NAMA : DWI KURNIA PUTRA

NIM : 09011181320019

MK : KEAMANAN JARINGAN KOMPUTER

ANALISIS MALWARE

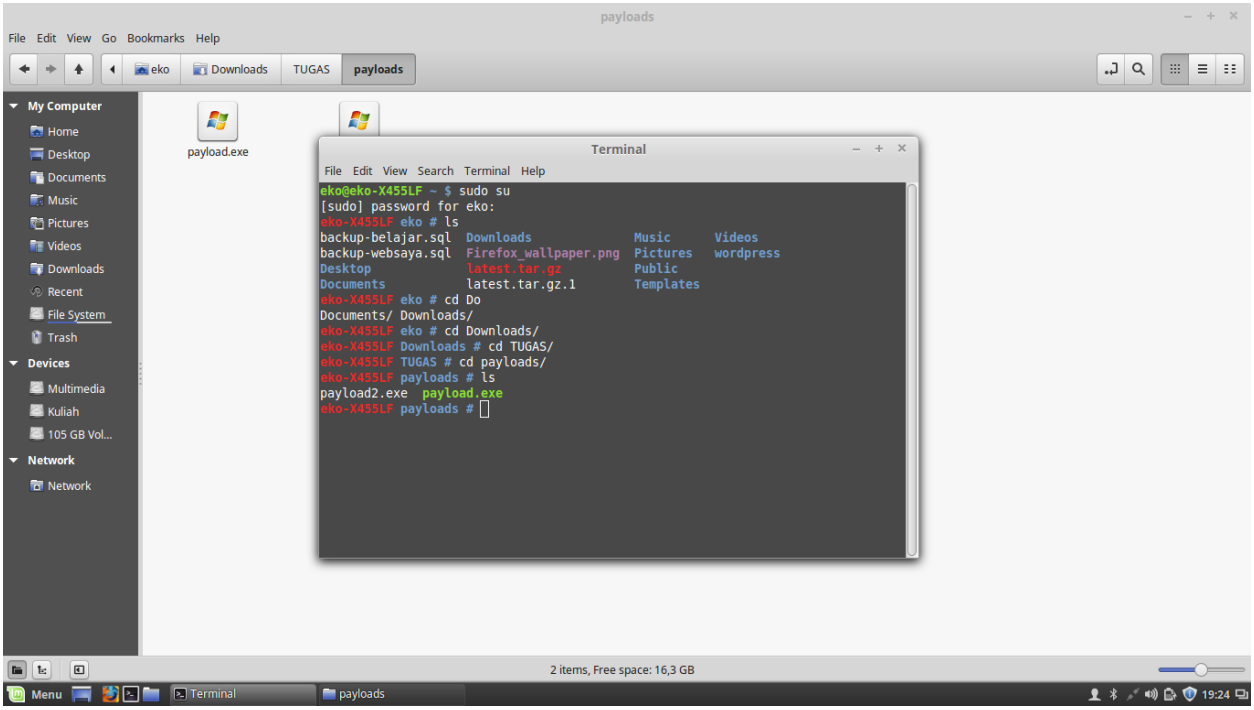
Modus operandi kejahatan di dunia siber sangatlah beragam dan bervariasi. Teknik yang dipergunakan oleh para kriminal pun semakin lama semakin mutakhir dan kompleks. Berdasarkan kejadian-kejadian terdahulu, hampir seluruh serangan melibatkan apa yang disebut sebagai "malicious software" atau "malware" – yang dalam terjemahan bebasnya adalah program jahat (karena sifatnya yang merusak atau bertujuan negatif). Analisa malware adalah suatu aktivitas yang kerap dilakukan oleh sejumlah praktisi keamanan teknologi informasi untuk mendeteksi ada atau tidaknya komponen subprogram atau data yang bertujuan jahat dalam sebuah file elektronik. Analisa atau kajian ini sangat penting untuk dilakukan karena:

