Nama : Muhammad Fachrurroji Ilham Saputra

Nim : 09011181322025

Analisa malware

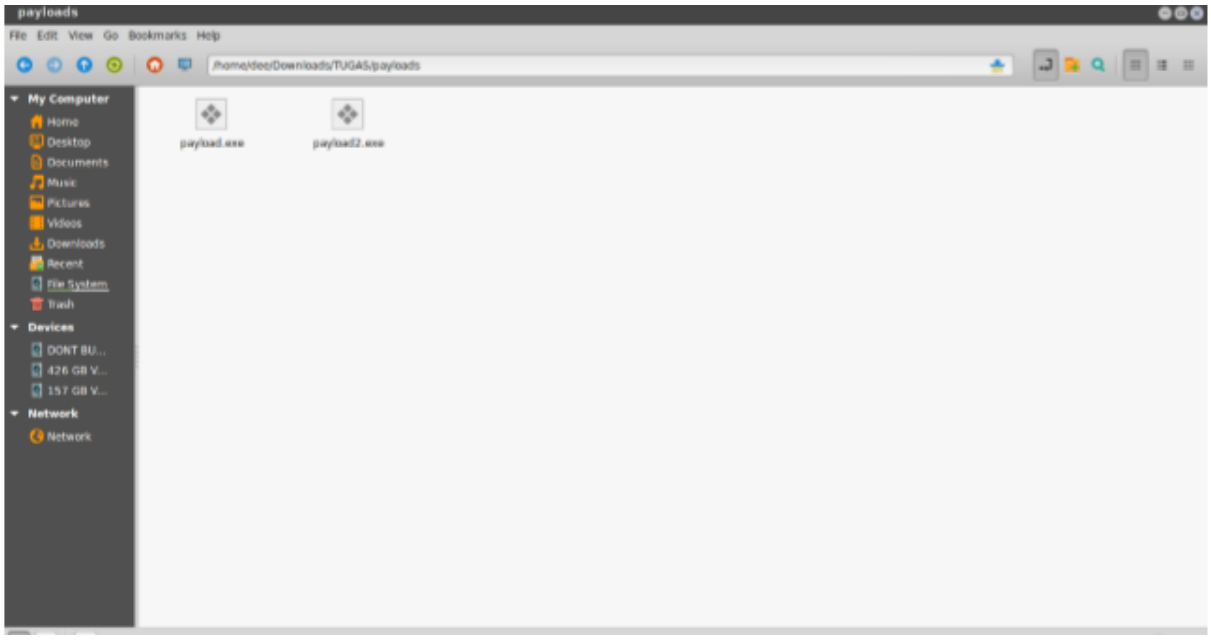
Analisa malware adalah suatu aktivitas yang kerap dilakukan oleh sejumlah praktisi keamanan teknologi informasi untuk mendeteksi ada atau tidaknya komponen sub program atau data yang bertujuan jahat dalam sebuah file elektronik.

Ada dasarnya malware adalah sebuah program, yang disusun berdasarkan tujuan tertentu dengan menggunakan logika dan algoritma yang relevan dengannya. Oleh karena itulah maka model analisa yang biasa dipergunakan untuk mengkaji malware sangat erat kaitannya dengan ilmu dasar komputer, yaitu: bahasa pemrograman, algoritma, struktur data, dan rekayasa piranti lunak.

