MD5 (Message-Digest algortihm 5)

Yama Fresdian Dwi Saputro
fds.yama@gmail.com

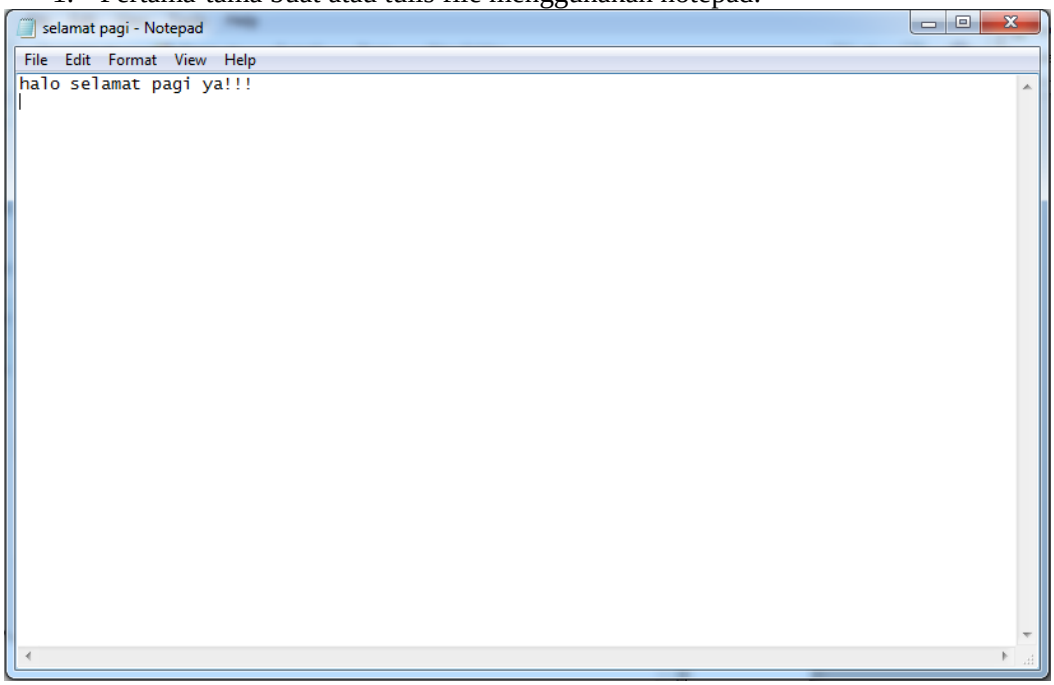
Pendahuluan

MD5 atau Message-Digest algortihm 5 adalah fungsi hash kriptografik. Algoritma ini terutama digunakan untuk melakukan pemeriksaan integritas file dalam berbagai situasi. Dalam ilmu kriptografi, MD5 adalah salah satu algoritma hash yang paling populer. Hash atau hashing sendiri adalah proses perubahan suatu data menjadi data lain dengan panjang tertentu, sedemikian sehingga data itu tidak dapat dipulihkan kembali. Teknik ini biasa digunakan dalam enkripsi data, misalnya untuk menyimpan password agar tidak ada yang dapat mengetahuinya meskipun dia dapat melihat hash dari password itu.

