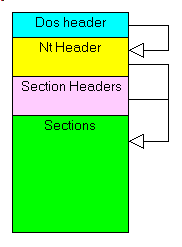
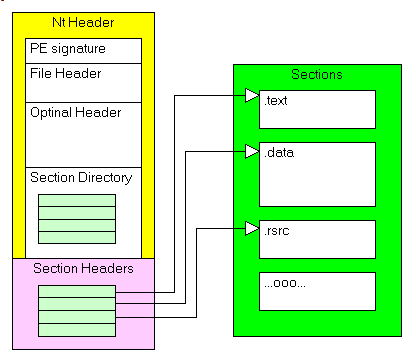
# Mengekstrak Kode dari Program Terkompilasi



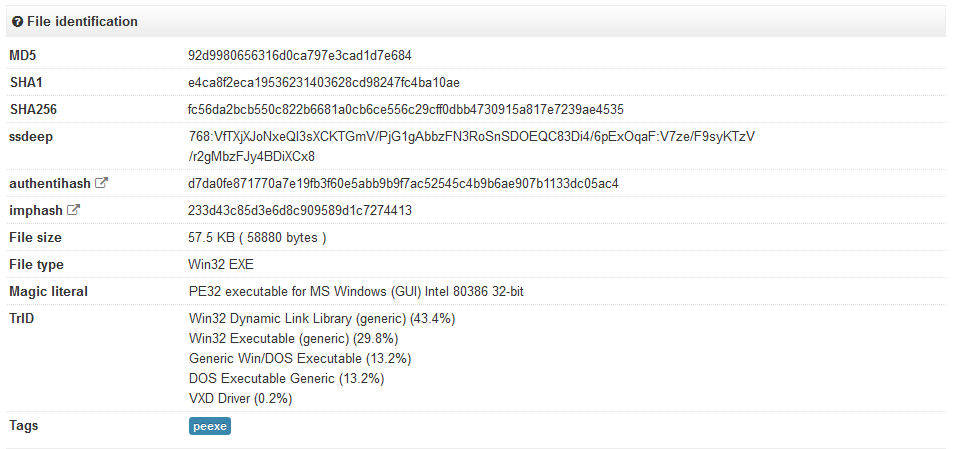
Program (file dengan ekstensi .exe) atau *library* (file dengan ekstensi .dll atau .ocx) yang sudah terkompilasi untuk sistem operasi Microsoft Windows dikemas dalam format file *Portable Executable* (PE). File tersebut memiliki susunan seperti ditunjukan pada gambar no 1.

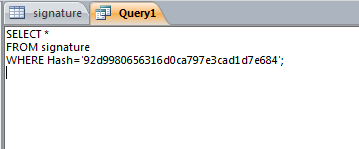
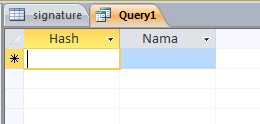


Lebih jelasnya, file PE terbagi menjadi tiga atau lebih *sections* sesuai dengan kebutuhan masing-masing program/library (ditunjukan pada gambar 2). Secara umum, file PE mengandung *text section* yang berisi kode-kode yang sudah berbentuk bahasa mesin, *data section* yang berisi library-library yang digunakan serta disediakan, dan *rsrc section* yang berisi *resource-resource* yang digunakan oleh program/library seperti kursor, atau ikon.

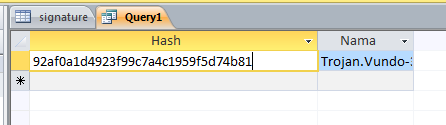
Dari *section-section* yang terdapat pada file PE, *section text* dan *section data* adalah dua bagian yang sangat penting untuk analisis statis sistem pendeteksi *malware*. Hal tersebut disebabkan kedua *section* ini mengandung kode serta *library-library* yang secara kasat mata menentukan apakah program tersebut adalah *malware*. Pada kasus antivirus ClamAV, antivirus ini tidak menganalisis keseluruhan program yang dicurigai sebagai *malware*, melainkan memecah belah program tersebut lalu memeriksa *section text* dan *section data* pada program tersebut.

Hal ini terlihat pada contoh kasus Trojan Vundo pada antivirus ClamAV. Trojan Vundo memiliki hash file seperti ditunjukan pada gambar 3. Namun, pada database ClamAV, tidak ditemukan virus dengan hash 92d9980656316d0ca797e3cad1d7e684 seperti ditunjukan pada gambar 4.

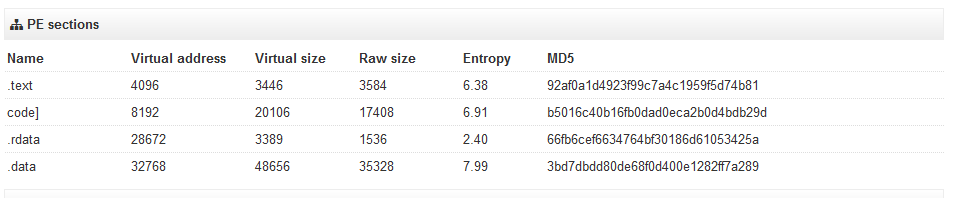


Hal tersebut bukan dikarenakan ClamAV tidak mengenal Trojan Vundo karena sebenarnya ClamAV mengenal Trojan Vundo seperti yang ditunjukan pada gambar 5.



Namun, ClamAV mengenal Trojan Vundo dengan *hash* md5 92af0a1d4923f99c7a4c1959f5d74b81. Jika dilihat lebih teliti, hash tersebut adalah *hash* dari *section text* yang terdapat pada Trojan Vundo seperti yang ditunjukan pada gambar 6.



Cara analisis ini memberikan dua keuntungan bagi sistem pendeteksi malware. Pertama, proses perhitungan *checksum* lebih cepat karena perhitungan tidak dilakukan ke seluruh program beserta *resource* yang dibawanya, melainkan hanya dilakukan terhadap kode dan *reference* terhadap *library* yang digunakan oleh program. Kedua, sistem pendeteksi *malware* lebih kebal terhadap *teknik-teknik* penyamaran yang dilakukan oleh pembuat *malware* dengan cara mengubah *resource* internal pada program sehingga *checksum* keseluruhan program akan berubah.