ANALISIS FORENSIK KOMPUTER PADA TIMESTAMPS SISTEM BERKAS NTFS

Nugroho Budhisantosa
Fakultas Ilmu Komputer Universitas Esa Unggul Jakarta
Jln. Arjuna Utara Tol Tomang-Kebon Jeruk Jakarta 11560
Nugroho.budhisantosa@esaunggul.ac.id

Abstract

For covering the tracks of cyber-crime purposes, the perpetrators might use anti-forensic techniques to modified timestamps easily in the NTFS file system. This paper describes how the knowledge of computer forensics is simply utilize wimc utility which is the default internal utility of Microsoft Windows operating system can be used to determine the authenticity of digital evidence through observation files on a 6 digit microsecond of timestamps.

***Keywords** : forensic, crime, system*

Abstrak

Dalam menutupi jejak kejahatan siber, pelaku kejahatan menggunakan teknik anti forensik dapat melakukan rekayasa pada penanda waktu dari sistem berkas NTFS dengan mudah.Tulisan ini memaparkan bagaimana pengetahuan forensik komputer secara sederhana memanfaatkan utilitas wimc yang merupakan utilitas bawaan dari sistem operasi *Microsoft Windows* dapat digunakan untuk mengetahui keaslian barang bukti berkas digital melalui pengamatan pada 6 digit mikrodetik dari penanda waktu.

Kata kunci : forensik, kejahatan, sistem

Pendahuluan

Barang bukti digital adalah informasi yang tersimpan di dalam media penyimpanan perangkat elektronik di dalam bentuk berkas-berkas digital yang digunakan untuk keperluan melakukan suatu kejahatan serta barang-barang yang didapatkan dari sebuah kejahatan. Secara fisik, barang bukti digital tersimpan di dalam media penyimpanan dalam bit-bit informasi yang tidak kasat mata sehingga memerlukan proses pengolahan menjadi informasi yang kasat mata.

Barang bukti digital dianggap sah dan dapat diajukan ke persidangan jika informasi yang tercantum di dalamnya dapat diakses, dijamin keutuhannya, dan dapat dipertanggungjawabkan. Untuk keperluan ini diperlukan prosedur forensik komputer berupa pengumpulan, akuisisi, pemulihan, penyimpanan/pemeliharaan, dan pemeriksaan barang bukti digital dengan cara yang dapat dipertanggung jawabkan.

Timestamp atau penanda waktu adalah salah satu bagian yang tidak terpisahkan di dalam investigasi barang bukti digital.Sedemikian pentingnya peran penanda waktu ini sehingga pada prosedur pemeliharaan barang bukti digital, perlu juga diperhatikan agar tidak terjadi perubahan pada penanda waktu ini.

Berpasangan dengan kegiatan Forensik komputer pada satu sisi, hadir pula anti komputer forensik pada sisi lainnya yaitu suatu kegiatan kontra investigasi digital yang bertujuan untuk melakukan penghapusan jejak-jejak

kejahatan yang ada di dalam barang bukti digital termasuk di dalamnya penghapusan jejak penanda waktu kejahatan oleh pelaku kejahatan siber.

