TUGAS
KEAMANAN JARINGAN KOMPUTER

Nama : Dede Triseptiawan

Nim : 09011181320001

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2017

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.

Pada saat ini, sudah tersedia berbagai macam software yang dapat digunakan untuk melindungi komputer / jaringan komputer dari serangan malware, diantaranya : antivirus, firewall, ids, internet protection dan lain-lain. Namun kecanggihan dari software tersebut, umumnya dapat dilewati menggunakan teknik-teknik tertentu sehingga software tersebut tidak dapat mendeteksi adanya aktivitas malicious program yang sedang berjalan.

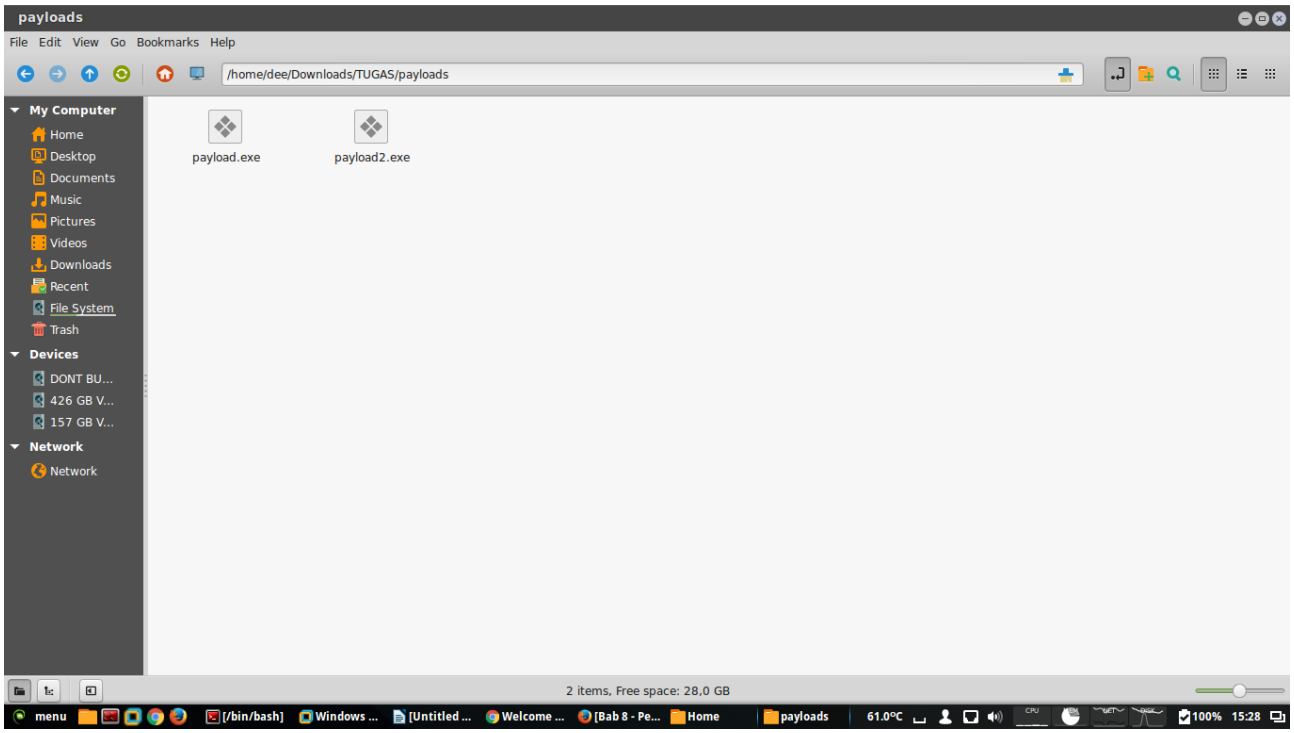
Ada dua metode untuk melakukan analisa terhadap malware, yaitu :

1. **Dynamic Analysis** : Merupakan metode yang digunakan untuk melakukan analisa terhadap malware dengan mengamati kinerja sistem yang dapat terlihat dari perilaku sistem sebelum malware dijalankan dengan perilaku sistem setelah malware tersebut dijalankan pada sistem tersebut. Metode dynamic analysis umumnya menggunakan software virtual seperti VirtualBox, VMWare dan lain-lain, sehingga apabila malware yang dijalankan tersebut ternyata merusak sistem, maka sistem utama tidak mengalami kerusakan akibat malware tersebut.
2. **Static Analysis** : Merupakan metode yang digunakan untuk melakukan analisa malware dengan cara mengamati secara langsung kode sumber (source code) malware tersebut. Dalam mengamati kode sumber malware, terdapat teknik yang umumnya digunakan, yaitu Reverse Engineering.

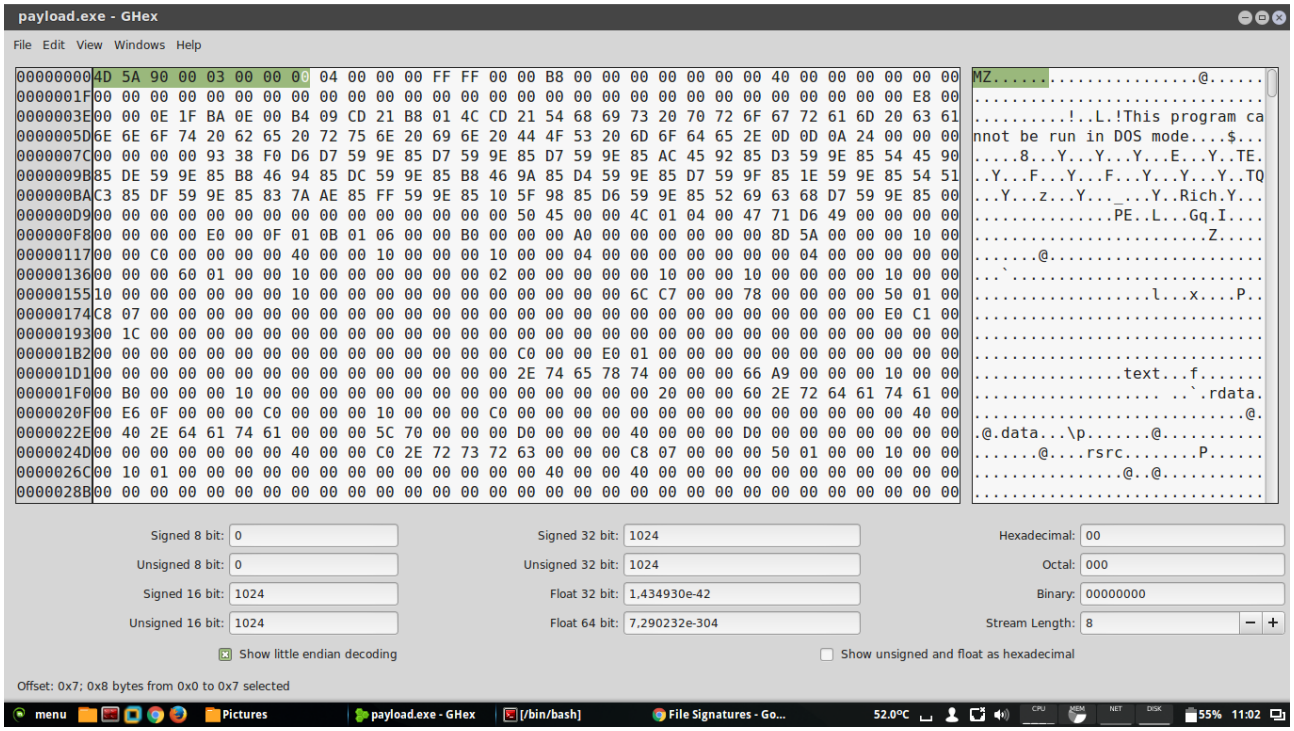
Sebagai uji coba, digunakan bahan yang telah diberikan berupa payload.exe, dan payload2.exe . Dan tools yang digunakan untuk menganalisa bahan yang diberikan berupa ghex, hexdump, strings, ollydbg, dan ida pro.Ghex berguna untuk debugging masalah dengan

kode, dan untuk memuat data dari file, melihat dan mengedit hex dan ascii. Hexdump fungsinya sama dengan ghex untuk melihat kode hex yang ada pada file tersebut, beda dengan ghex tampilan berbentuk gui. Strings befungsi untuk melihat program/ perintah-perintah dalam sebuah file. Ollydbg berfungsi untuk debugging / debug dan melakukan dumping, serta melakukan pengintaian proses apa saja yang terjadi pada sebuah program. Ida pro adalah piranti bantuan untuk melakukan debug dengan melihat kode program dalam bentuk assembler.

