TUGAS KEAMANAN JARINGAN KOMPUTER

NAMA: SYAMSUDIN
NIM: 09011281320012

UNIVERSITAS SRIWIJAYA
FAKULTAS ILMU KOMPUTER
JURUSAN SISTEM KOMPUTER

Alat

1. GHex
2. OllyDbg

Tugas

- Analisis cara kerja program payload.exe dan payload2.exe

Dasar Teori

Malware adalah sebuah software atau kode yang diciptakan oleh seseorang dengan tujuan jahat. Sebenarnya Malware itu adalah sebuah software atau program komputer, namun Malware dibuat dengan tujuan untuk merugikan orang lain. Malware dapat mengubah data (menghapus, menyembunyikan, dan mencuri), menghabiskan bandwith dan juga sumber daya lain tanpa seijin pemilik komputer yang tentunya akan merugikan orang lain. Contoh malware yaitu Virus, Worm, Trojan Horse dan Spyware.

Trojan Horse atau Kuda troya merupakan program perangkat lunak berbahaya yang bersembunyi di dalam program lain. Program ini memasuki komputer dengan bersembunyi di dalam program yang sah, seperti screen saver. Kemudian dia akan menaruh kode ke dalam sistem operasi yang memungkinkan hacker untuk mengakses komputer yang terinfeksi. Kuda troya biasanya tidak menyebar sendiri. Mereka disebar oleh virus, worm, atau perangkat lunak yang diunduh.

Percobaan

“Analisis cara kerja program payload.exe”

Menggunakan tools OllyDbg untuk mendapatkan informasi dari program “payload.exe”