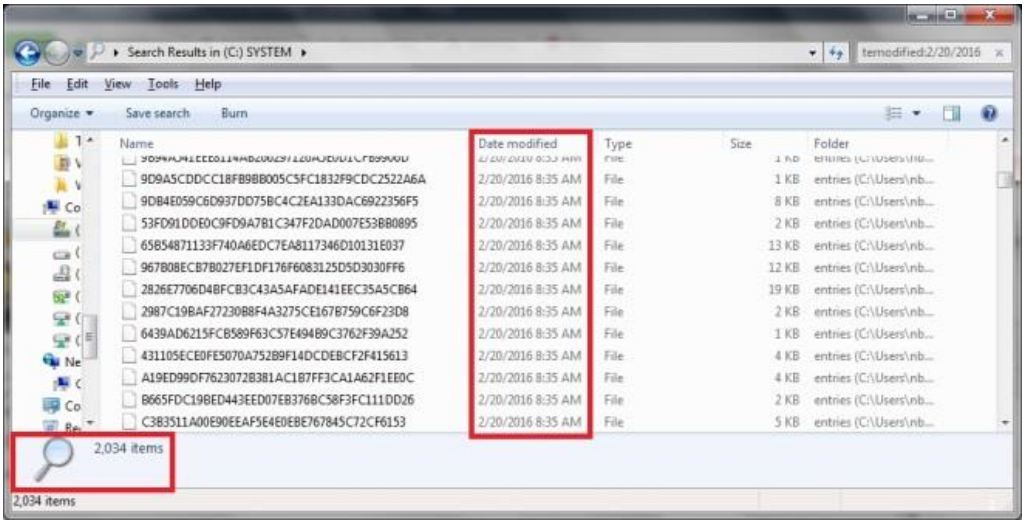
Manfaat

1. Mempelajari cara kerja sistem berkas NTFS di dalam pengelolaam penanda waktu
2. Memberikan referensi pada pihak-pihak yang tertarik untuk mendalami investigasi forensik komputer

Forensik Komputer adalah kata serapan dari bahasa Inggris yaitu *Computer Forensics* dimana kata *Forensics* sendiri berasal dari kata *Forensis* yang di dalam Bahasa latin berarti *belonging to the forum* yang di dalam istilah hukum dapat diartikan sebagai *pertaining to the courts* yang berarti membawa ke pengadilan. Secara terminologi istilah Forensik Komputer sendiri lebih diartikan sebagai membawa barang bukti digital ke pengadilan guna keperluan peneggakan hukum, bukan sekedar membawa komputer secara fisik ke persidangan.

Penanda waktu di dalam sistem berkas komputer adalah waktu saat suatu even dicatat oleh komputer. Di dalam investigasi forensik komputer, penanda waktu digunakan untuk mengetahui waktu dari barang bukti berkas digital dibuat, dimodifikasi, dan terakhir kalinya mengalami pengaksesan. Penanda waktu ini harus dipelihara keasliannya dengan hati-hati dan dicatat di dalam riwayat barang bukti atau *chain of custody*.

Ketika barang bukti kejahatan yang berupa komputer dengan sistem operasi Windows 7 secara ceroboh mengabaikan prosedur pemelihataan dinyalakan, ribuan berkas di dalam media penyimpanannya dapat mengalami perubahan pada penanda waktunya yang menyebabkan seluruh berkas digital di dalam media penyimpanannya tidak lagi dapat digunakan sebagai barang bukti karena sudah terjadi perubahan atasnya atau tercemar.

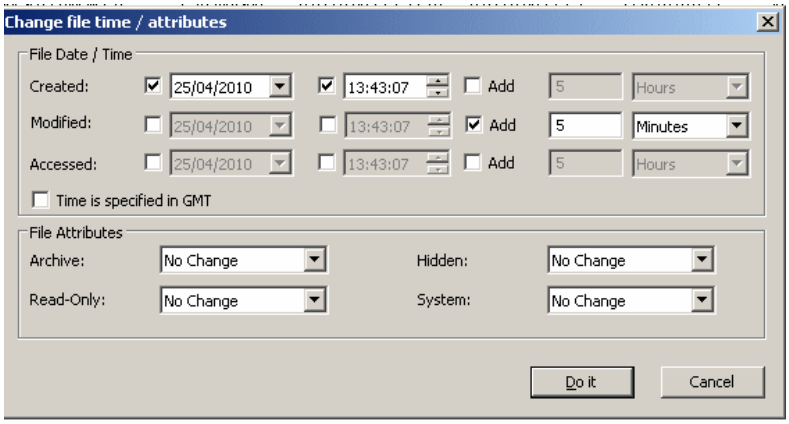


Gambar 1
Ribuan berkas dapat mengalami perubahan penanda waktu ketika komputer dengan sistem operasi Windows 7 dinyalakan

Memahami rapuhnya barang bukti digital, seseorang pelaku kejahatan dapat saja menanam file/berkas di dalamnya yang telah dimodifikasi penanda waktunya 1 bulan ke depan ketika pelaku kejahatan ini mengetahui bahwa minggu ini petugas kepolisian akan menahannya berikut menyita unit komputernya.