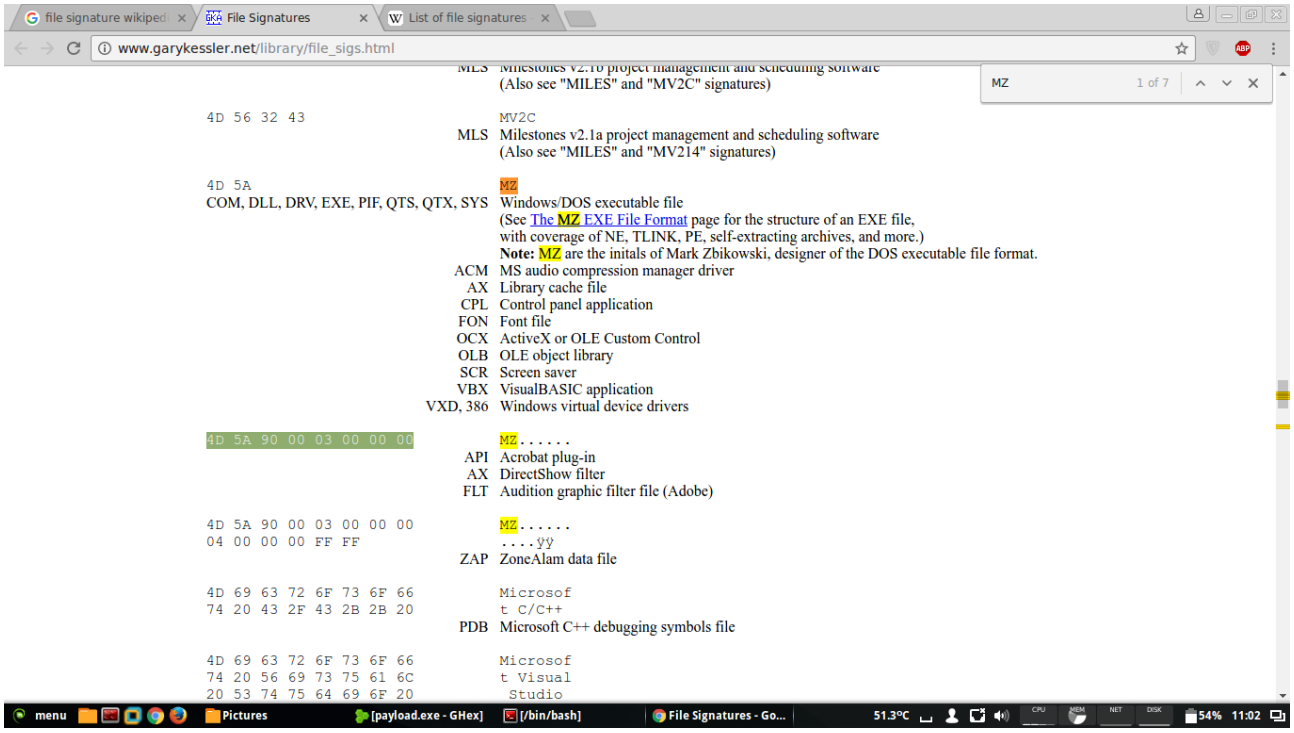
Pertama yang dilakukan membuka file yang diberikan



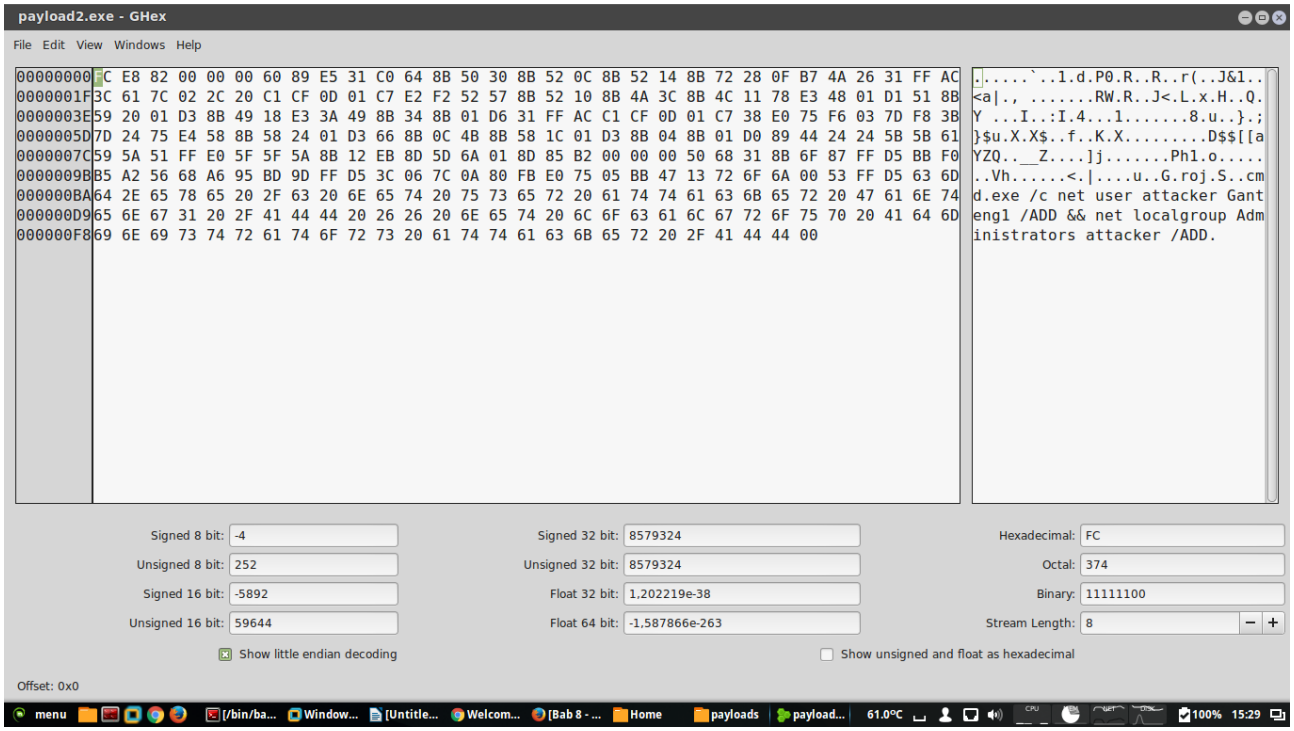
Terdapat 2 file pada gambar di atas berupa payload.exe dan payload2.exe. kemudian kita coba terlebih dahulu payload.exe. dengan cara klik kanan pada file tersebut dan open with dengan ghex.