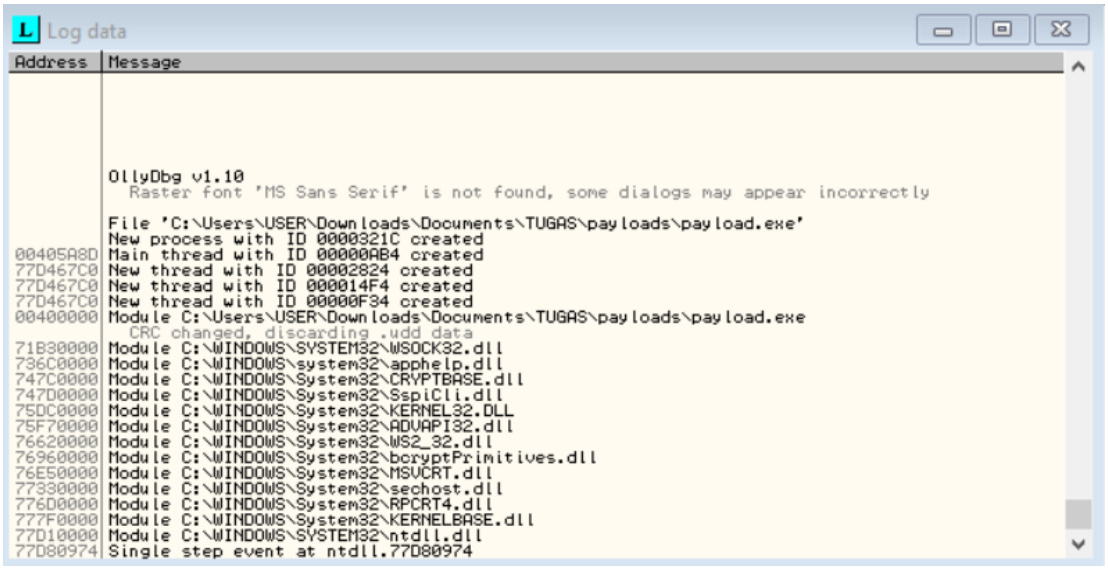

Figure 1

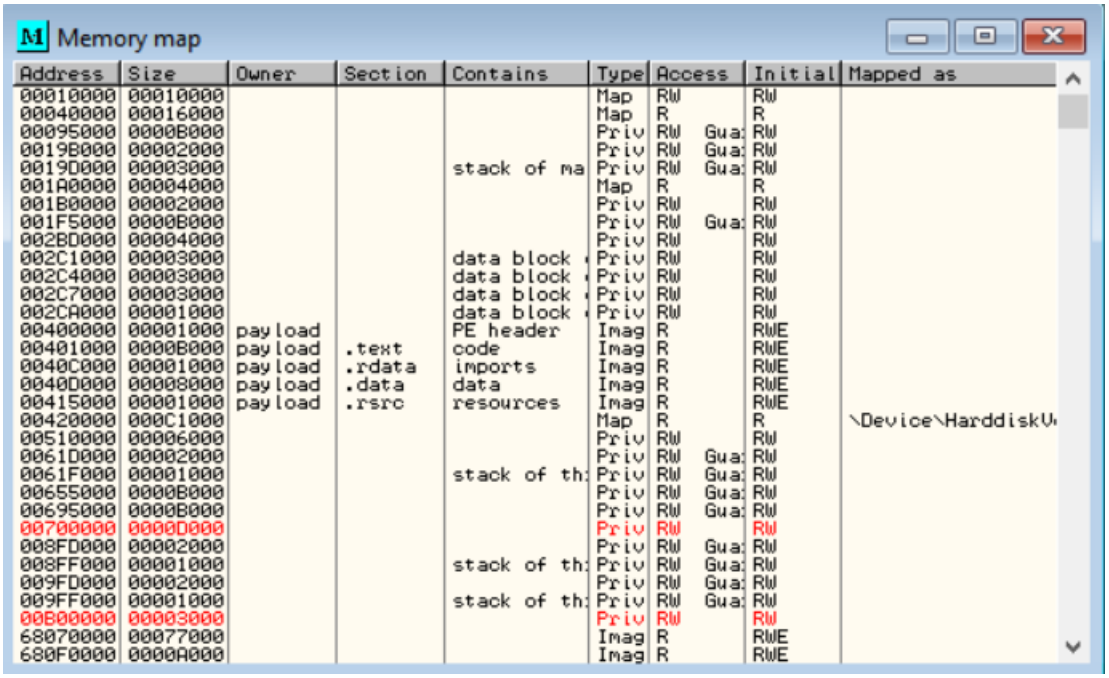

Figure 2

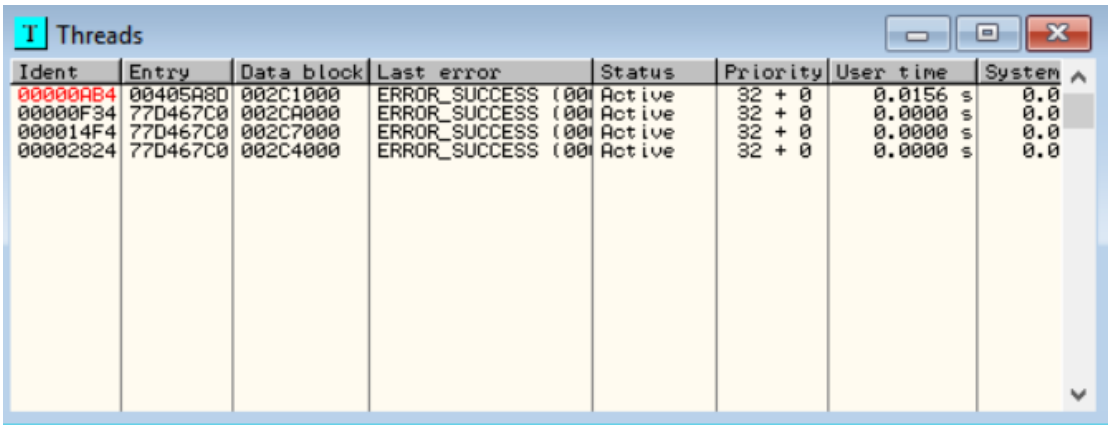

Figure 3

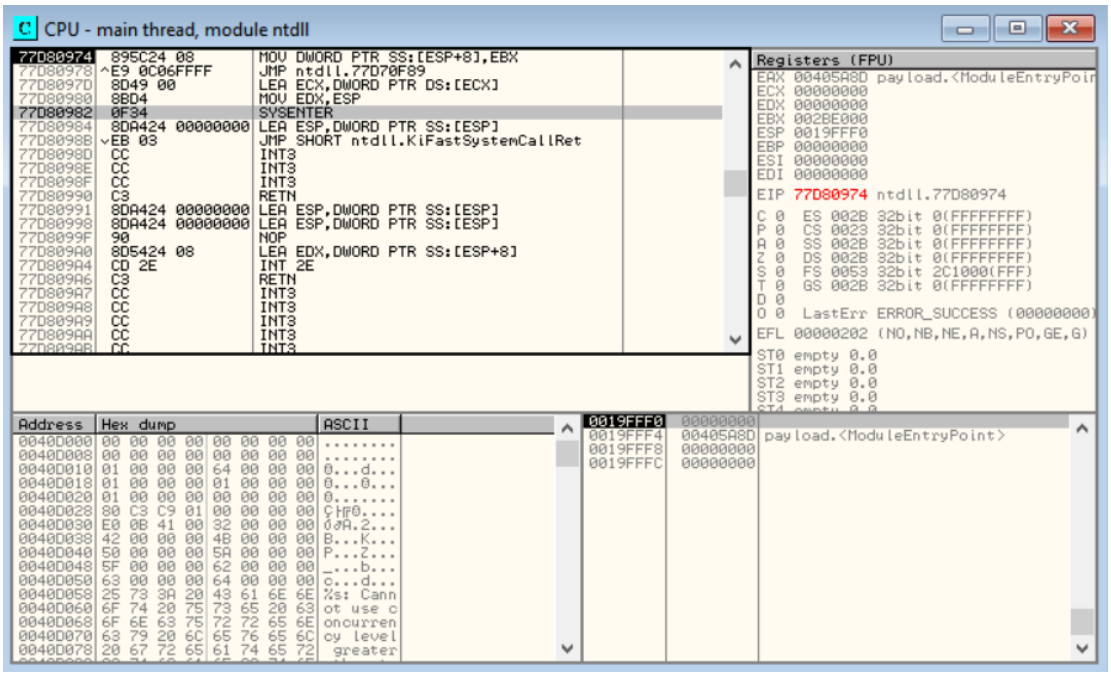

Figure 4

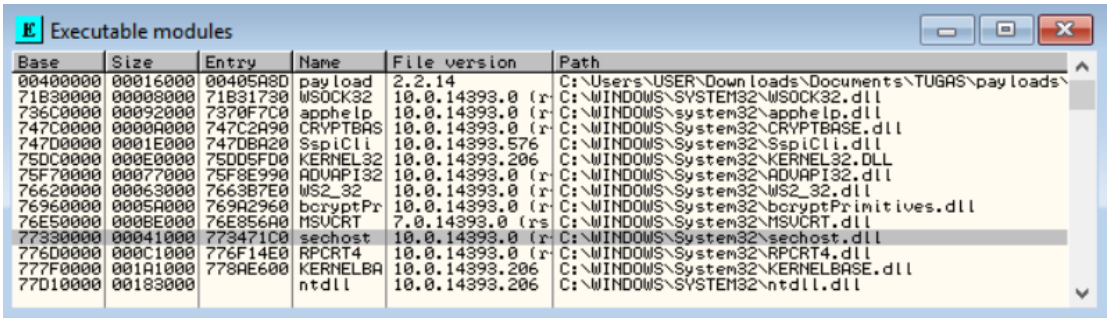

Figure 5

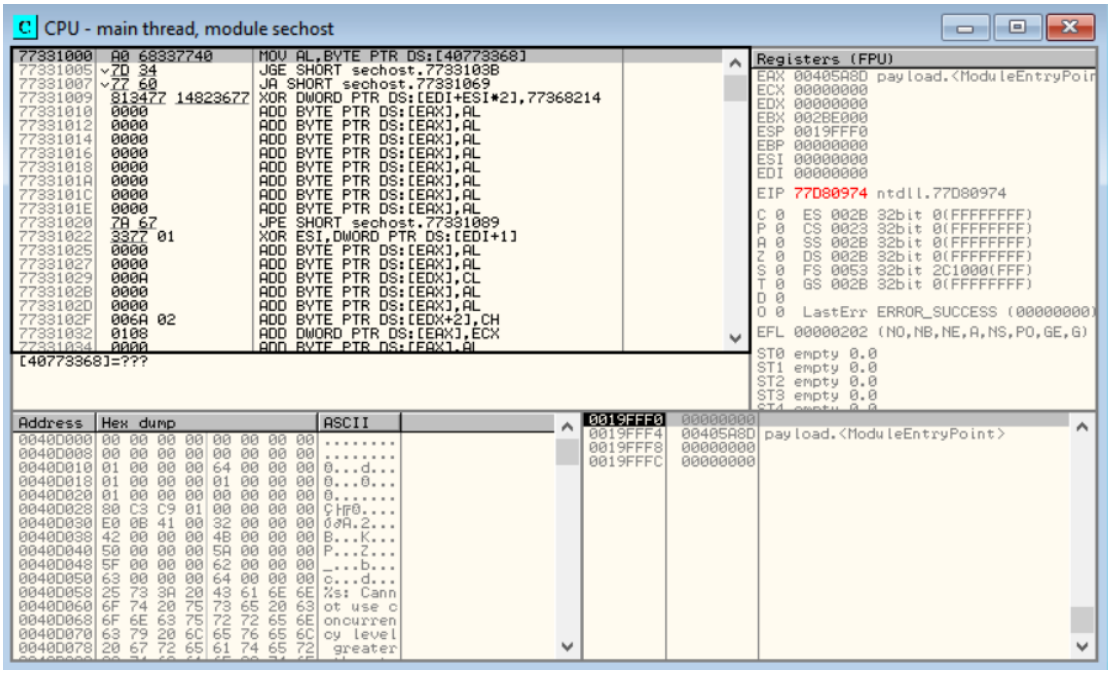

Figure 6

Menggunakan tools GHex untuk mendapatkan informasi dari program “payload.exe”

```
root@sam-VirtualBox:/home/sam/Downloads/TUGAS/payloads# ls
html  payload2.exe  payload.exe
root@sam-VirtualBox:/home/sam/Downloads/TUGAS/payloads# ghex payload.exe
```

