows Explorer
- Bitstream atau forensik image diperlukan untuk memperoleh data ini

Archival Data

- Disebut juga Backups
- Biasanya disimpan di:
    - External harddrives
    - DVDs
    - *Cloud backup services* seperti Iron Mountain atau Symform

Selanjutnya, data dibedakan lagi menjadi dua berdasarkan kondisinya apakah *persisten* atau *volatile*. Terdapat dua jenis data dasar yang dikumpulkan dalam komputer forensik: data persisten (*nonvolatile*) dan *volatile*. Data yang persisten adalah data yang tersimpan pada hard drive lokal (*harddisk*) dan dipelihara saat komputer dimatikan. Data volatil disimpan dalam memori utama yang akan hilang saat komputer kehilangan daya atau dimatikan. Data tersebut berada pada *register*, *cache*, dan *random access memory* (RAM).

Yang tergolong data *nonvolatile* adalah sebagai berikut:

1. File konfigurasi yang digunakan dalam menyimpan informasi berkenaan setting sistem operasi, dan program aplikasi; misalnya: resolusi layar, printer setting, *connection setting*, dan sebagainya.
2. *Log file* yang berisi catatan aktivitas dari sistem operasi, bahkan menyimpan pula aktivitas spesifik dari program aplikasi. Metode penyimpanannya beragam, mungkin disimpan pada file teks atau database; dan pada beberapa kasus, bisa saja aktivitas disimpan pada beberapa log file yang berbeda:
    a. **System event** merupakan kegiatan operasional sistem operasi, misalnya sewaktu sistem *startup* atau proses *shutdown*. Kegagalan atau keberhasilan aktivitas yang dilakukan ini akan dicatat.
    b. **Audit record** berisi serangkaian informasi yang berhubungan dengan sekuritas, misalnya berhasil atau gagalnya proses autentikasi.
    c. **Application events** berisi serangkaian kegiatan yang dilakukan oleh program aplikasi sewaktu aplikasi

dijalankan, kemudian ditutup (*terminated*), bahkan kegagalan aplikasi.

d. **Command history**, berupa catatan perintah-perintah sistem operasi yang di-*request* oleh user.

e. **Recently accessed file**, sistem operasi mencatat file-file dan program-program aplikasi yang diakses baru-baru ini.

3. *Application file*, berupa program yang bisa di-eksekusi yang saling teritengrasi seperti file script pemrograman, file konfigurasi, grafik, audio, dan ikon.

4. *Data file* digunakan untuk menyimpan informasi dari program aplikasi. File semacam ini, umumnya dikenal oleh pengguna dan sering digunakan untuk menyimpan pekerjaan user.

5. *Swap file*, digunakan untuk memperluas kemampuan memori komputer yang difungsikan sebagai memori sementara/temporer.

6. *Dump file*, yaitu file yang menyimpan isi dari memori komputer.

7. *Hibernation file*, yaitu file yang diciptakan untuk menjelaskan sistem saat ini dan akan di-*restore* saat sistem dinyalakan kembali (*turn on*).

8. *Temporary file*, yaitu file yang diciptakan saat instalasi sistem operasi, aplikasi, proses *update*, dan bahkan diciptakan seraya program aplikasi berjalan. Umumnya, file tersebut dihapus segera setelah software aplikasi ditutup. Meskipun demikian, bisa saja karena hal-hal tertentu, file tersebut masih tersimpan.

Yang tergolong data *volatile* adalah sebagai berikut:

1. *Slack space*
2. *Free space*
3. *Network configuration*
4. *Network connection*
5. *Running process*
6. *Open file*
7. *Login session*
8. *Operating system time* (waktu pada sistem operasi)

Juga terdapat hubungan antara data dengan kondisi shutdown sebuah komputer:

Sleep - data masih tersimpan di RAM

- Power masih menyala
- Dokumen hilang jika power mati

Hibernate - RAM di-copy ke dalam file Hiberfil.sys

- Power off
- Dokumen tidak hilang

Hybrid Sleep

- Default untuk desktop Windows 7
- Meletakkan dokumen yang terbuka dan program di disk kemudian menyimpannya di RAM agar segera bisa dijalankan
- Dokumen tidak hilang meskipun power mati

Gambar 1.4 Menu shutdown Windows 10 dan Windows 7

Metode Windows Forensic

Salah satu metode yang dulu sering digunakan untuk mengumpulkan informasi pada komputer forensik adalah dengan mematikan komputer dan mencabut harddisk-nya. Padahal, dalam beberapa kasus, informasi yang paling berharga kadang justru ditemukan dalam memori komputer yang artinya hanya bisa diakses ketika komputer dalam kondisi aktif. Belum lagi dalam melakukan proses forensik komputer tersebut harus selalu menyala, seperti sebuah server yang dikenal dengan istilah *live analysis*.

Kebanyakan informasi yang dikumpulkan ketika komputer atau laptop yang masih hidup adalah informasi yang sifatnya *volatil*, yaitu informasi yang hilang ketika komputer dimatikan. Informasi volatil ini biasanya ada di dalam RAM. Dalam buku ini akan dibahas teknik forensik baik yang *live forensic* maupun dengan mengambil image sebuah media penyimpanan dan juga memori. Sebab, dengan melakukan *live forensic* itulah kita dapat mengumpulkan informasi volatil dari sistem yang *live*. Sehingga kita bisa mendapatkan gambaran keseluruhan mengenai kondisi sistem.

TENTANG PENULIS

Prof. Dr. Sarjon Defit, S.Kom, MSc. Lahir di Padang Sibusuk tanggal 07 Agustus 1970. Lulus S1 di Program Studi Manajemen Informatika Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK"YPTK") Padang tahun 1993. Lulus S2 di Program Studi Master of Science in Computer Science Universiti Teknologi Malaysia Johor Bahru tahun 1996 dan lulus S3 di Program Studi Doctor of Philosophy in Computer Science Universiti Teknologi Malaysia Johor Bahru tahun 2003.

Saat ini adalah Dosen tetap pada Magister Teknik Informatika Fakultas Ilmu Komputer Universitas Putra Indonesia "YPTK" Padang dan menjabat sebagai Rektor. Telah menulis di berbagai Jurnal Nasional dan Internasional bereputasi terindeks dan juga sebagai pembicara pada berbagai seminar baik nasional maupun internasional. Bidang penelitian adalah bidang Data Mining, Big Data dan Artificial Intelligence.

Efvy Zamidra Zam, M.Kom., MPM. Lahir di Kerinci, 28 Januari 1982. Saat ini berprofesi sebagai salah satu tenaga pengajar di Akademi Manajemen dan Informatika Depati Parbo (AMIK) Depati Parbo-Sungai Penuh, Kerinci. Menamatkan Pasca Sarjana dari Universitas Putra Indonesia "YPTK" Padang. Telah menulis berbagai Jurnal, artikel dan buku bertemakan IT.

Penulis dapat dihubungi melalui email:

efvy.zam@gmail.com

Catatan:

Untuk melakukan pemesanan buku, hubungi
Layanan Langsung PT Elex Media Komputindo:
Gramedia Direct
Jl. Palmerah Barat No. 29-37, Jakarta 10270
Telemarketing/CS: 021-53650110/111 ext: 3901/3902/3292/3427