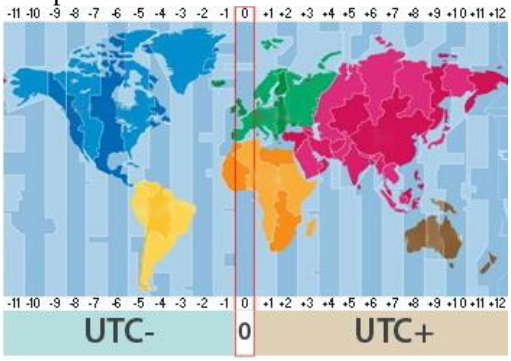
Beberapa perangkat lunak perubah penanda waktu sepertiAttributeMagic, Moo0 TimeStamp, BulkFileChanger (BFC), eXpress TimeStamp, dan sejenisnya dengan mudah dapat digunakan untuk keperluan ini. Menggunakan modus ini pelaku kejahatan akan dapat berkata dipersidangan kelak bahwa telah terjadi perubahan pada barang bukti pada 1 bulan setelah barang bukti disita petugas melalui berkas-berkas yang telah ditanam sebelumnya sebagai alibinya.

Sistem berkas NTFS melakukan pencatatan waktu dalam format 64-bit yang mewakili jumlah interval 100-nanosecond. Perhitungan ini dihitung sejak jam 00:00, 1 Januari 1601 megikuti standar waktu *Coordinated Universal Time* (*UTC*) yang merupakan waktu matahari di longitudinal 0° bumi atau waktu di Greenwich Mean Time (GMT).



Gambar 2
Tampilan aplikasi pengubah penanda waktu

Dipilihnya penggunaan standar UTC, menyebabkan sistem pencatatan sistem berkas NTFS tidak lagi terpengaruh oleh perubahan zona waktu seperti yang terjadi pada oleh Sistem berkas FAT yang menyimpan nilai waktu berdasarkan waktu lokal komputer. Sistem operasi mengenali waktu lokal komputer berdasarkan zona lokasi yang dimasukkan oleh pengguna komputer ketika sistem operasi diinstal pada komputer. Jika informasi zona waktu untuk Jakarta adalah UTC +7, maka komputer akan mencatat waktu lokal komputer berdasarkan waktu di Greenwich Mean Time (GMT) ditambahkan (+) nilai 7.



Gambar 3
Longitudinal 0°

Di dalam sistem operasi Microsoft Windows, format 64-bit ini akan diubah ke dalam format yang dapat dibaca oleh

manusia oleh *System call File Time To System Time ()*, ke dalam bentuk tahun, bulan, hari, jam, menit, detik dan milidetik.

Satu teknik umum yang digunakan di dalam pembuktian keaslian barang bukti digital adalah penggunaan sidik jari digital atau *digital hash*. *Digital hash*merupakan pentransformasian string dari karakter-karakter didalam barang bukti ke dalam bentuk nilai yang lebih ringkas.

Seperti halnya sidik jari pada manusia yang berbeda-beda, berkas-berkas digital yang berbeda juga akan memiliki *digital hash*yang berbeda. Didalam persidangan, pembela terdakwa dapat meminta seorang saksi ahli digital forensik untuk membandingkan *digital hash* dari berkas-berkas digital yang ada di dalam barang bukti asli dengan *digital hash* dari berkas-berkas yang diajukan jaksa penuntut untuk membuktikan keaslian barang bukti digital yang dibawa di dalam persidangan dengan menggunakan metode pembuatan *digital hashing* yang sama. Berapa metoda hashing yang umum digunakan di persidangan adalah MD5, SHA1, dan SHA2.

Selain dapat mengetahui informasi penanda waktu berkas melalui utilitas*property*, Sistem operasi Microsoft Windows juga memiliki perintah utilitas internal yaitu*Windows Management Instrumentation Command-line* (*WMIC*) yang dapat digunakan untuk mengetahui informasi penanda waktu berkas secara lebih mendetail.

Utilitas wmic memberikan informasi detail penanda waktu dalam format yyyymmddHHMMSS.mmmmmmsUUU dimana:

- **Yyyy** merupakan empat digit tahun (0000 sampai 9999).
- **mm** merupakan dua digit bullan (01 sampai 12).
- **dd** merupakan dua digit tanggal (01 sampai 31).
- **HH** merupakan dua digit jam yang menggunakan format 24-jam-an (00 sampai 23).
- **MM** merupakan dua digit menit di dalam jam (00 sampai 59).
- **SS** merupakan dua digit detik di dalam menit (00 sampai 59).
- **mmmmmm** merupakan 6 digit angka mikrodetik di dalam detik (000000 sampai 999999)