Figure 7

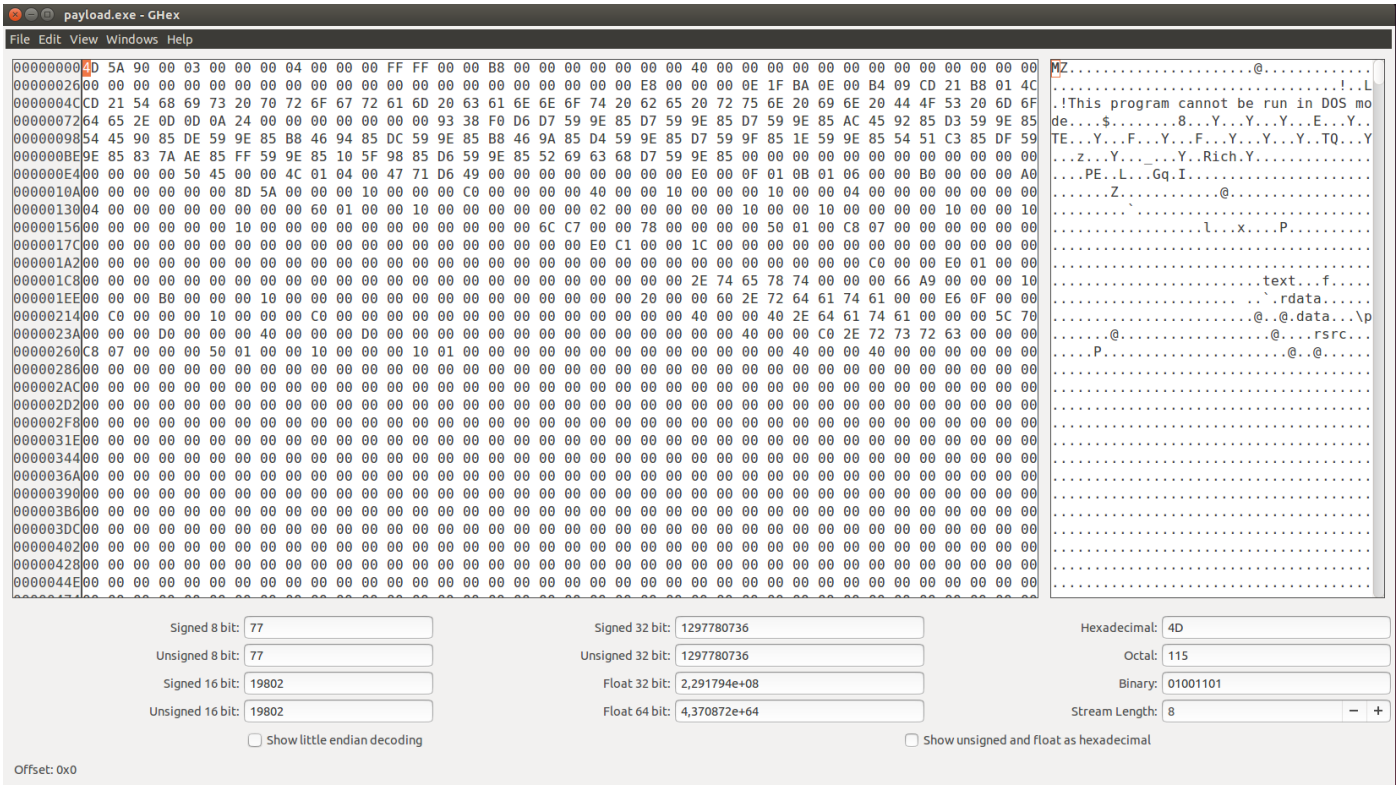

Figure 8

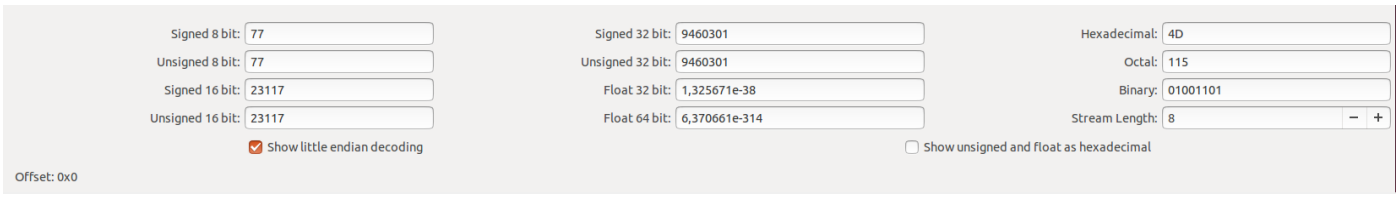

Figure 9

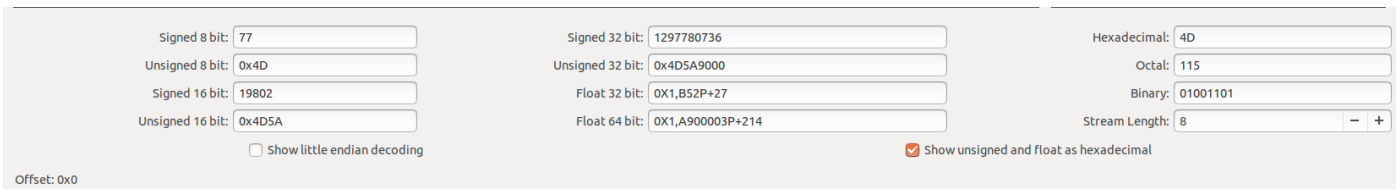

Figure 10

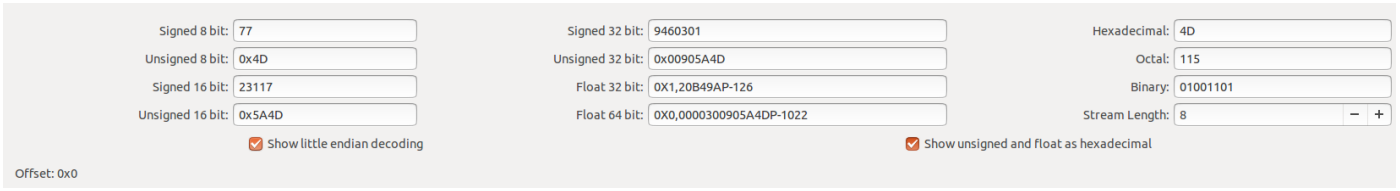

Figure 11

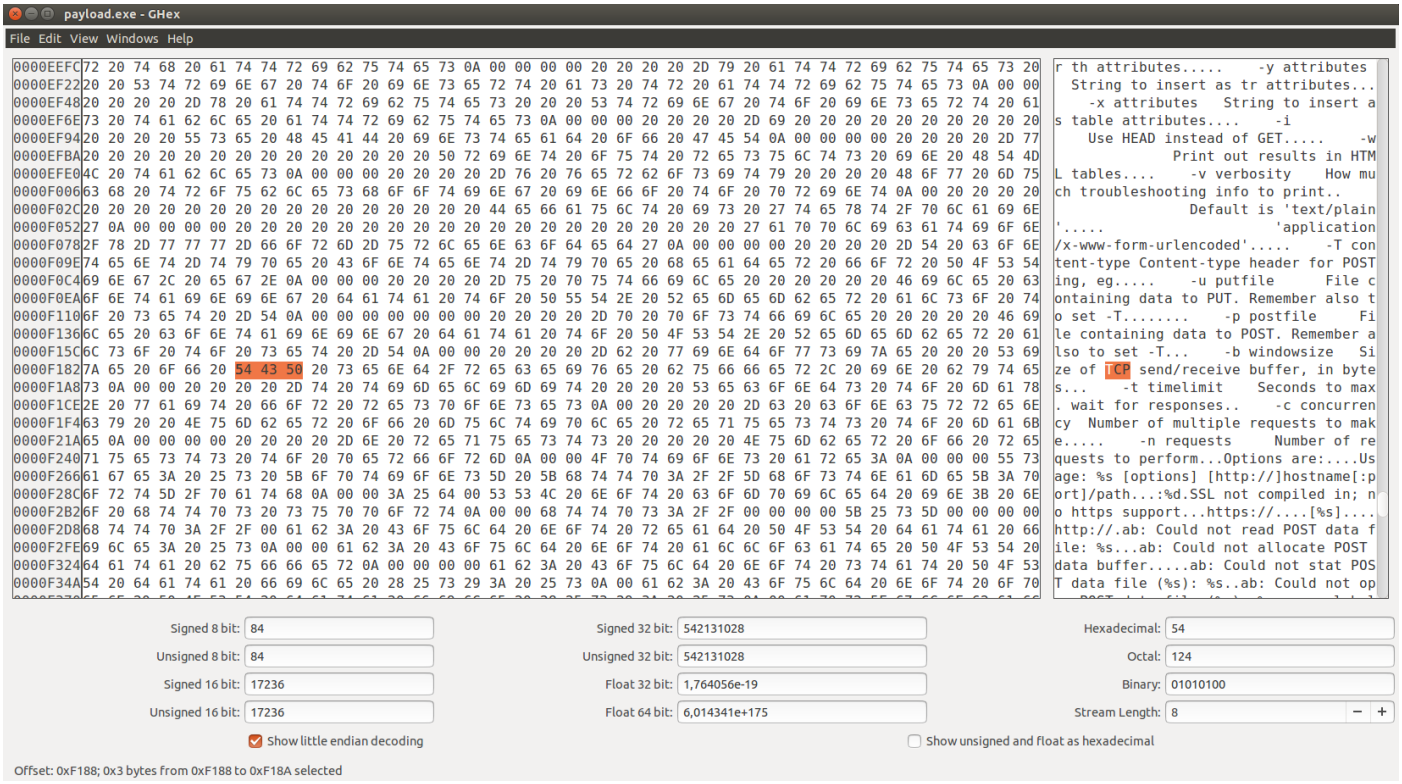

Figure 12

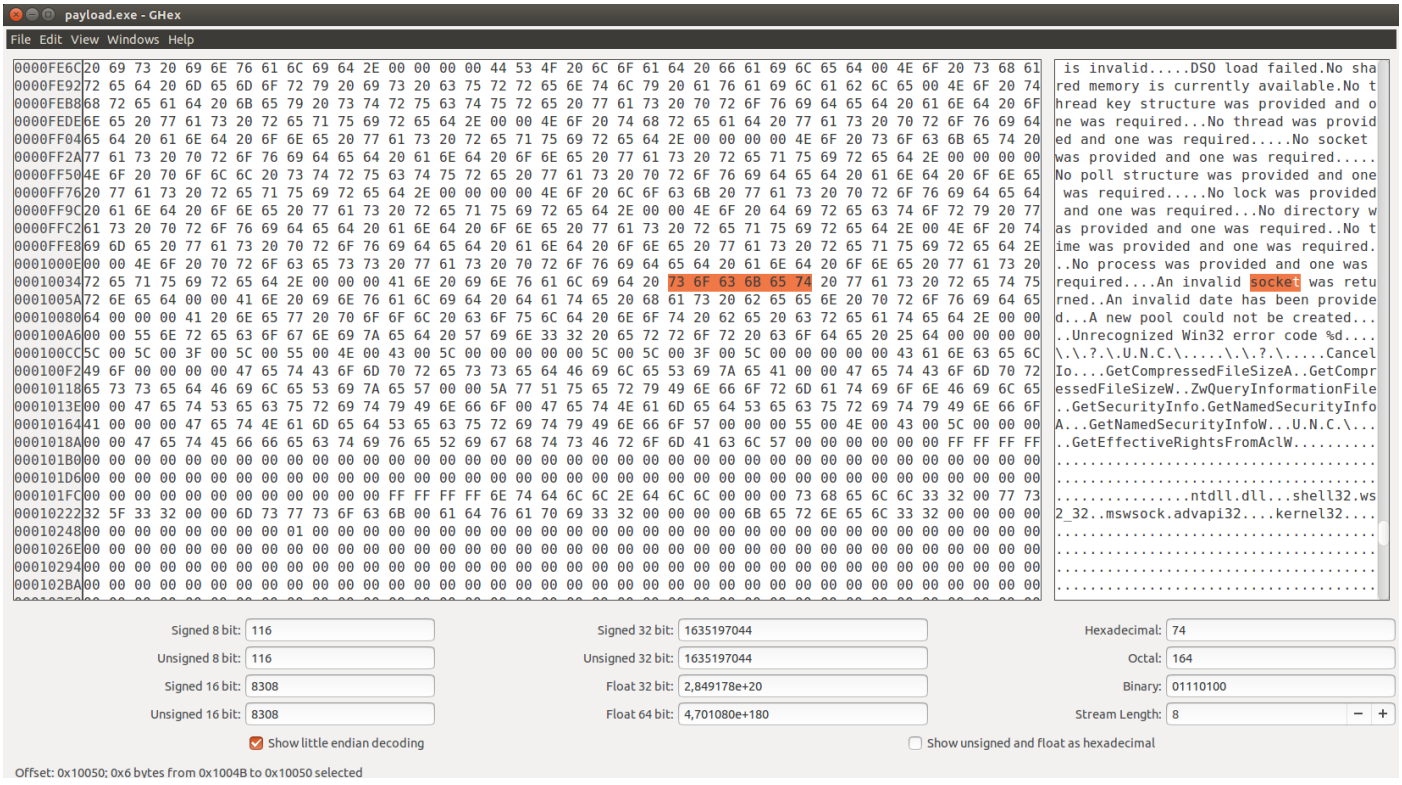

Figure 13

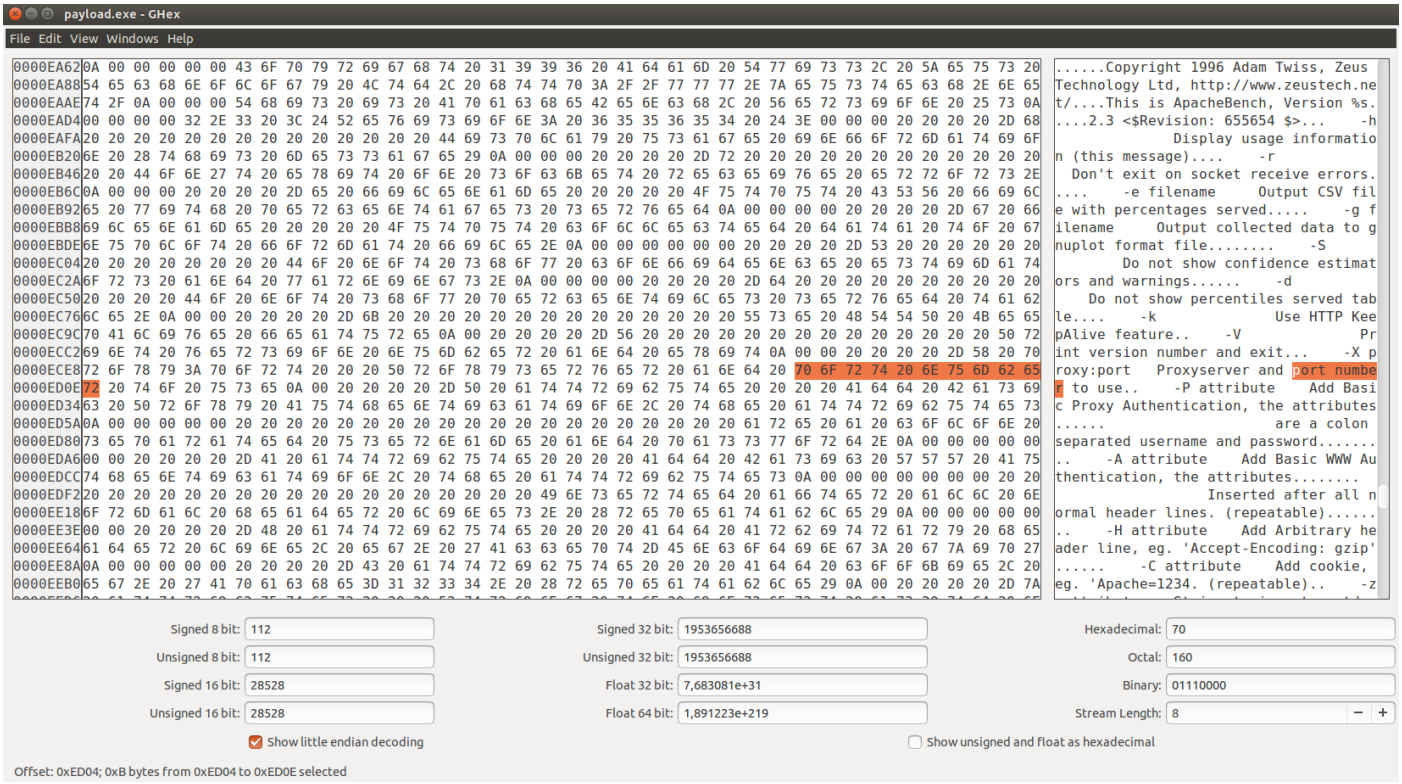

Figure 14

Dari kedua tools yang sudah digunakan yaitu OllyDbg dan GHex, diketahui bahwa program “payload.exe” beroperasi pada system operasi Windows, hal ini bisa diketahui dari melihat ekstensi dari program payload yaitu .exe, selain itu juga bisa dilihat pada (Figure 8) terdapat string “MZ” dengan offset 0x0 pada sky dum yang merupakan salah satu ciri khas dari setiap file .exe.

Program “payload.exe” beroperasi menggunakan port karena terdapat displayed string “port number” pada sky dum (Figure 14) yang mana port ini akan digunakan sebagai portal dalam melakukan ekploitasi, program ini menggunakan socket sebagai interface jaringan komunikasinya (Figure 13), socket sendiri terdiri dari beberapa elemen yaitu Protokol, Local IP, Local Port, Remote IP, Remote Port. Dikarenakan menggunakan socket berarti akan terjadi pertukaran data secara continue atau terus menerus. Adapun protocol yang digunakan dalam komunikasinya adalah protocol TCP (The Transmission Control Protocol) (Figure 12).