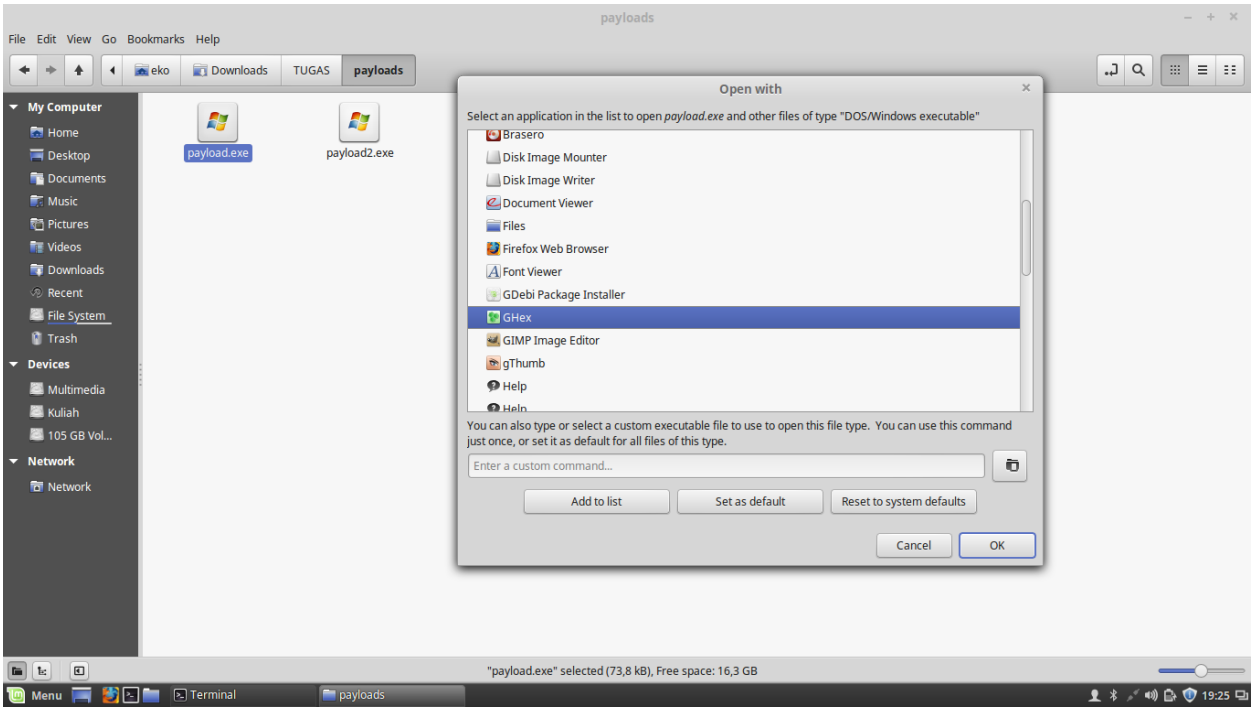
- Malware sering diselundupkan melalui file-file umum dan popular seperti aplikasi (.exe), pengolah kata (.doc), pengolah angka (.xls), gambar (.jpg), dan lain sebagainya – sehingga jika pengguna awam mengakses dan membukanya, akan langsung mejadi korban program jahat seketika;
- Malware sering diselipkan di dalam kumpulan file yang dibutuhkan untuk menginstalasi sebuah program atau aplikasi tertentu – sehingga jika sang pengguna melakukan instalasi terhadap aplikasi dimaksud, seketika itu juga malware diaktifkan;
- Malware sering disamarkan dengan menggunakan nama file yang umum dipakai dalam berbagai keperluan, seperti driver (.drv), data (.dat), library (.lib), temporary (.tmp), dan lain-lain – sehingga pengguna tidak sadar akan kehadirannya di dalam komputer yang bersangkutan;
- Malware sering dikembangkan agar dapat menularkan dirinya ke tempattempat lain, dengan cara kerja seperti virus atau worms – sehingga computer pengguna dapat menjadi sarang atau sumber program jahat yang berbahaya;
- Malware sering ditanam di dalam sistem komputer tanpa diketahui oleh sang pengguna – sehingga sewaktu-waktu dapat disalahgunakan oleh pihak yang tidak berwenang untuk melakukan berbagai tindakan kejahatan; dan lain sebagainya.

Pada 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. Secara umum, ada 3 (tiga) jenis analisa terhadap sebuah program untuk mendeteksi apakah yang bersangkutan merupakan malware atau bukan, yaitu Surface Analysis, Runtime Analysis, Static Analysis.