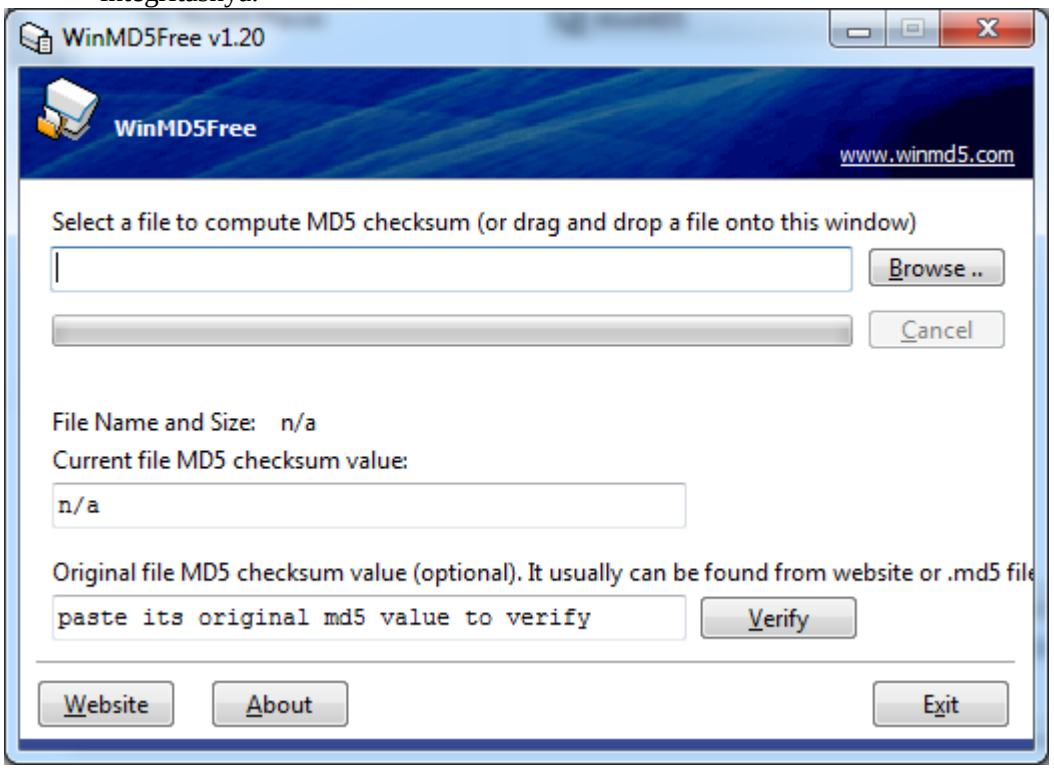
Sebenarnya istilah “enkripsi” tidaklah tepat karena jika data itu dienkripsi, pastilah ada cara untuk dekripsi untuk mendapatkan kembali data yang disembunyikan itu. Sedangkan hash, seperti disebutkan di atas, adalah proses yang irreversibel (tidak ada istilah de-hash atau un-hash). Artinya data yang sudah di-hash tidak dapat dipulihkan kembali menjadi seperti data awal. Algoritma hash MD5 sendiri menerima input berupa data dengan panjang bebas, dan menghasilkan output heksadesimal sepanjang 32 karakter. Jadi, seberapapun panjang data input, output yang dihasilkan akan selalu sepanjang 32 karakter. Perubahan sedikit saja di input akan mengubah output dengan drastis.

Langkah Percobaan Md5

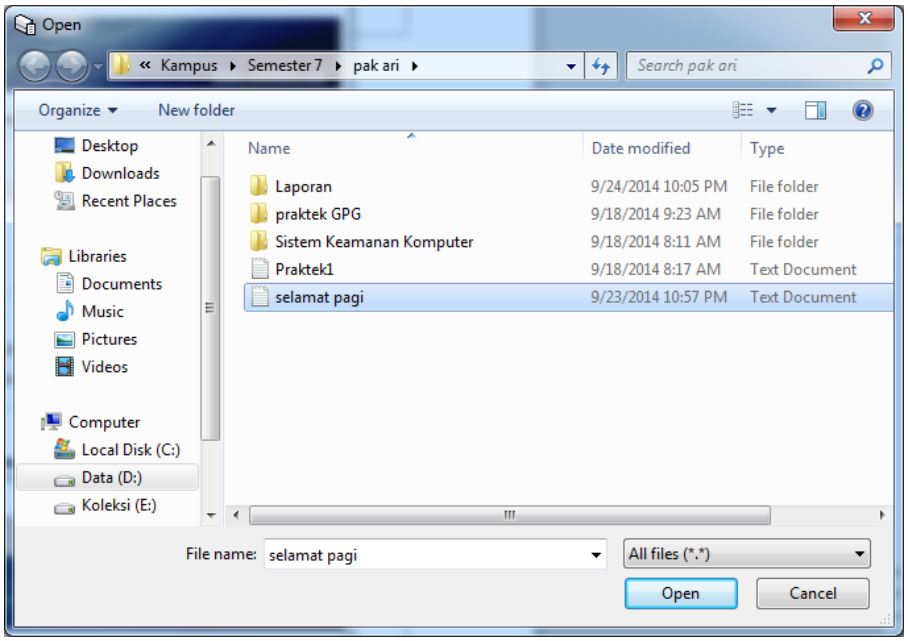
1. Pertama-tama buat atau tulis file menggunakan notepad.