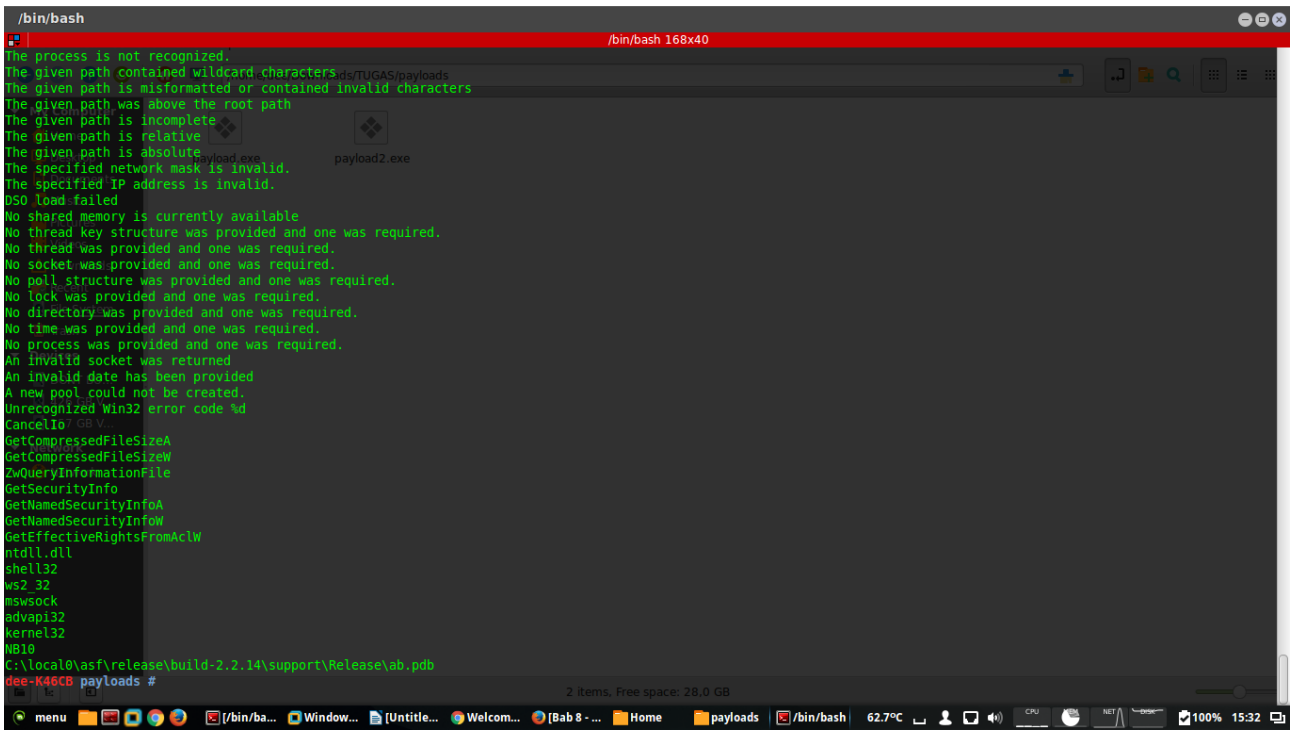
Berikut tampilan pada ghex, terdapat kode yang diblok berupa 4D 5A 90 00 03 00 00 00 dan kode sebelahnya MZ..... kemudian kita cari di list of file signiture



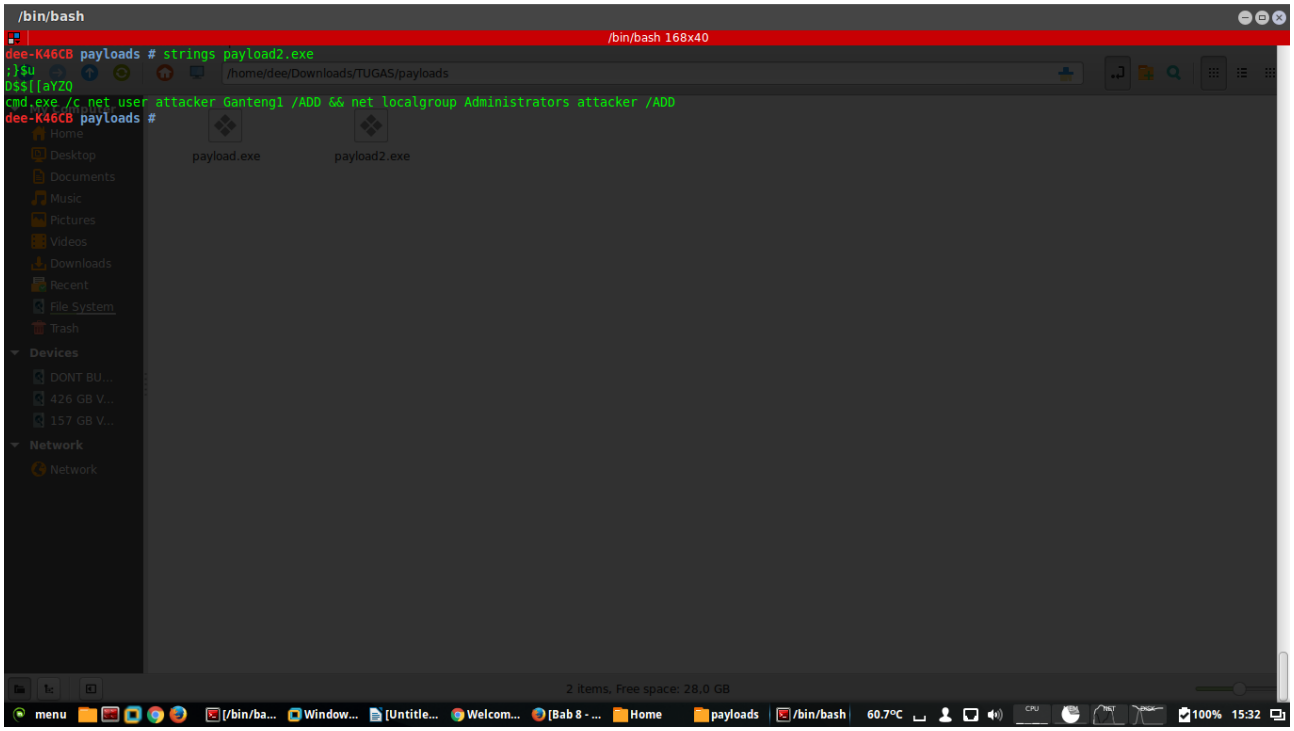
File MZ..... merupakan jenis file yang hanya tersedia untuk windows dan berjenis aplikasi API(acrobat plug-in), AX(directshow filter) dan FLT(audition graphic filter file(adobe)). Kemudian kita coba file payload2.exe