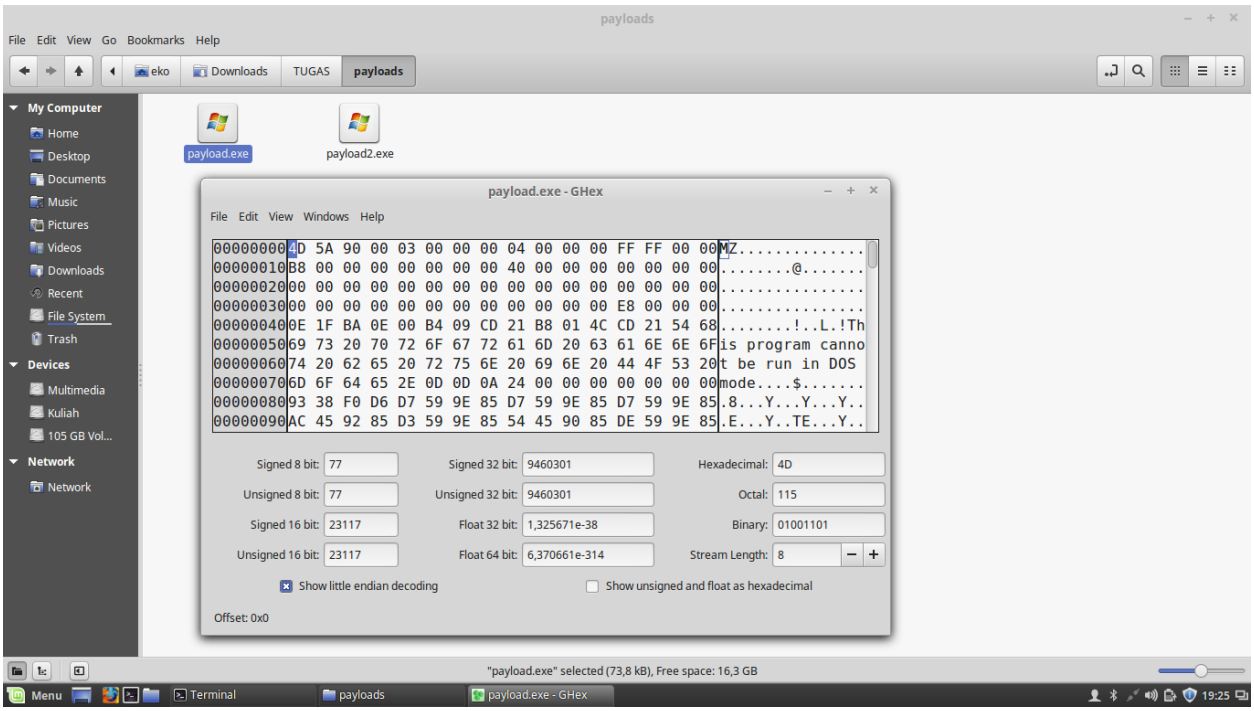
PERCOBAAN DARI ANALISIS MALWARE

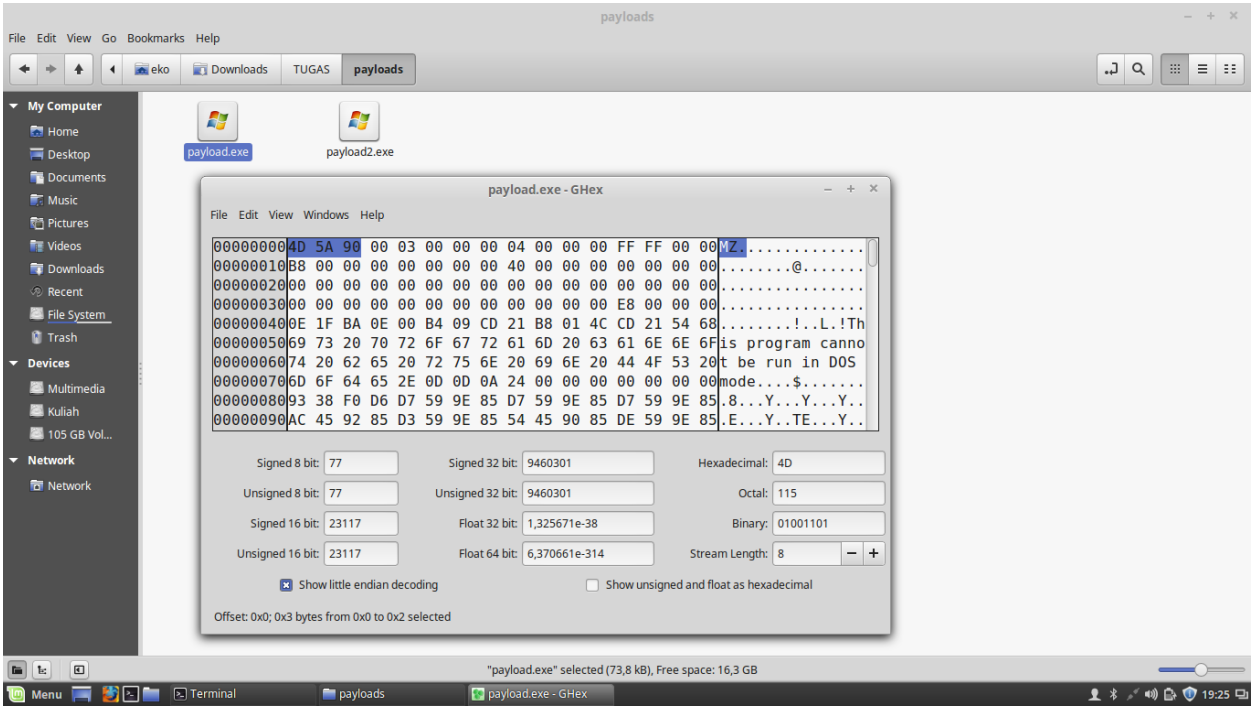
File dengan nama dan ekstensi paylouds.exe dan paylouds2.exe sebagai bahan dari malware yang akan di analisis.