UUU merupakan tiga digit zona waktu yang diekpresikan dalam hitungan perbedaan menit terhadap GMT atau UTC

Metode Penelitian

Analisis forensik penanda waktu pada sistem berkas NTFS pada tulisan ini dilakukan pada berkas grafis b.jpg yang merupakan salinan dari berkas asli a.jpg. Pada berkas b.jpg ini akan dilakukan modifikasi penanda waktu menggunakan aplikasi perangkat lunak AttributeMagic Free 2.4

Perangkat lunak AttributeMagic Free 2.4 adalah perangkat lunak buatan elwinsoft.com yang didistribusikan secara bebas untuk di Internet untuk digunakan oleh publik.

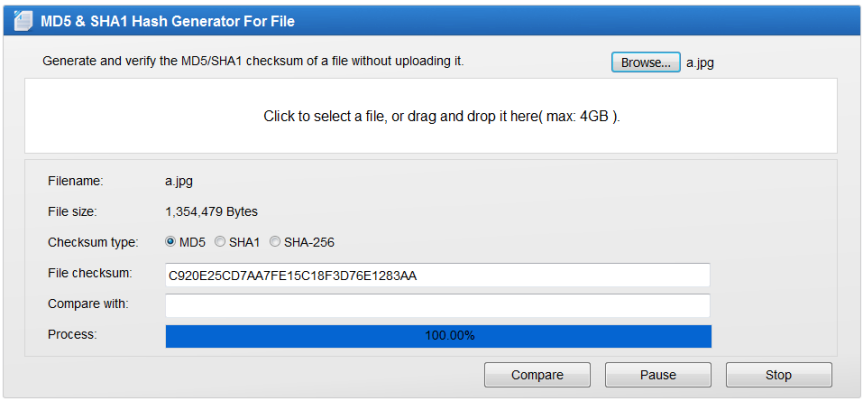
Secara antar muka, aplikasi AttributeMagic memiliki kesamaan dengan aplikasi Moo0 TimeStamp, BulkFIleChanger, dan eXpress TimeStamp yang dapat melakukan perubahan catatan waktu dari Created, Modified, dan Accessed pada tanggal, jam, menit, hingga detik dari berkas.

Pada berkas a.jpg dan berkas b.jpg akan dilakukan identifikasi digital hashing menggunakan metoda MD5 dan pengambilan informasi penanda waktunya menggunakan ultilitas *wmic*.

Hasil dan Pembahasan

Pengujian hashing MD5 yang dilakukan pada berkas a.jpg menghasilkan nilai M1:

C920E25CD7AA7FE15C18F3D76E1283 AA

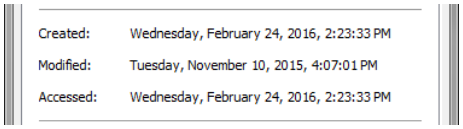


Gambar 4
Aplikasi Online MD5 Hash Generator & SHA1 Hash Generator

Identifikasi penanda waktu pada berkas a.jpg yang merupakan berkas asli dapat diperoleh menggunakan utilitas *property* dengan cara melakukan klik kanan pada *mouse* komputer.

Menggunakan utilitas *property*, berkas a.jpg yang telah dipersiapkan tersebut memiliki atribut penanda waktu seperti pada gambar 6 di bawah.

Gambar 5
Berkas a.jpg



Gambar 6
Properti dari berkas a.jpg

Perintah *wmic* dengan *switchget creationdate*, *get lastmodified* dan *get lastaccessed*yang digunakan untuk mendapatkan informasi waktu pembuatan, waktu modifikasi dan waktu pengaksesan terakhir dioperasikan pada file a.jpg melalui mode *command line* untuk menghasilkan data penanda waktu berikut:

```
wmic datafile where name="d:\\temp\\wmic\\a.jpg" get creationdate
CreationDate
20160224142333.138183+420
```

```
wmic datafile where name="d:\\temp\\wmic\\a.jpg" get lastmodified
LastModified
20151110160701.491550+420
```

```
wmic datafile where name="d:\\temp\\wmic\\a.jpg" get lastaccessed
LastAccessed
20160224142333.138183+420
```

Dari data yang diperoleh menggunakan utilitas wmic dapat diperoleh informasi detail berikut:

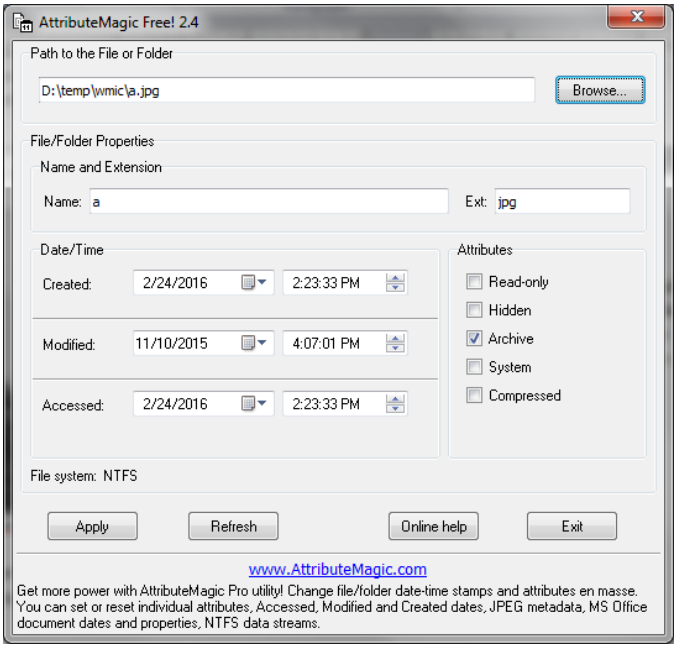
Berkas a.jpg	Created	Modified	Accessed
yyyy (tahun)	2016	2015	2016
Mm (bulan)	02 (Feb.)	11 (Nov.)	02 (Feb.)
dd (tanggal)	24	10	24
HH (jam)	14	16	14
MM (menit)	23	07	23
ss (detik)	33	01	33
mmmmmm (milidetik)	138183	491550	138183
UUU (UTC)	+420 = +7	+420 = +7	+420 = +7

Tabel 1
Hasil bacaan WMIC berkas a.jp

Setelah penanda waktu dan digital hashing dari berkas diperoleh maka penanda waktu berkas a.jpg diubah dengan menggunakan aplikasi AttributeMagic.

Secara antar muka, aplikasi AttributeMagic memiliki kesamaan dengan aplikasi Moo0 TimeStamp, BulkFIleChanger, dan eXpress TimeStamp yang dapat melakukan perubahan catatan waktu dari Created, Modified, dan Accessed pada tanggal, jam, menit, hingga detik dari berkas.

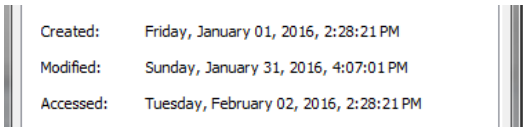
Gambar 6
Berkas a.jpg



Gambar 7
Tampilan antarmuka AttributeMagic

Hasil Pengamatan

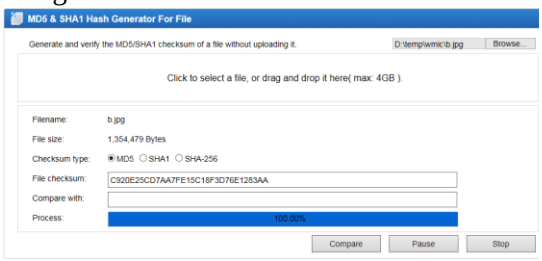
Menggunakan aplikasi Attribute Magic 2.4, pada berkas a.jpg dilakukan modifikasi penanda waktu menjadi berikut:



Gambar 8
Penanda waktu berkas b.jpg

Setelah dilakukan modifikasi pada penanda waktu maka berkas tersebut disimpan menggunakan nama b.jpg.