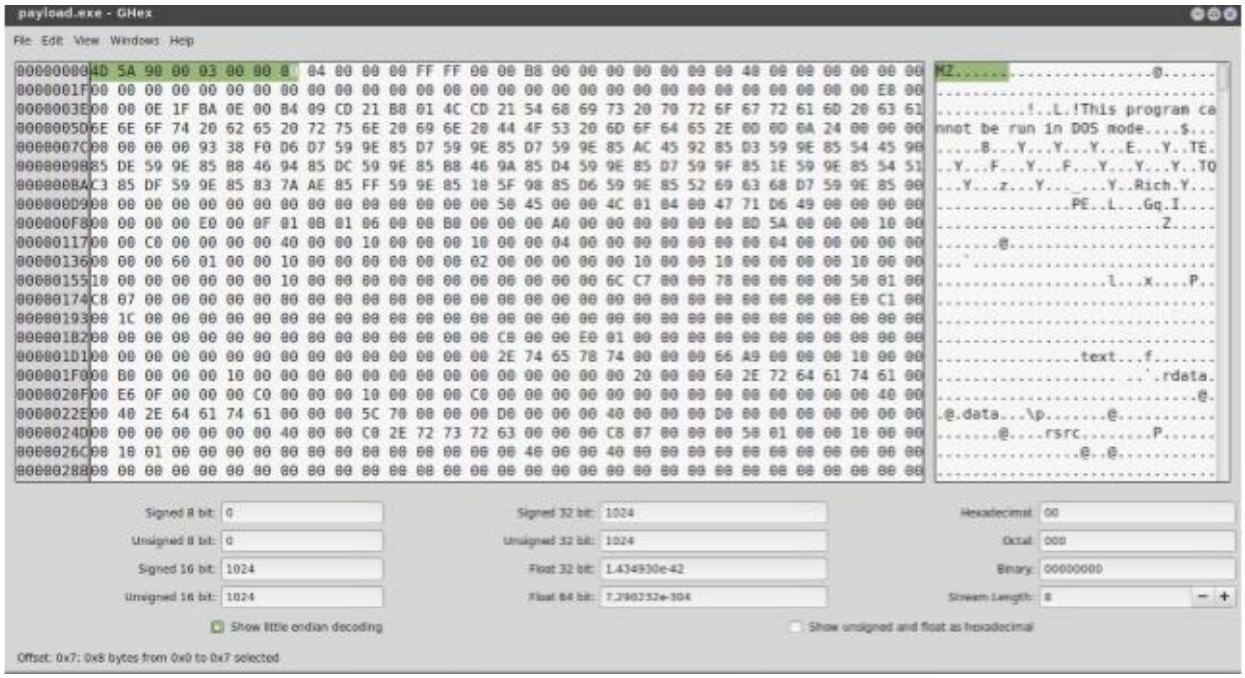
- Sebagai bahan praktek, digunakan bahan yang telah diberikan berupa payload.exe, dan payload2.exe . tools yang digunakan untuk menganalisa bahan yang diberikan berupa ghex, hexdump, strings, ollydbg, dan ida pro.Ghex berguna untuk debugging masalah dengan kode, dan untuk memuat data dari file, melihat dan mengedit hex dan ascii.

Pertama yang dilakukan membuka file yang diberikan :