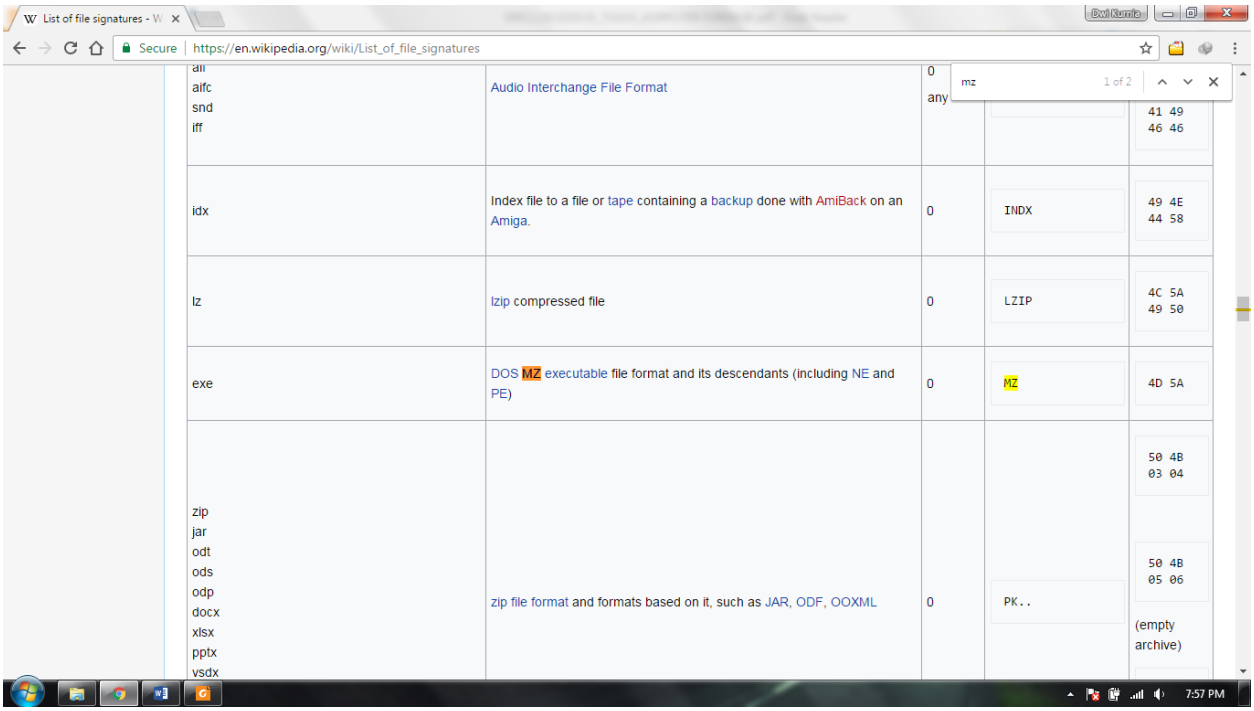


Membuka file dari paylouds.exe dengan tool Ghex untuk mengecek kode biner dari file tersebut.