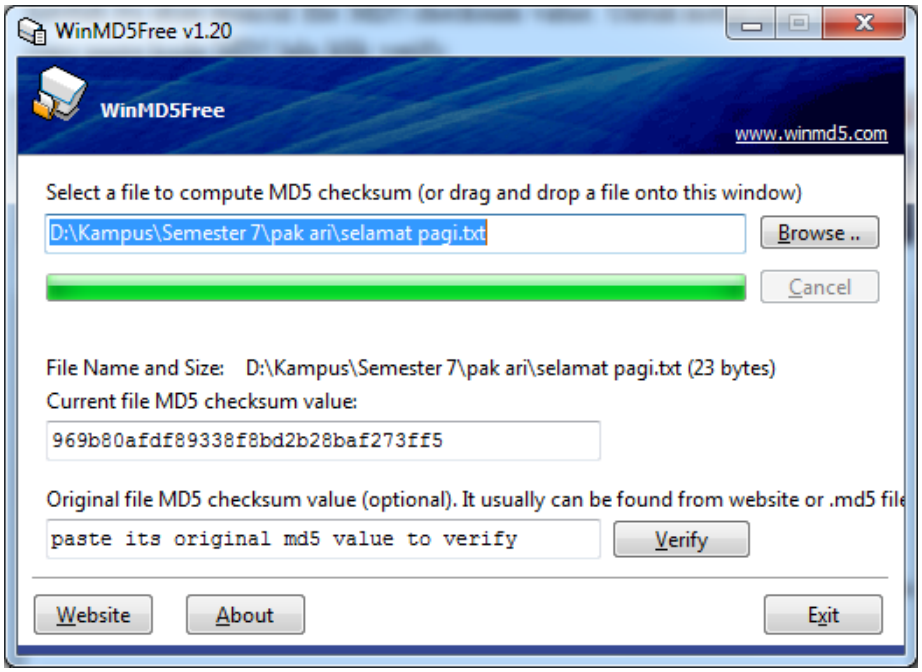
2. Buka software WinMD5Free. Klik browse untuk memasukkan file yang akan di cek integritasnya.



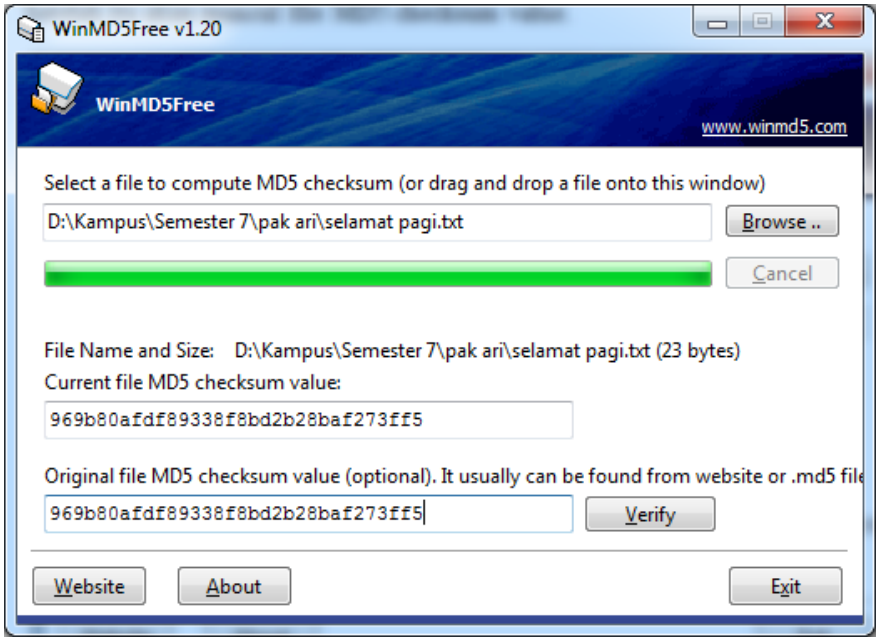
3. Kemudian pilih file yang akan dicek.