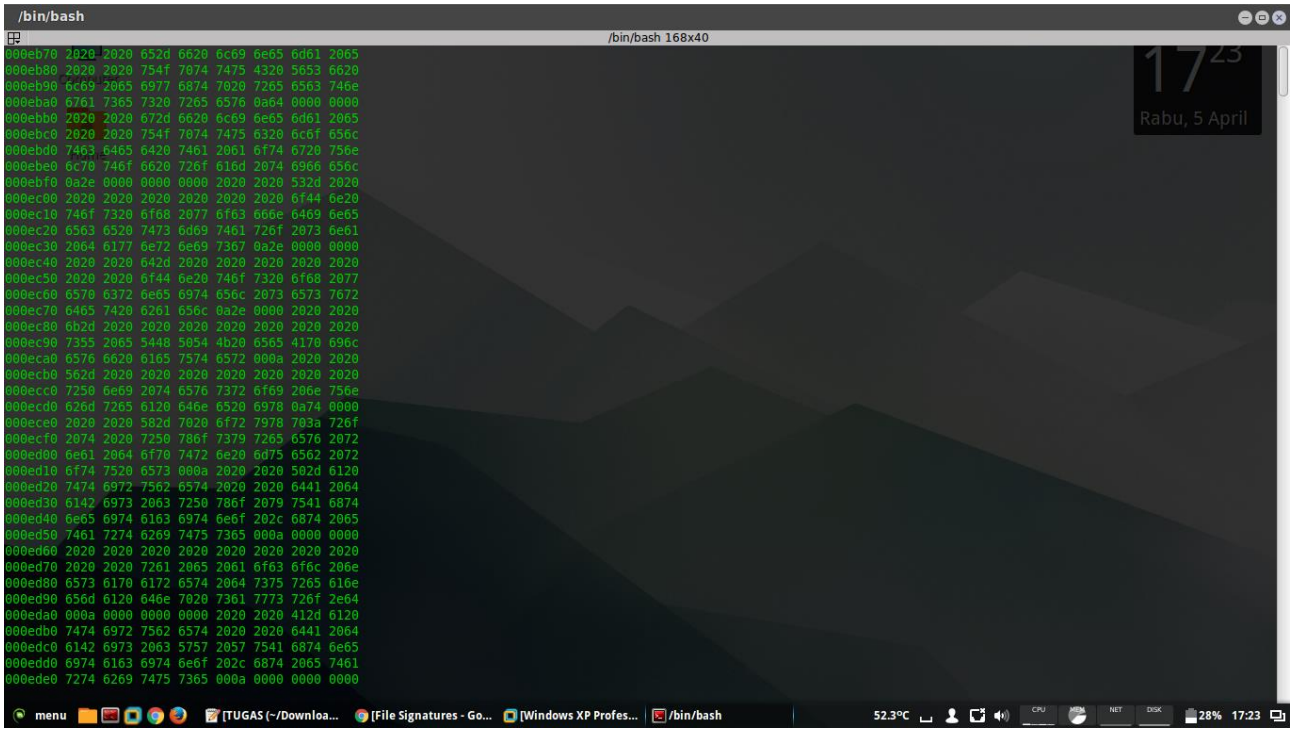
Berikut pada gambar diatas hasil kode hex pada file payload2.exe. kemudian kita lakukan dengan perintah di terminal strings payload.exe



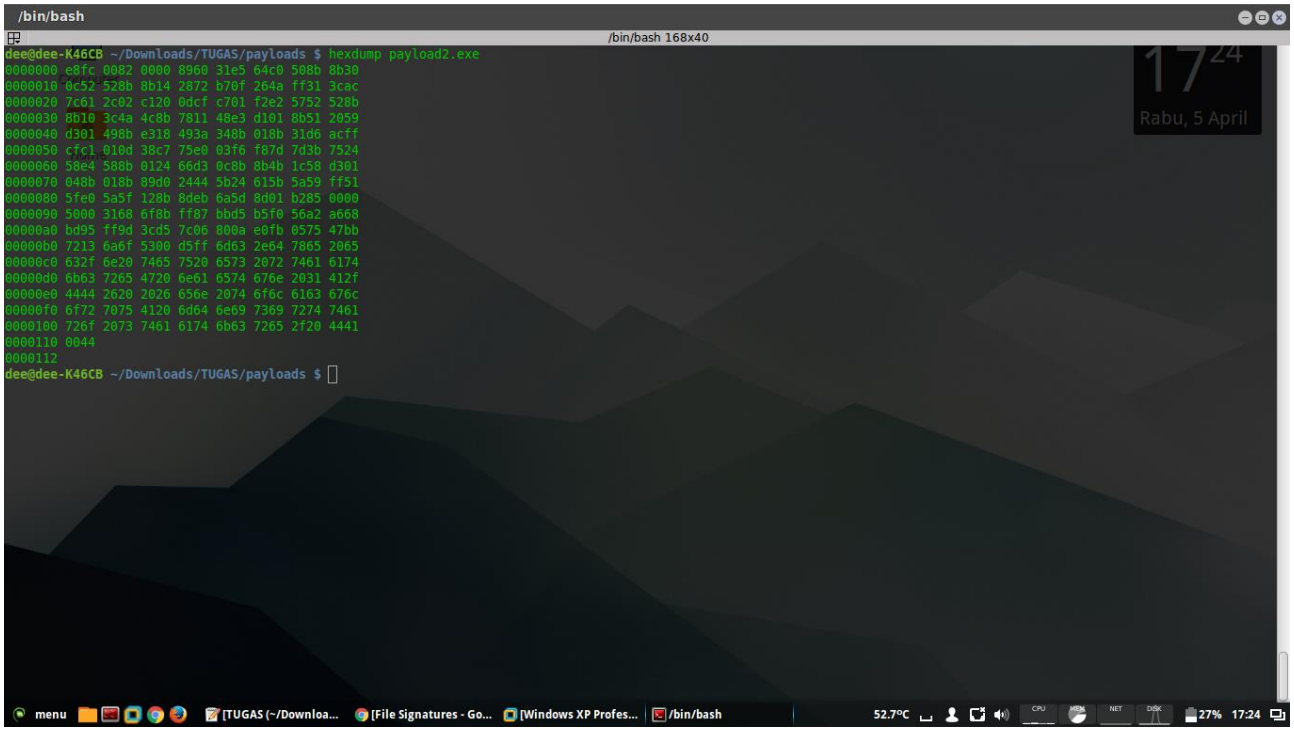
Maka akan keluar seperti gambar diatas, kemudian kita lakukan ke file selanjutnya



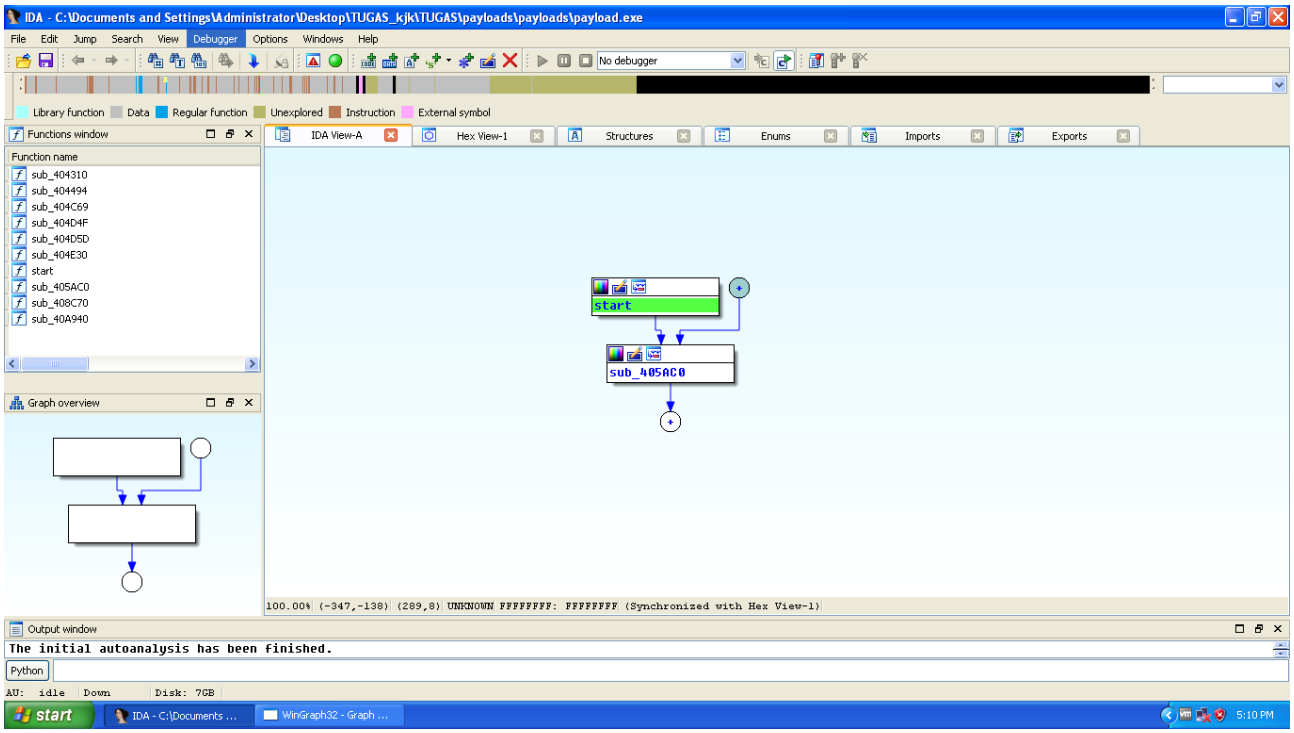
Maka akan tampil seperti gambar diatas. Kemudian kita lakukan perintah pada terminal dengan perintah hexdump payload.exe