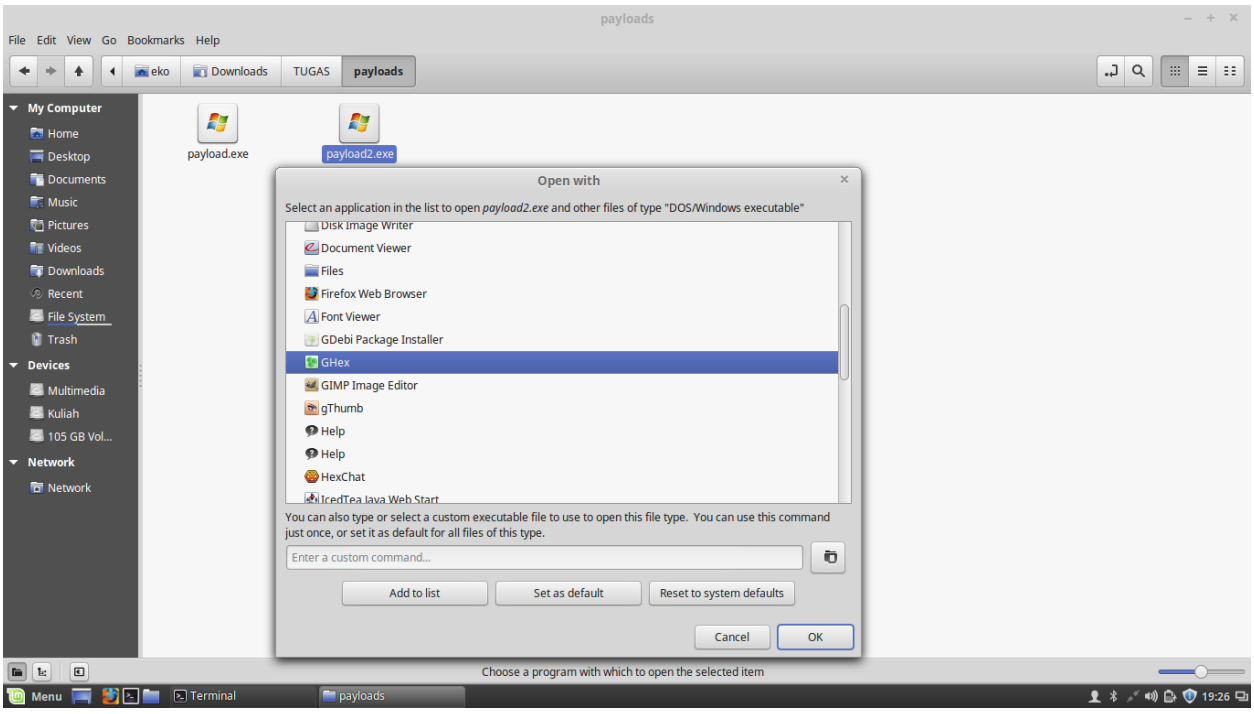


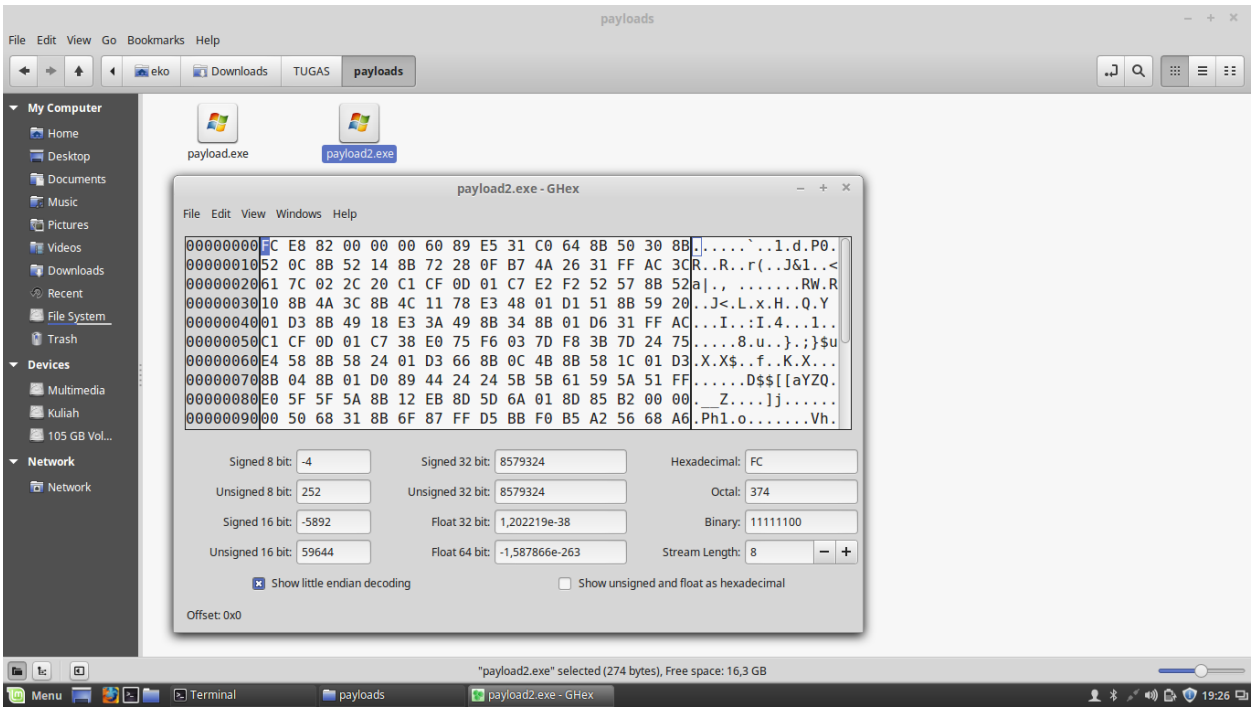


Didapatkan biner berupa 4D 5A 90 dari file tersebut dan huruf MZ.