Terdapat dua file pada gambar dibawah berupa payload.exe dan payloads2.exe

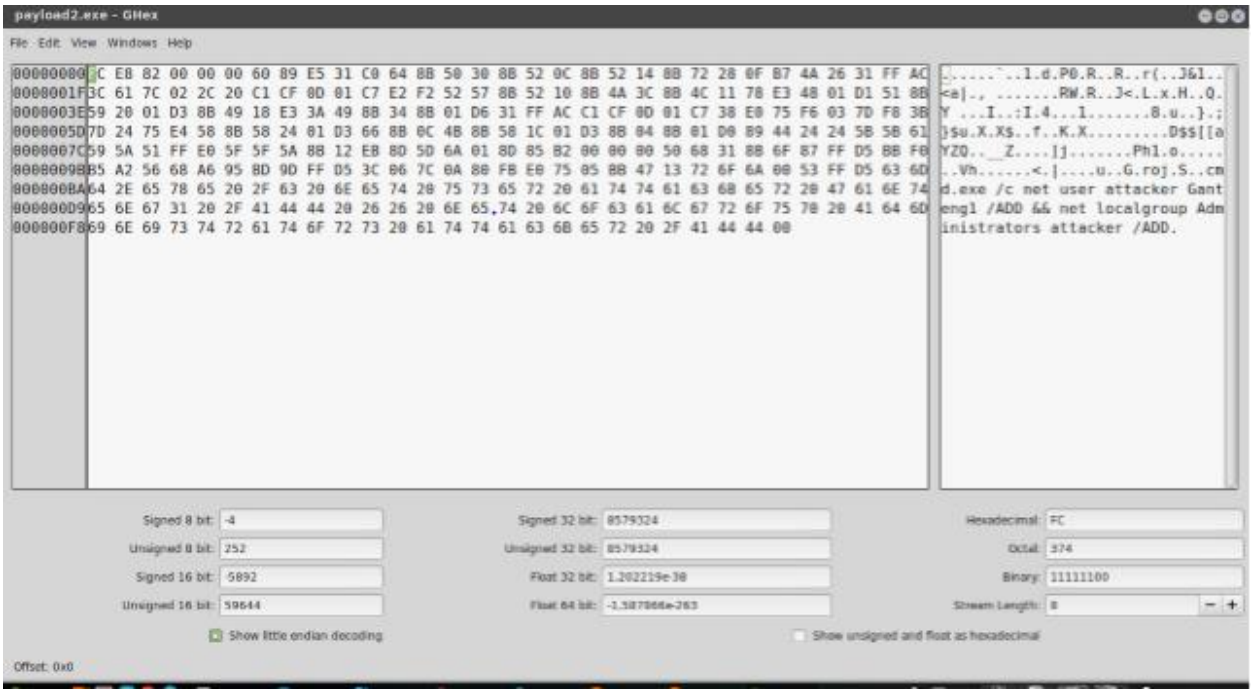


Pada langkah selanjutnya kita melakukan terlebih dahulu pada payload.exe. dengan cara klik kanan pada file tersebut dan open with dengan ghex maka akan tampil seperti gambar dibawah yang menampilkan kode yang diblok berwarna hijau tersebut.

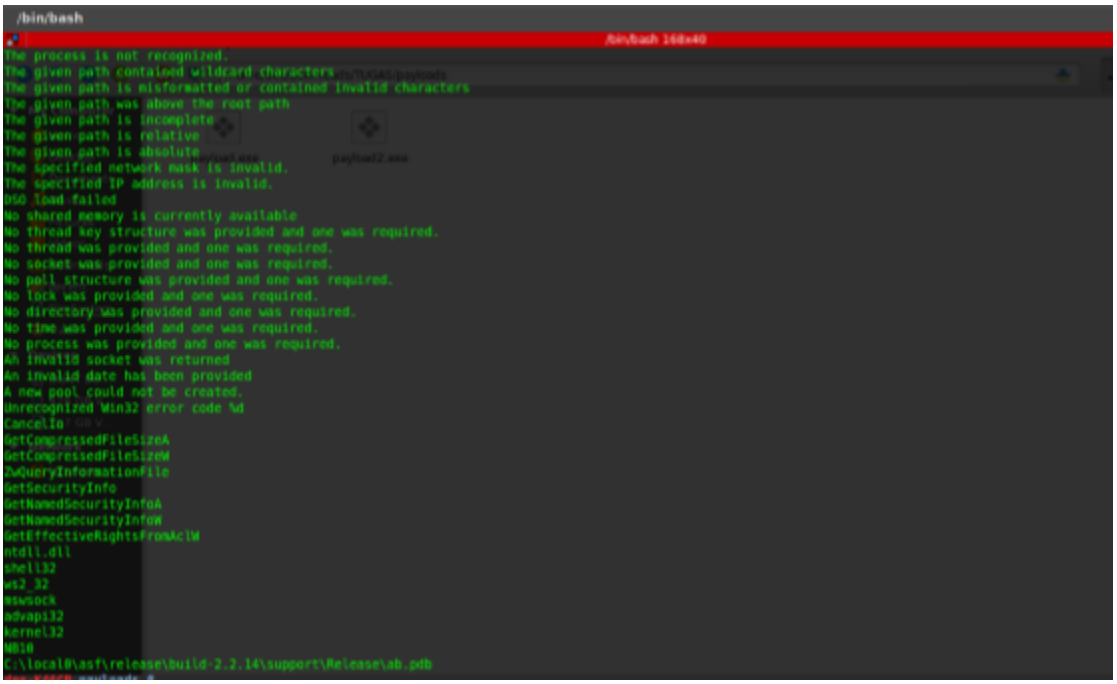


Langkah selanjutnya kita dapat mencari di list file signature, dapat dilihat dari gambar dibawah terdapat file yaitu file mz. File MZ ialah jenis file yang hanya tersedia untuk windows dan berjenis aplikasi.

Berikut kita lakukan file yang kedua yaitu payloads2.exe. gambar dibawah ini menunjukan hasil dari kode hex pada file payloads2.exe