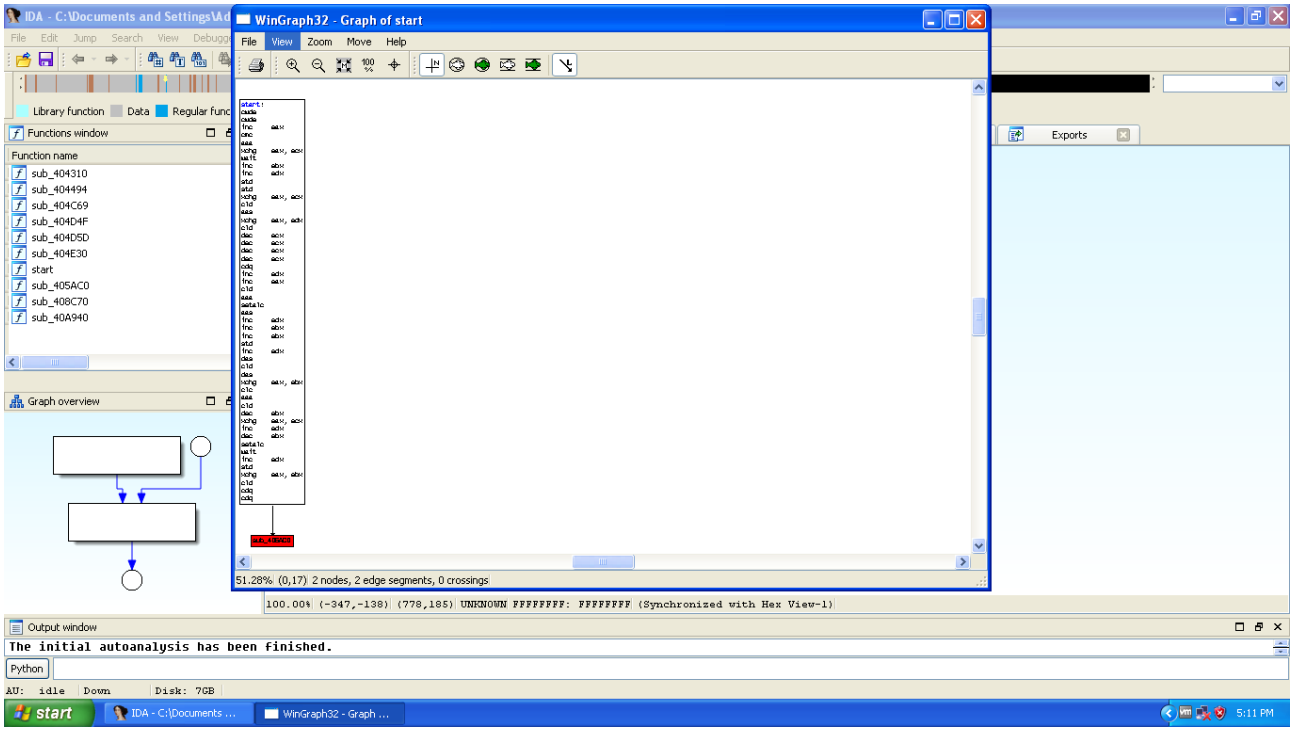


Maka akan keluar seperti gambar diatas, kemudian kita lakukan ke file satunya.

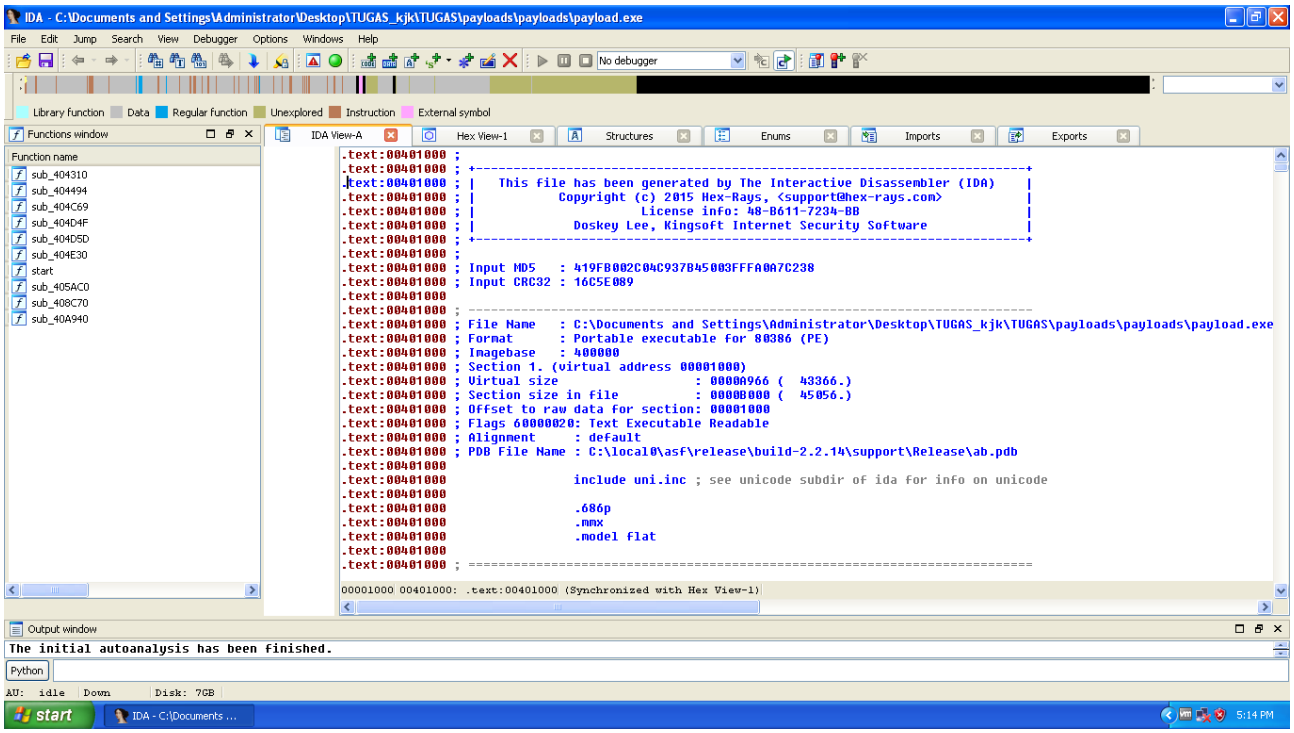


Maka akan keluar file hex seperti diatas. Kemudian kita buka tools virtual machine pada hal ini menggunakan vmware dan menggukan windows xp sebagai sistem operasi untuk menjalankan tools ollydbg dan idapro. Dan berikut hasil untuk payload.exe