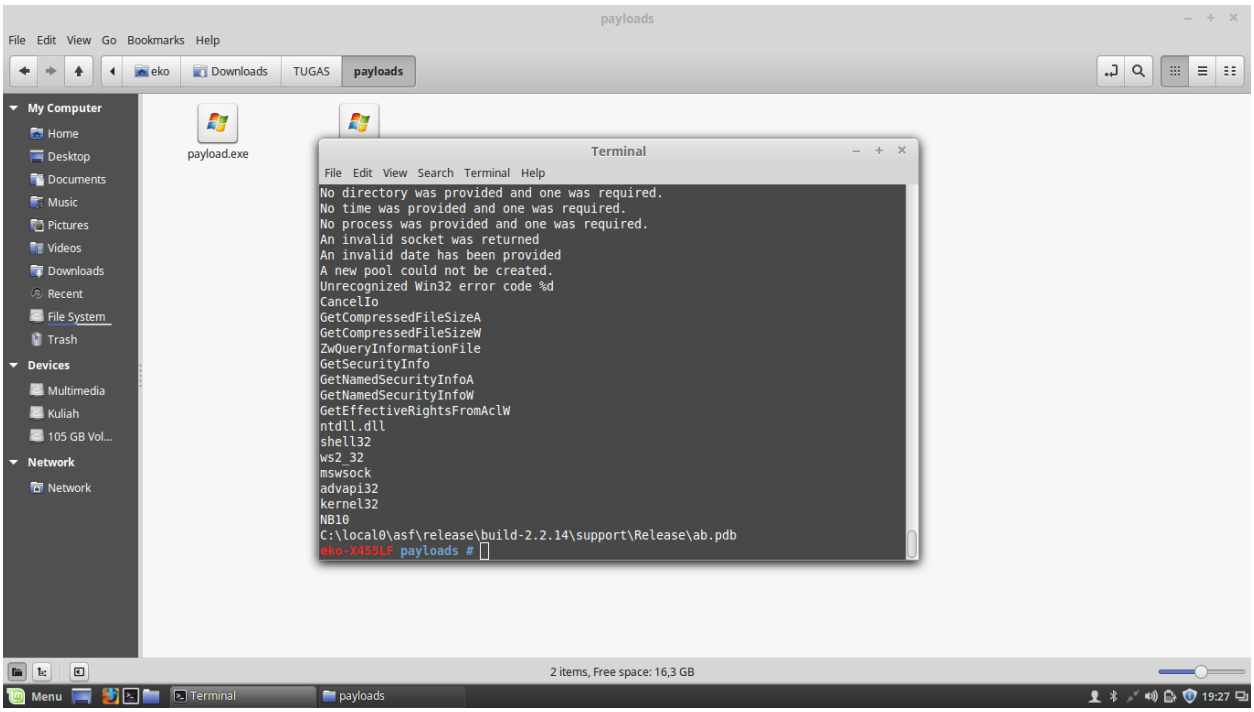


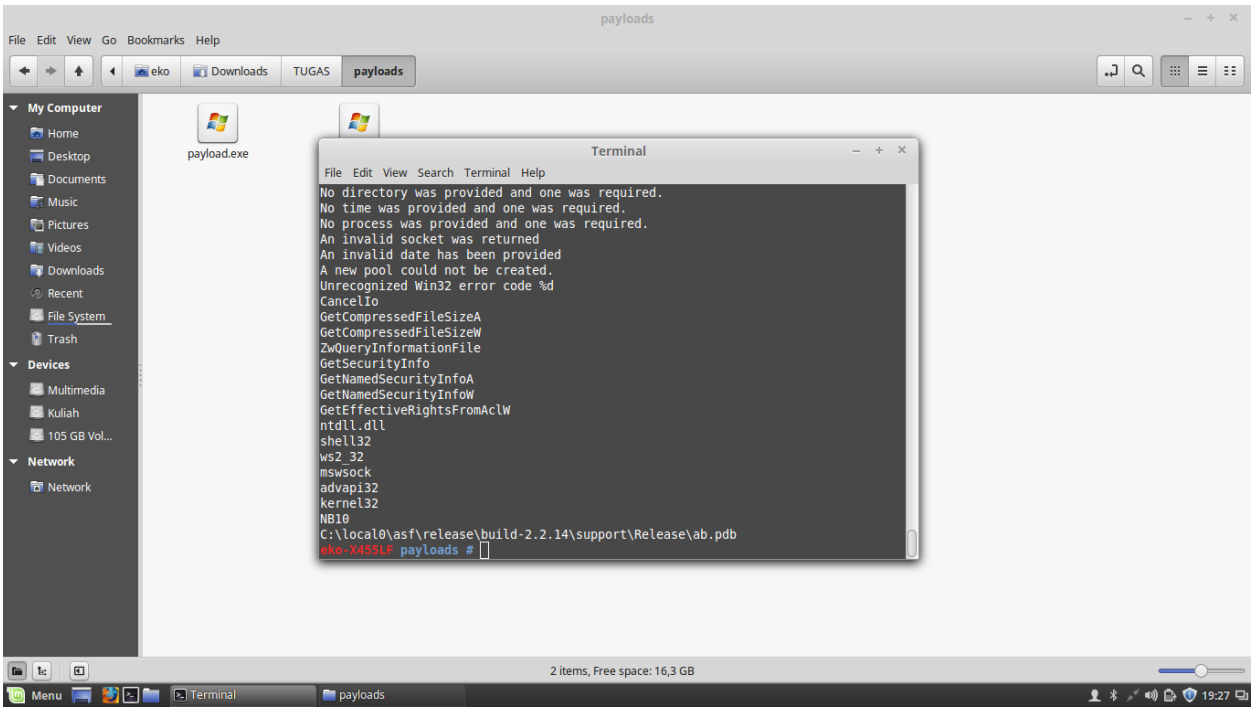
Dan sesuai dari list of signatures Wikipedia, kode 4D 5A atau MZ merupakan file berekstensi exe.