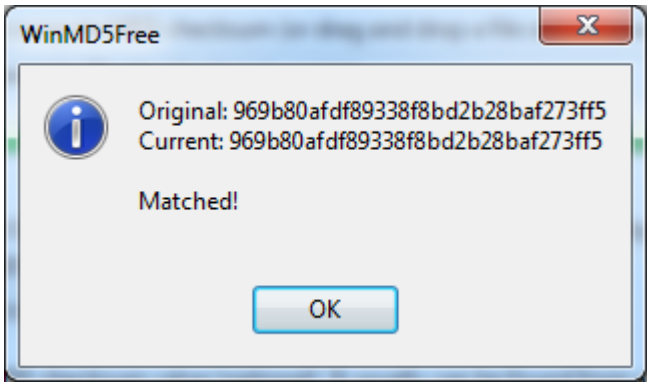
4. Setelah itu akan muncul file MD5 checksum value.



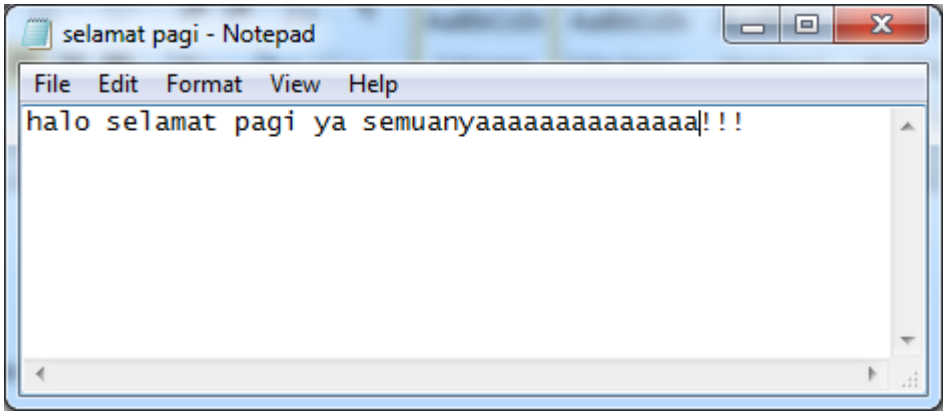
5. Untuk melakukan verifikasi file copy paste kode MD5 lalu masukkan ke kotak dialog "*Original file MD5…*" kemudian klik verify untuk mengecek.



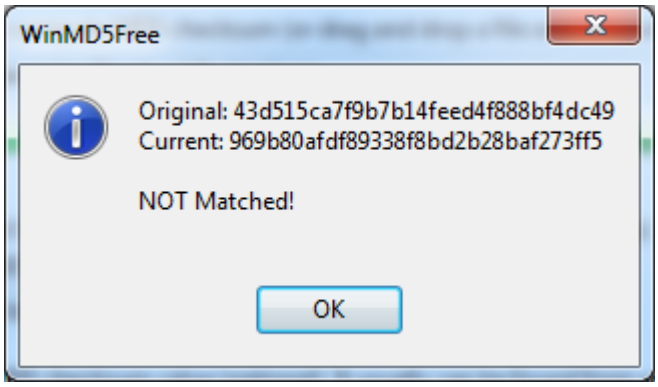
6. Jika file benar maka akan muncul tulisan “Matched”