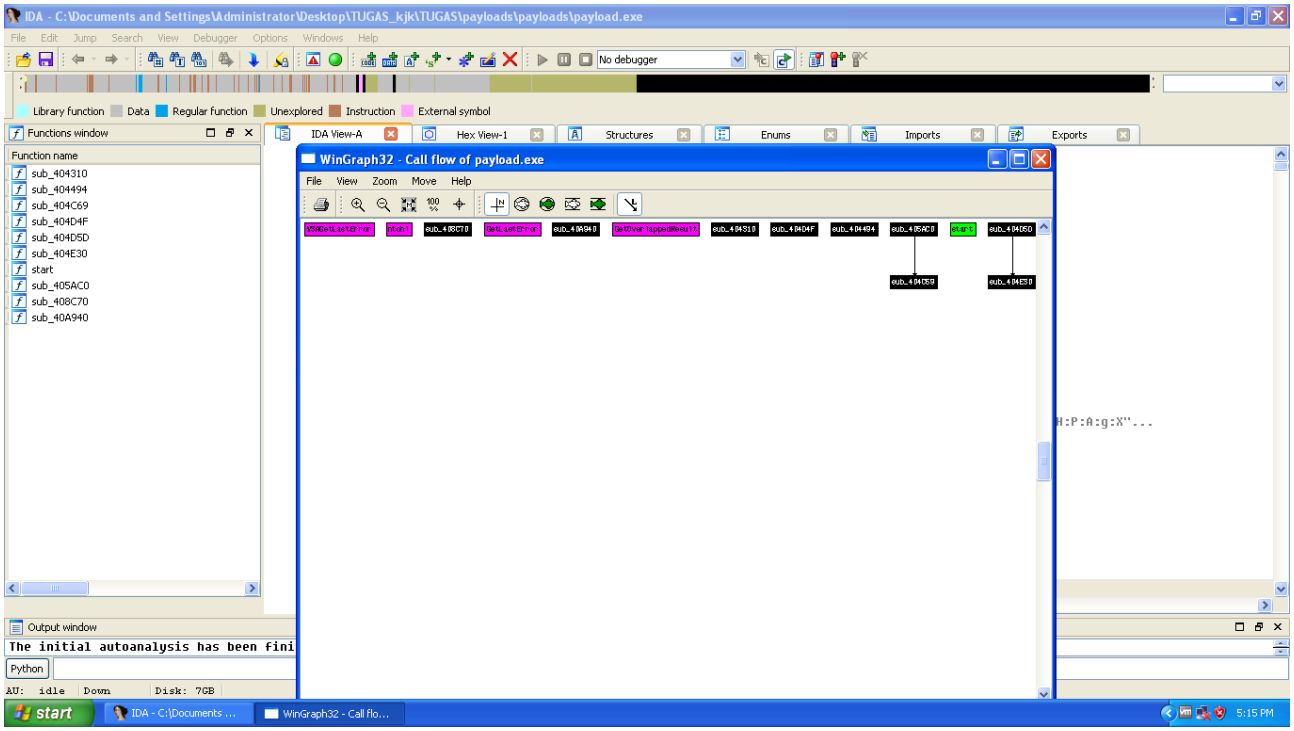




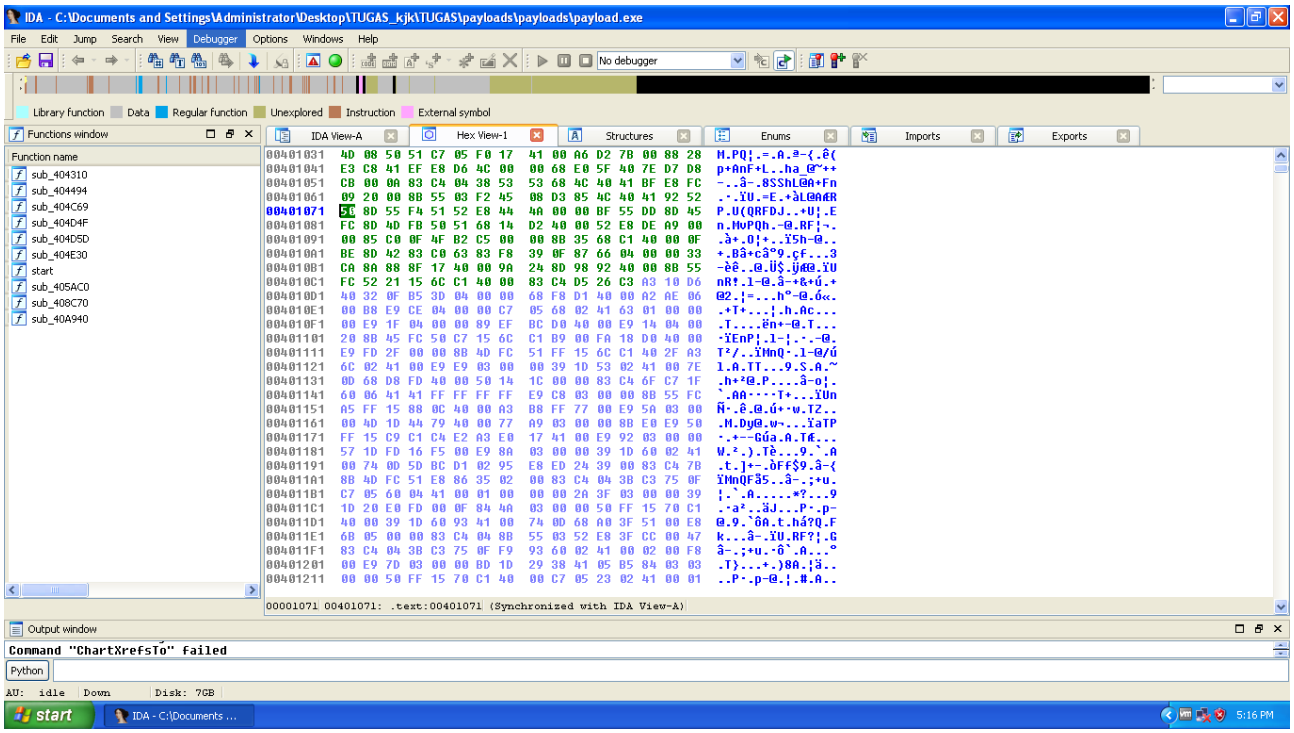
Pada gambar diatas merupakan alur (flowchart) graph yang tersedia pada aplikasi ida pro