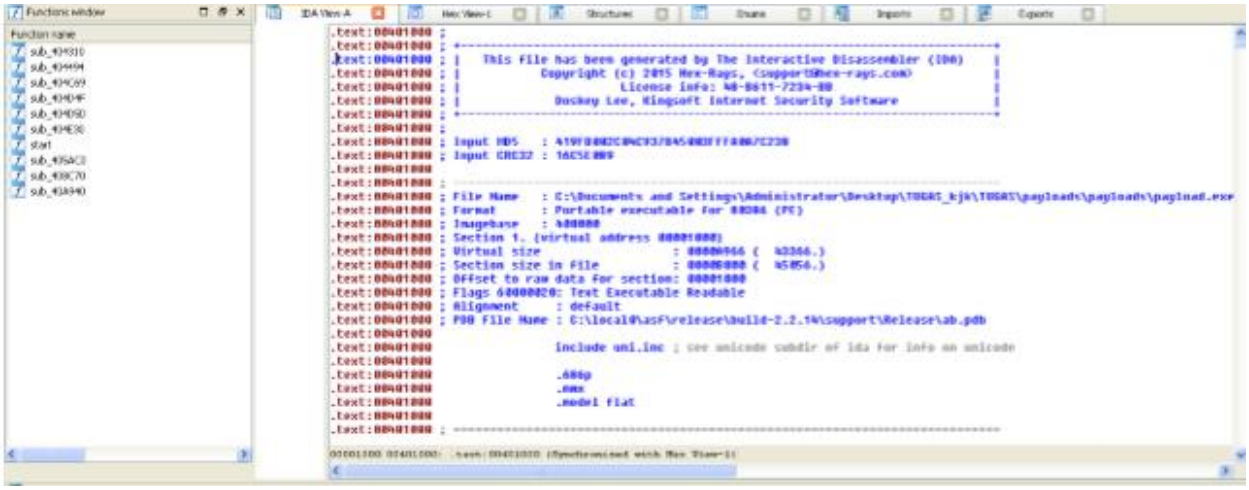


Kita dapat melakukkan perintah diterminal untuk menampilkan file strings payload.exe , maka yang akan tampil seperti gambar dibawah.

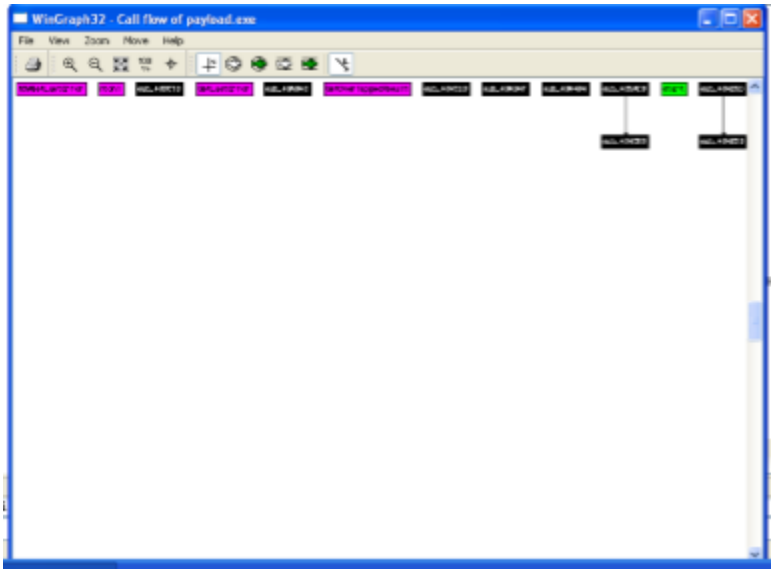


Kita dapat melakukkan perintah tersebut pada dua file yaitu strings payload.exe dan payload2.exe

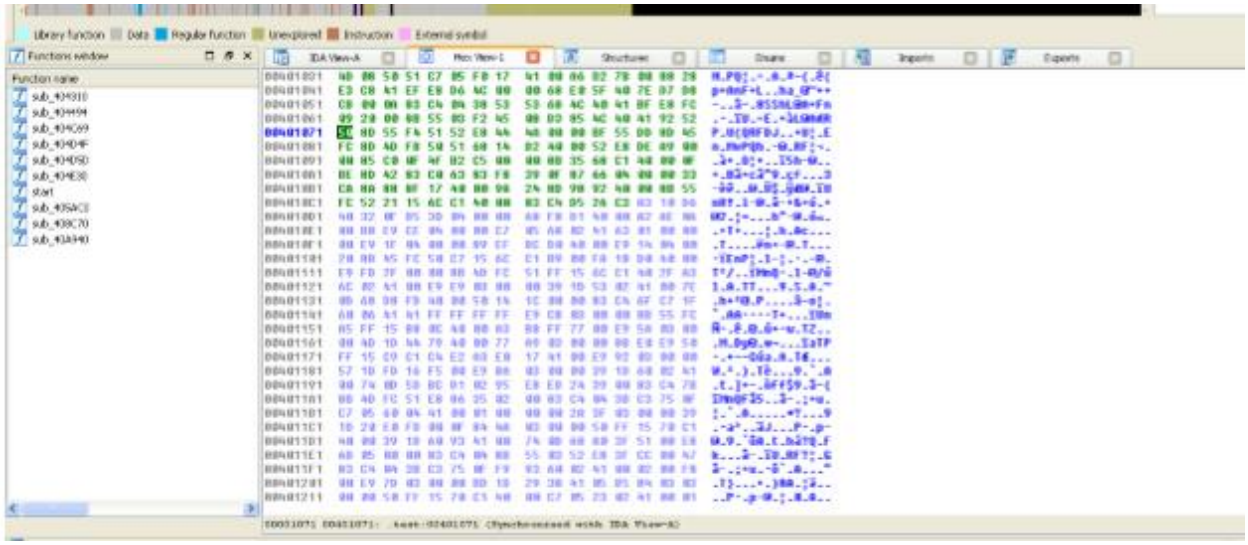
Pada gambar dibawah terdapat hasil convert file tersebut dalam assembly.