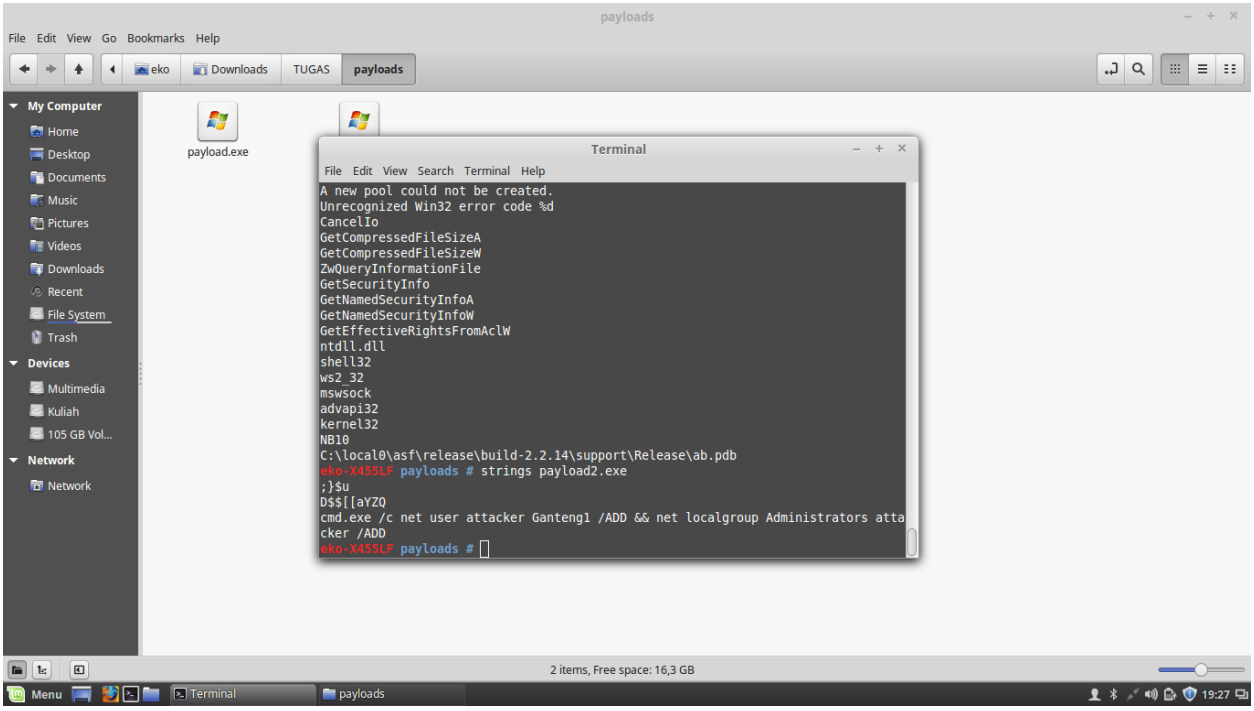


Kemudian membuka file berikutnya yaitu paylouds2.exe dengan tool Ghex. Dan didapatkan kode kembali.

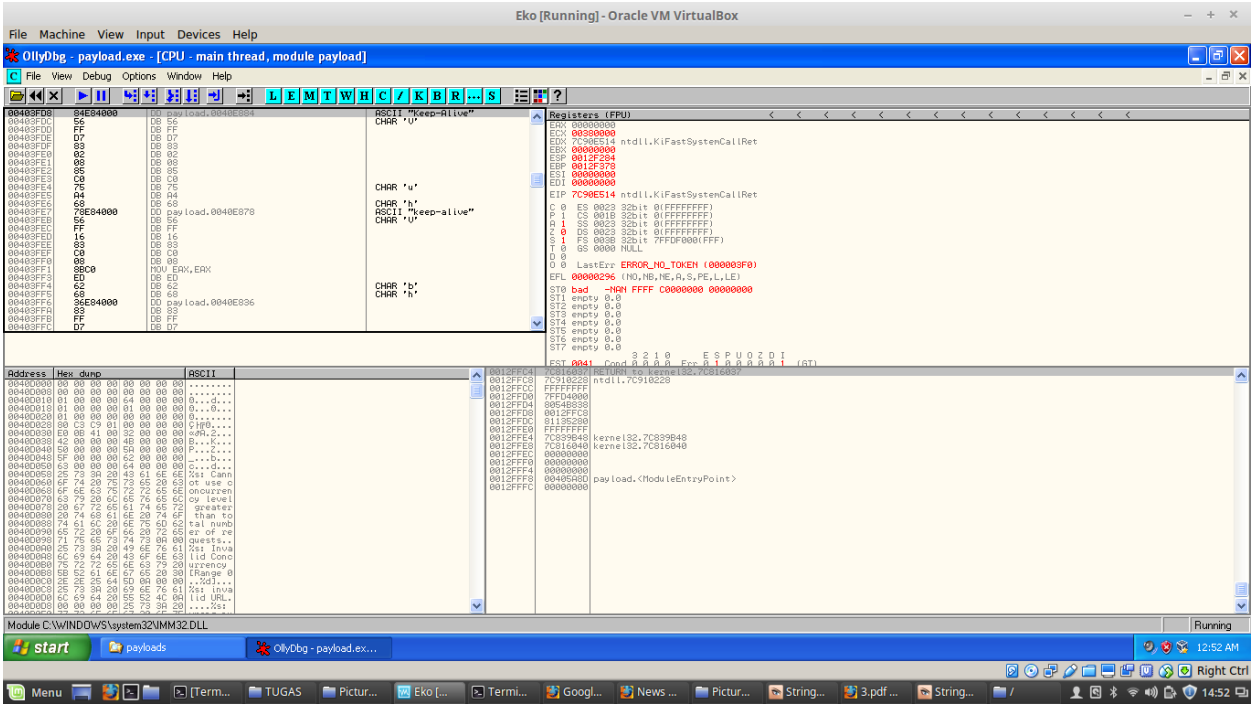




Kemudian menggunakan tool strings untuk menjalan paylouds.exe . Didapatkan beberapa informasi berupa program/perintah-perintah yang dilakukan oleh file paylouds.exe



Begitu pula dengan file paylouds2.exe, dan didapatkan informasi berupa net user attacker Ganteng1 dengan maksud admin membuat user baru dengan nama Ganteng1. Didapatkan juga informasi berupa net localgroup Administrators attacker dengan maksud local group dari admin yang diberi nama attacker.



Gambar di atas merupakan, analisis malware menggunakan tool Ollydbg dengan virtualisasi menggunakan windows xp dan didapatkan informasi berupa kode-kode.