Identifikasi MD5 dan wimc pada berkas b.jpg yang kemudian dilakukan menghasilkan informasi berikut:



Gambar 9
Nilai MD5 dari b.jpg

M2C920E25CD7AA7FE15C18F3D76E12
83AA

Perintah *wmic* dengan *switchget creationdate, get lastmodified* dan *get lastaccessed* dapat dioperasikan pada file b.jpg melalui mode *command line* untuk menghasilkan data penanda waktu berikut:

wmic datafile where name="d:\\temp\\wmic\\a.jpg" get creationdate
CreationDate
20160101142821.000000+420

wmic datafile where name="d:\\temp\\wmic\\a.jpg" get lastmodified
LastModified
20160131160701.000000+420

wmic datafile where name="d:\\temp\\wmic\\a.jpg" get lastaccessed
LastAccessed
20160202142821.000000+420

Dari data yang diperoleh menggunakan utilitas wmic dapat diperoleh informasi detail berikut:

Berkas a.jpg	Created	Modified	Accessed
yyyy (tahun)	2016	2015	2016
mm (bulan)	01 (Jan.)	01 (Jan.)	02 (Feb.)
dd (tanggal)	1	31	2
HH (jam)	14	16	14
MM (menit)	28	07	28
ss (detik)	21	01	21
mmmmmm (milidetik)	000000	000000	000000
UUU (UTC)	+420 = +7	+420 = +7	+420 = +7

Tabel 2: hasil bacaan WMIC berkas b.jp

Analisa

Tidak terdapat perubahan pada nilai *hash* pada berkas M1 dan M2 yang diambil dari berkas a.jpg dan b.jpg dimana keduanya memiliki nilai yang sama

Nilai MD5 Sebelum modifikasi (M1)
M1:
C920E25CD7AA7FE15C18F3D76E1283
AA

Nilai MD5 Setelah modifikasi (M2)
M2 :
C920E25CD7AA7FE15C18F3D76E1283
AA

Tidak terjadinya perubahan pada nilai *hash* di atas disebabkan karena algoritma nilai MD5 memang tidak untuk mengakomodir pentransformasian *string* pada karakter

dari atribut berkas. Algoritma yang sama juga dilakukan pada pengambilan nilai hashSHA1, dan SHA2.

Yang menarik dari analisa di atas adalah bahwa analisa penanda waktu yang menggunakan utilitas wimc menunjukkan 6 digit angka baik pada waktu*Created*, waktu*Modified*, dan waktu*Accessed* pada berkas yang mengalami modifikasi pada penanda waktunya menggunakan perangkat lunak AttributeMagic Free 2.4yaitu berkas b.jpgmenunjukkan angka 000000 ada bilangan penunjuk mikrodetiknya seperti ditunjukkan pada tabel 2 di bawah.

Berkas a.jpg	Created	Modified	Accessed
yyyy (tahun)	2016	2015	2016
mm (bulan)	01 (Jan.)	01 (Jan.)	02 (Feb.)
dd (tanggal)	1	31	2
HH (jam)	14	16	14
MM (menit)	28	07	28
Ss (detik)	21	01	21
Mmmmmm (milidetik)	000000	000000	000000
UUU (UTC)	+420 = +7	+420 = +7	+420 = +7

Tabel 2
Hasil bacaan WMIC berkas b.jp

Hal menarik lainnya adalah parameter zona waktu yang tidak mengalami perubahan mengikuti zona waktu local dari komputer yaitu +420.

Kesimpulan

Dari Analisa forensik keaslian penanda waktu pada sistem berkas NTFS di atas dapat disimpulkan bahwa: Analisa keaslian penanda waktu pada sistem berkas NTFS tidak dapat dilakukan pada nilai *hash* MD5 karena tidak terjadi perubahan pada nilai *hashing*-nya pada berkas yang telah dimodifikasi menggunakan perangkat lunak AttributeMagic Free 2.4. Analisa penanda waktu menggunakan utilitas wimc dapat dilakukan untuk melakukan pengujian penanda waktu yaitu pada 6 digit mikrodetik pada berkas yang telah dimodifikasi yang menghasilkan angka 000000. Perangkat lunak perubah penanda waktu AttributeMagic Free 2.4 yang tidak mengakomodir perubahan pada atribut mikrodetik dari berkas adalah penyebab6 digit mikrodetik pada berkas yang telah dimodifikasi menunjukkan nilai default 000000 hal ini disebabkan karena perangkat lunak AttributeMagic Free 2.4 tidak mencoba melakukan pembacaan pada 6 digit mikrodetik dari waktu lokal komputer.

Daftar Pustaka

https://msdn.microsoft.com/en-us/library/windows/desktop/ms724290%28v=vs.85%29.aspx

http://searchsqlserver.techtarget.com/definition/hashing

http://onlinemd5.com/