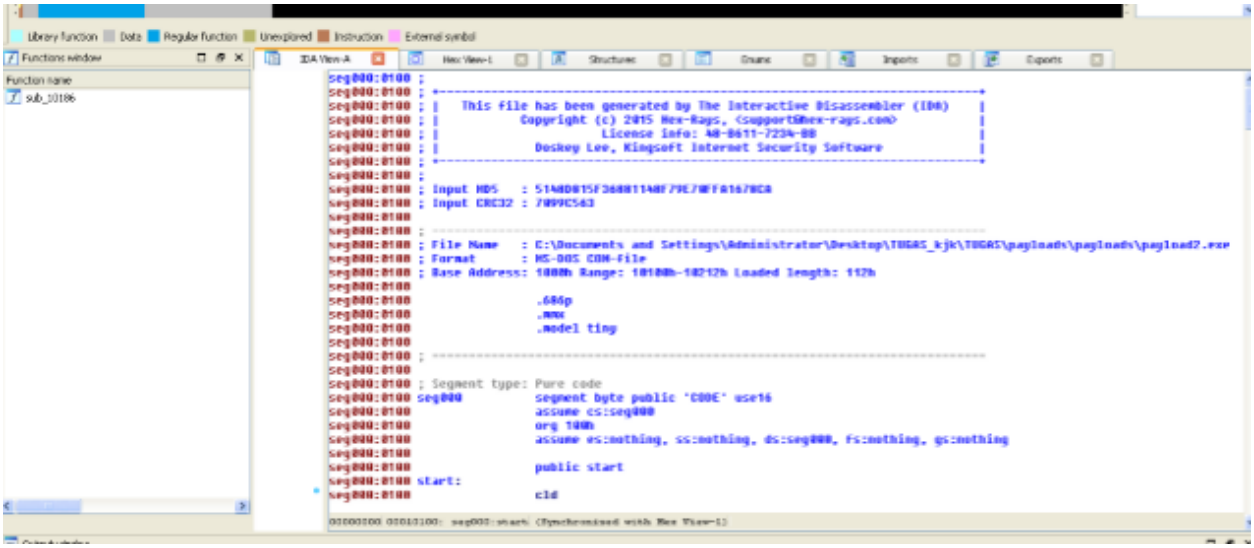
Terdapat graph alur pada payload.exe



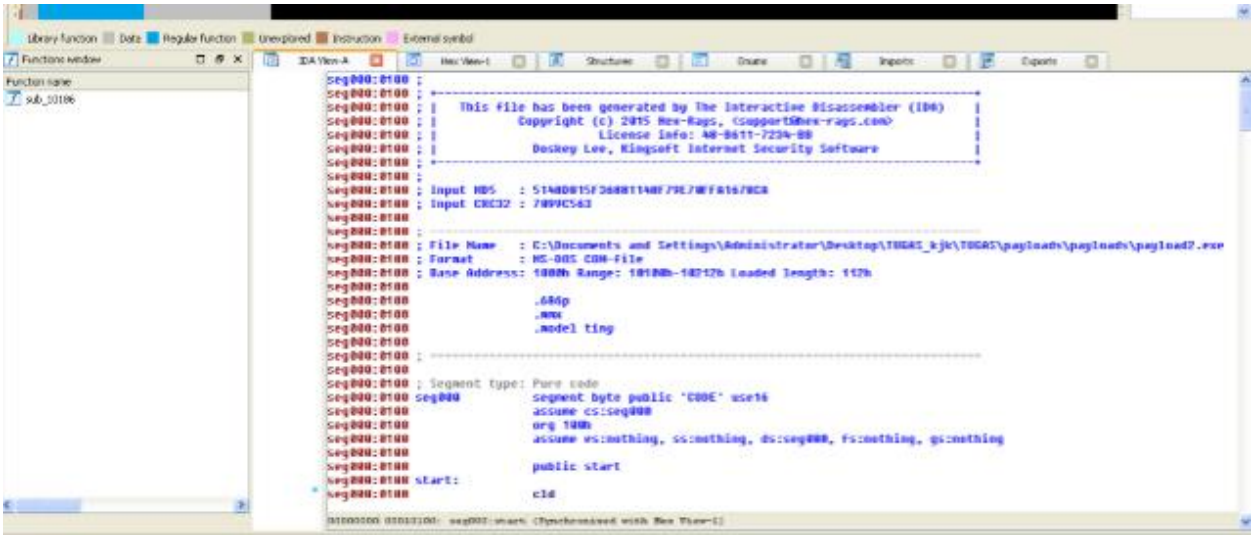
Pada gambar dibawah inilah hasil dari hex.



Gambar dibawah langkah melakukkan file yang kedua yaitu payload2.exe