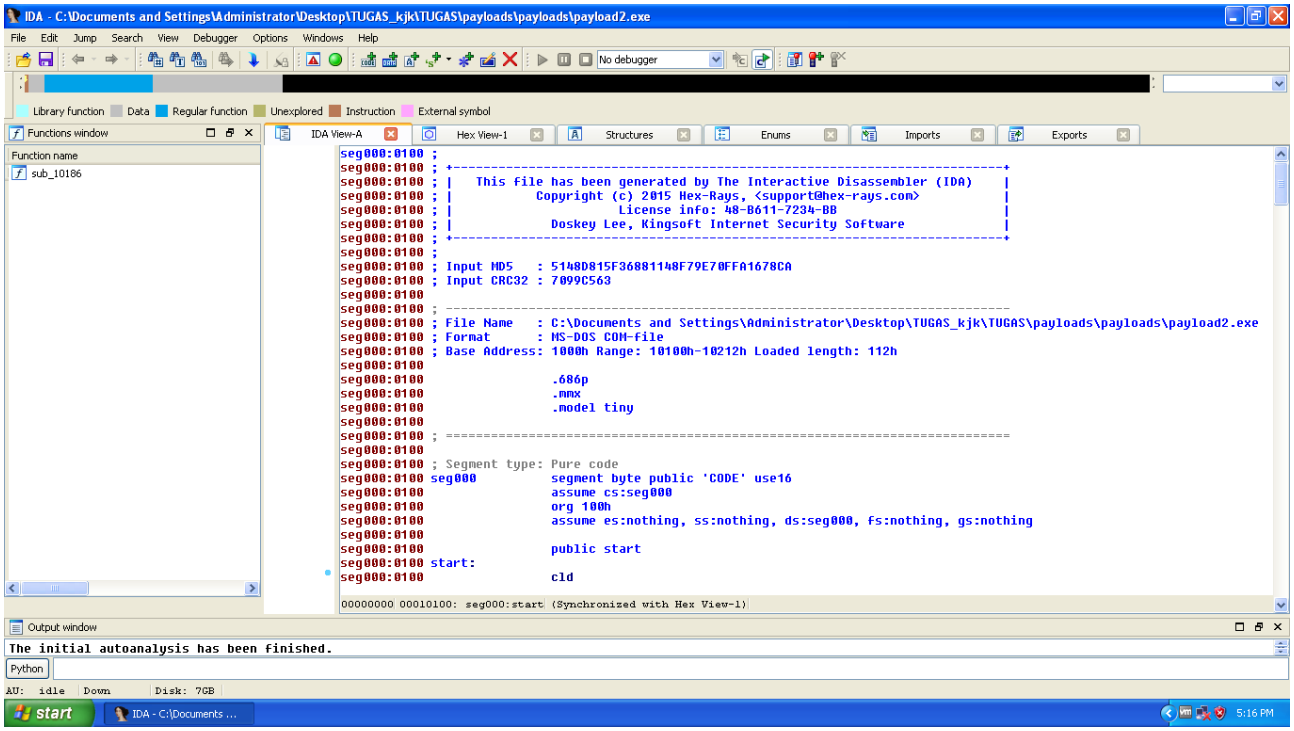
Pada gambar diatas merupakan hasil convert file tersebut dalam assembly



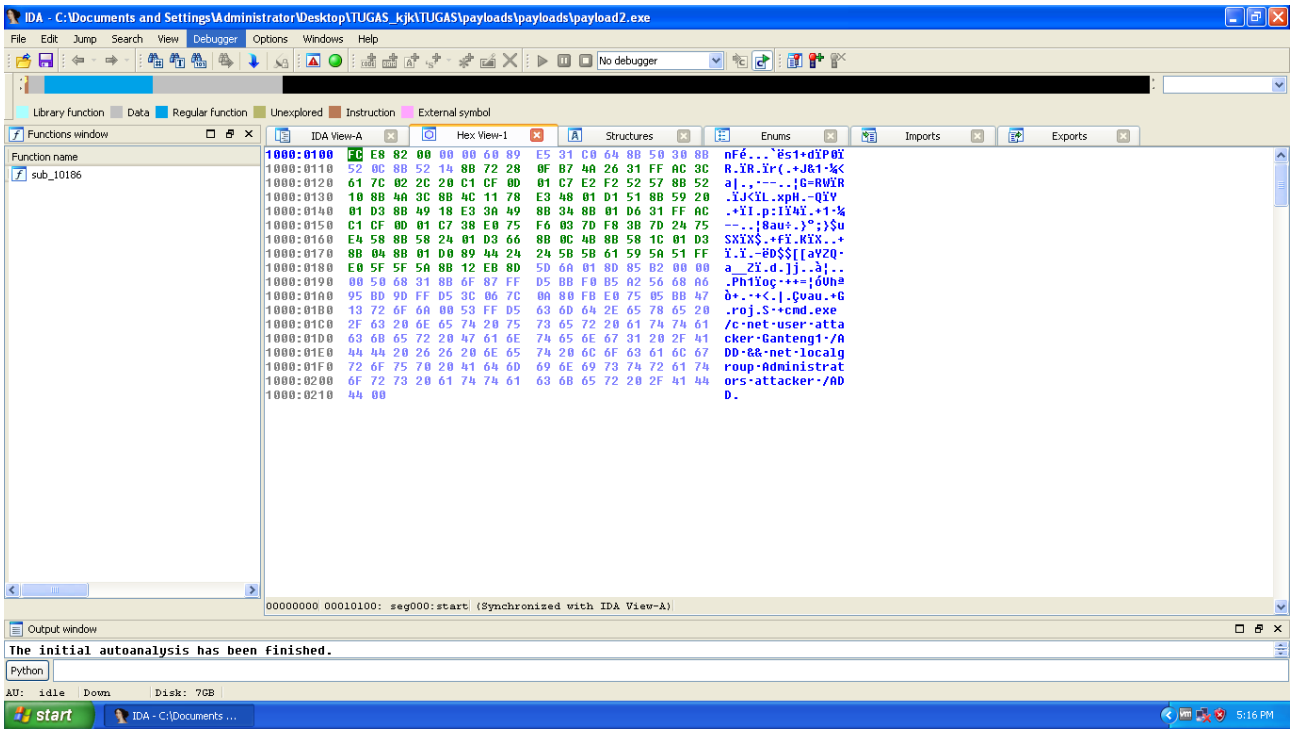
Berikut pada gambar diatas hasil graph alur pada payload.exe



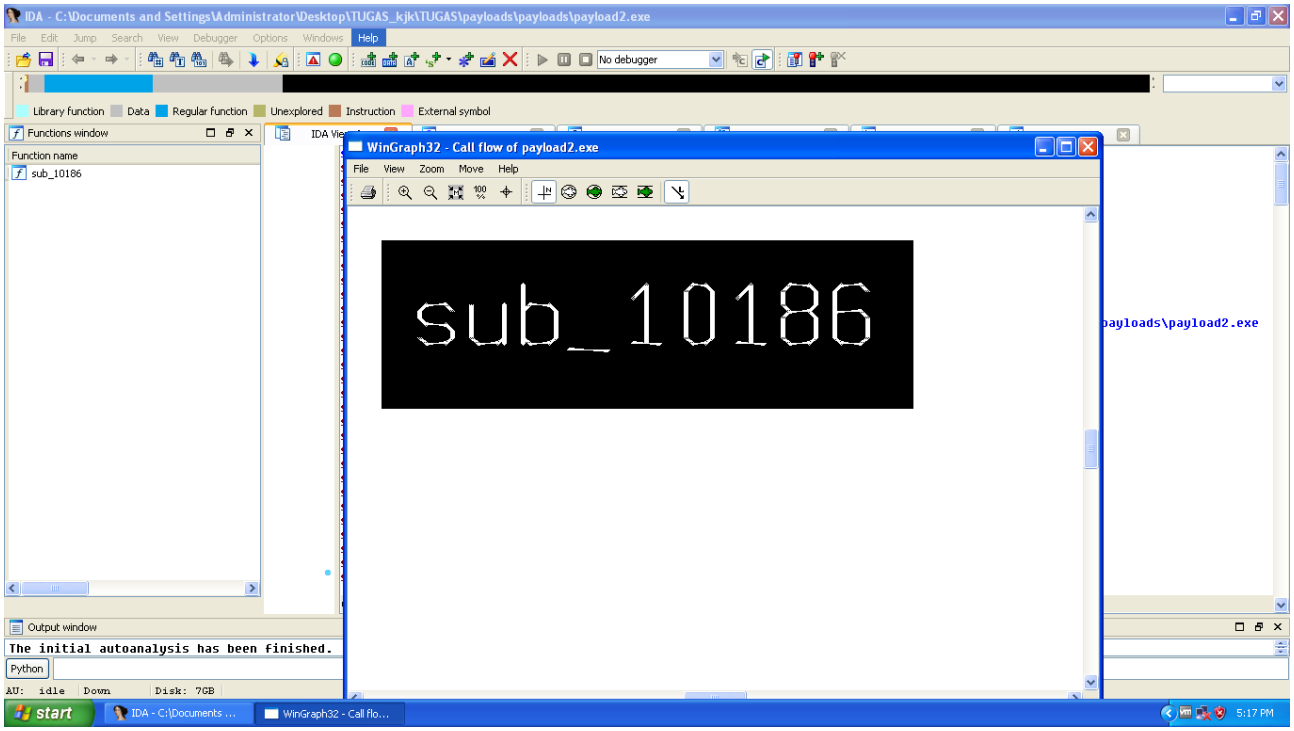
Pada gambar diatas merupakan hasil hex pada aplikasi ida pro. Kemudian kita lakukan pada file satunya payload2.exe