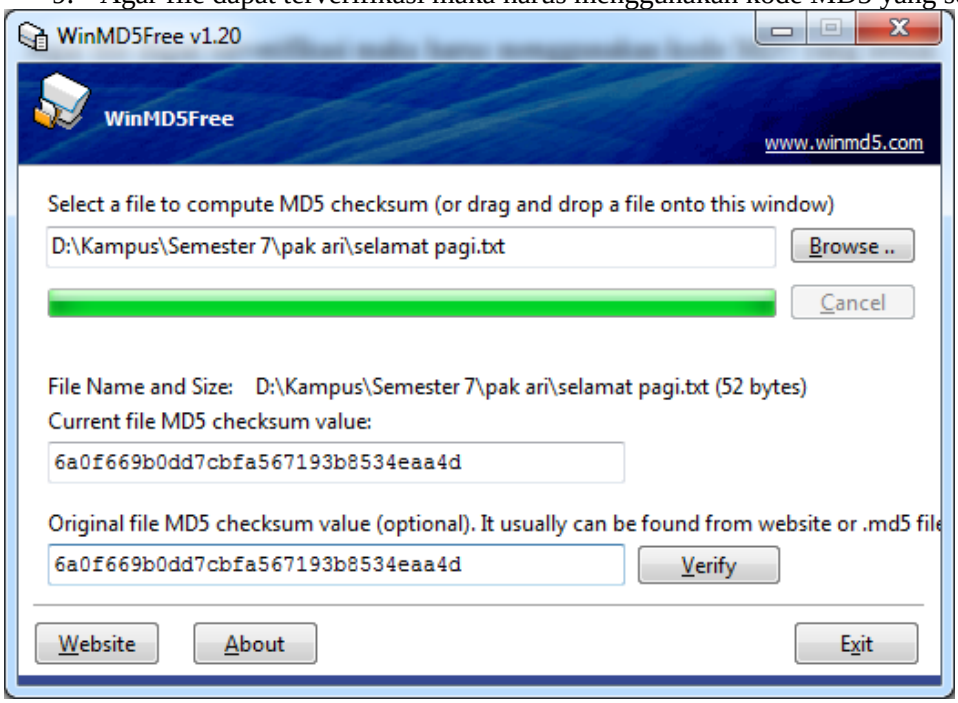
7. Jika file dimodifikasi maka kode MD5 akan berbeda.

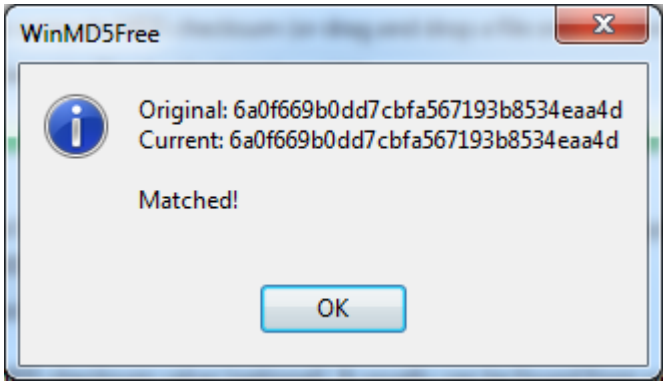


8. Apabila diverifikasi dengan kode MD5 yang berbeda maka akan muncul tulisan “NOT MATCHED”



9. Agar file dapat terverifikasi maka harus menggunakan kode MD5 yang sesuai.





Analisa Data

Pada hasil data yang didapat saat praktikum Algoritma hash MD5 menghasilkan output heksadesimal sepanjang 32 karakter. Jadi, seberapapun panjang data input, output yang dihasilkan akan selalu sepanjang 32 karakter. Perubahan sedikit saja di input akan mengubah output dengan drastis.

Selain itu juga terlihat bahwa perubahan input sedikit saja akan mengubah output secara keseluruhan. Dengan sifat ini, algoritma ini dapat dimanfaatkan untuk mengecek integritas atau

keutuhan suatu data. Misalnya pada saat melakukan download file dengan ukuran besar akan lebih mudah untuk memastikan integritas atau keutuhan data yang disertai MD5 checksum untuk mengetahui apakah file yang diterima sempurna atau mengalami kerusakan pada saat proses pengiriman., karena kerusakan paling kecil saja akan mengubah MD5 checksum dari file itu.

Kesimpulan

1. MD5 merupakan fungsi hash kriptografik yang digunakan untuk memeriksa integritas file.
2. Seberapapun panjang data input pada MD5, output yang dihasilkan akan selalu sepanjang 32 karakter. Perubahan sedikit saja di input akan mengubah output dengan drastis.
3. Perubahan input sedikit saja pada MD5 akan mengubah output secara keseluruhan.

Biografi Penulis

Yama Fresdian Dwi Saputro. Menyelesaikan Program D4 Telekomunikasi di Politeknik Negeri Semarang.