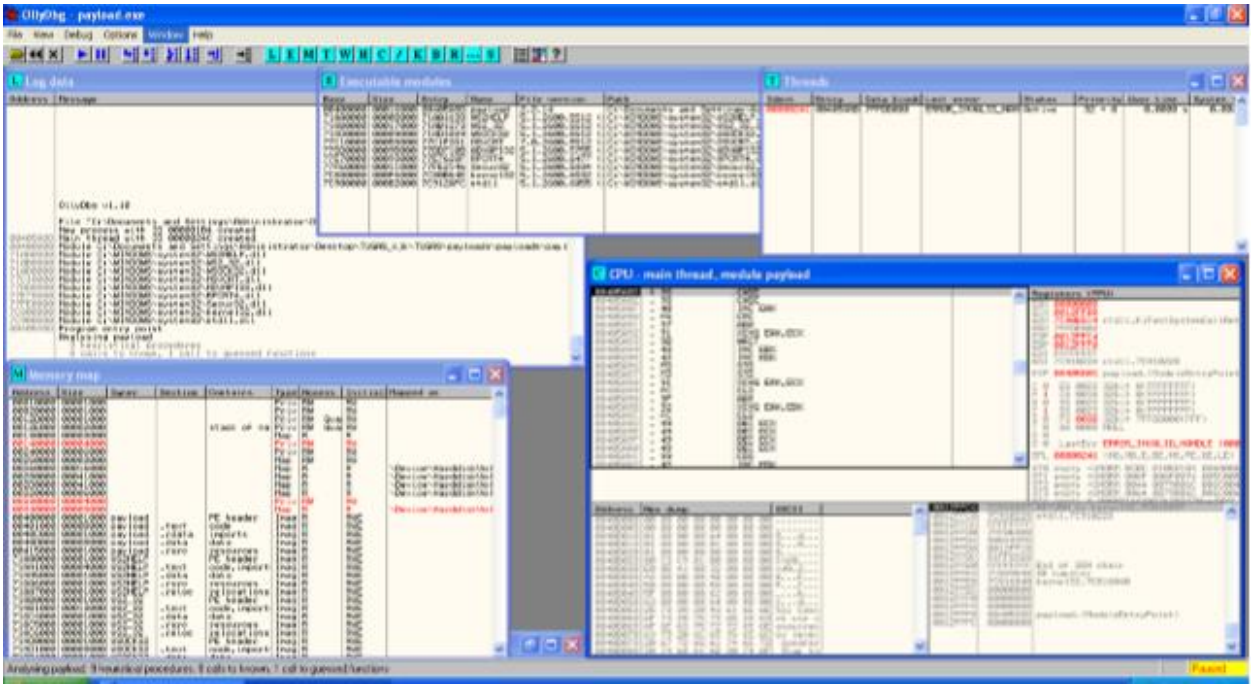


Contoh gambar convert assembly pada file payload2.exe



Terdapat dua contoh gambar hasil dari masing – masing file:

Gambar dibawah ialah hasil dari file payload.exe



Gambar dibawah ialah hasil dari file payload2.exe