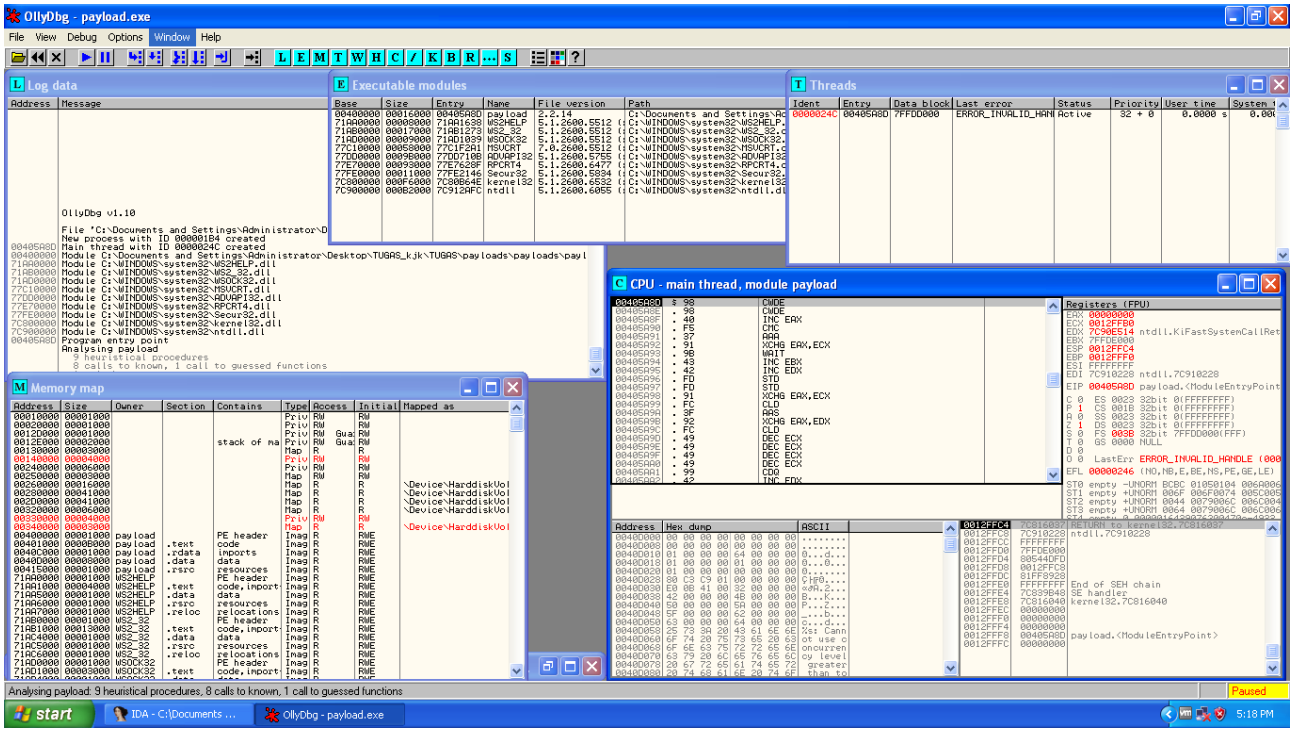
Pada gambar diatas merupakan hasil convert assembly pada file payload2.exe



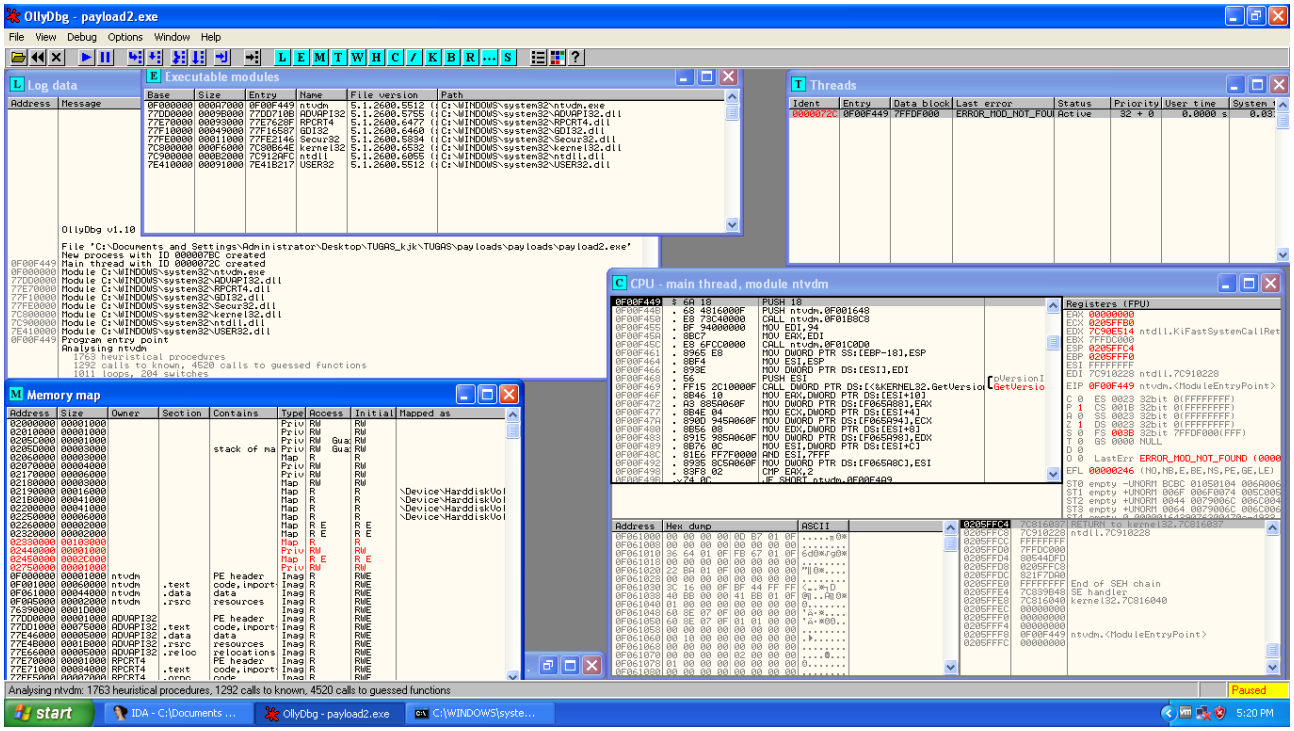
Pada gambar diatas merupakan hasil hex pada file payload2.exe



Pada gambar diatas merupakan hasil graph pada payload2.exe. kemudian kita gunakan aplikasi ollydbg



Pada gambar diatas merupakan hasil dari file payload.exe



Pada gambar diatas merupakan hasil dari file payload2.exe