Pada (Figure 5) diketahui bahwa program "payload.exe" executable pada beberapa modul di komputer victim, yaitu pada WSOCK32 apphelp, CRYTBAS, SspiCli, KERNEL32, ADVAPI32, WS2_32, boryptOr, MSVCRT, sechost, RPCRT4, KERNELBA, ntdll. Pada modul atau dll seperti WSOCK32 yang menyediakan WinSock API. WinSock mendukung multiple stack protocol, interface, dan service provider. Ini yang dieksploit oleh program “payload.exe”. Dengan dapatnya melakukan eksekusi pada modul penting tersebut memungkinkan computer victim untuk dilakukan ekploitasi dan juga spy karena dapat melakukan remote access.

“Analisis cara kerja program payload2.exe”

Menggunakan tools OllyDbg untuk mendapatkan informasi dari program “payload2.exe”

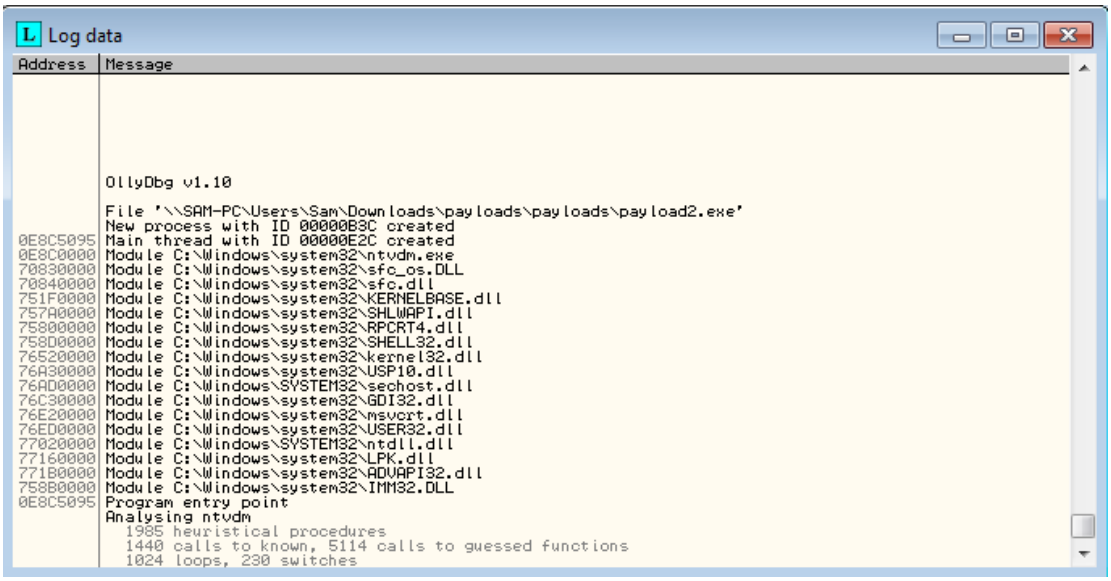

Figure 15

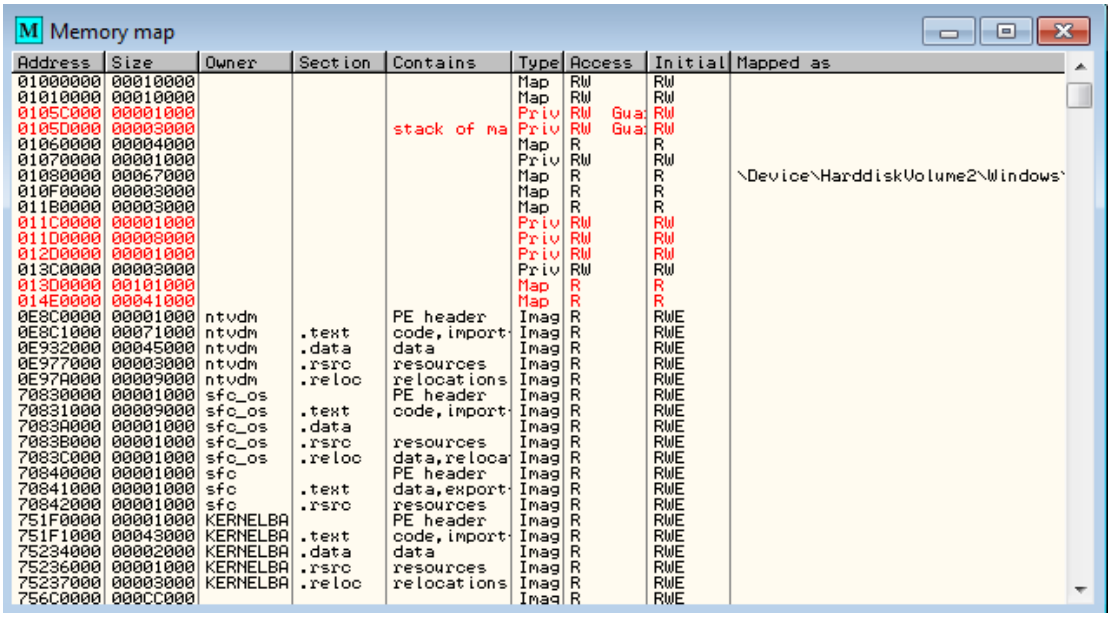

Figure 16

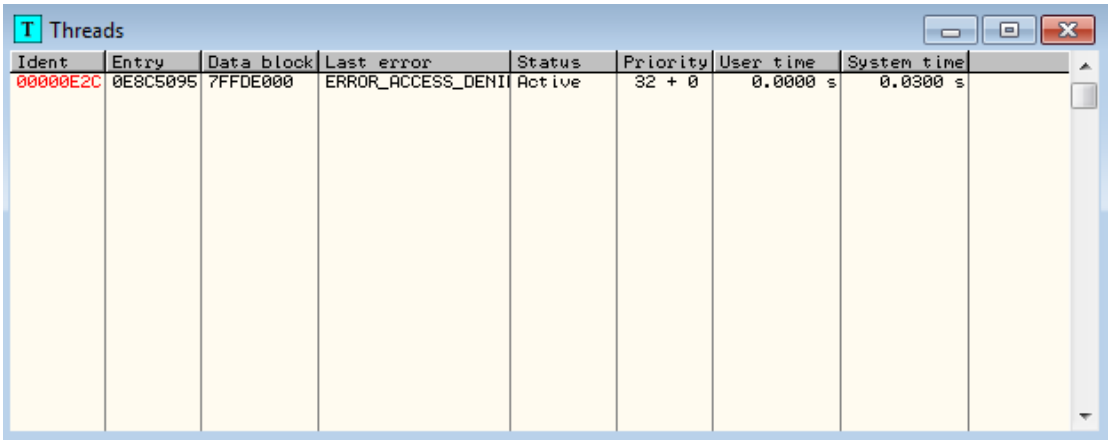

Figure 17

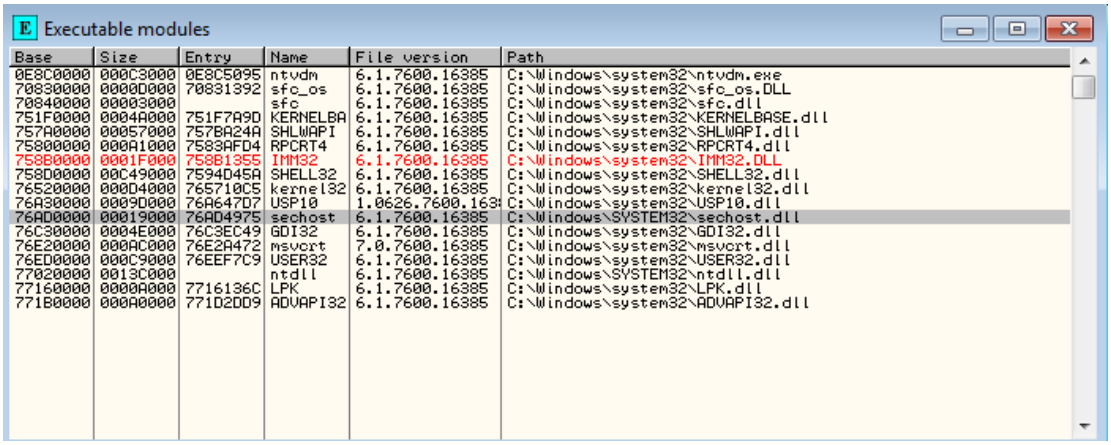

Figure 18

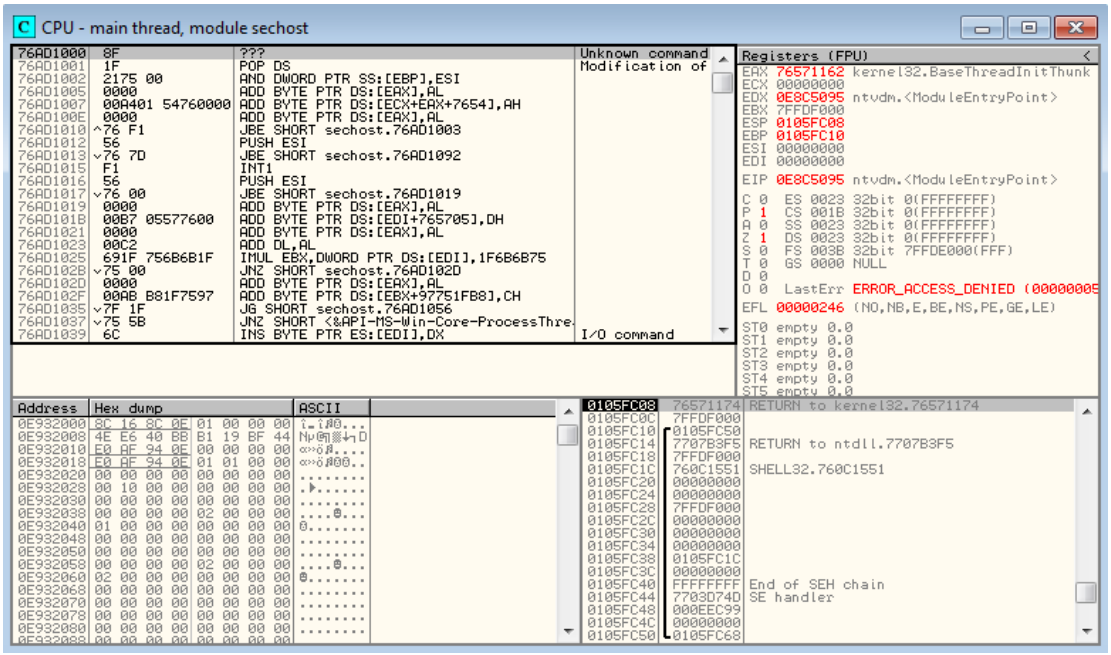

Figure 19

Menggunakan tools GHex untuk mendapatkan informasi dari program “payload2.exe”

```
root@sam-VirtualBox:/home/sam/Downloads/TUGAS/payloads# ls
html  payload2.exe  payload.exe
root@sam-VirtualBox:/home/sam/Downloads/TUGAS/payloads# ghex payload2.exe
```

Figure 20

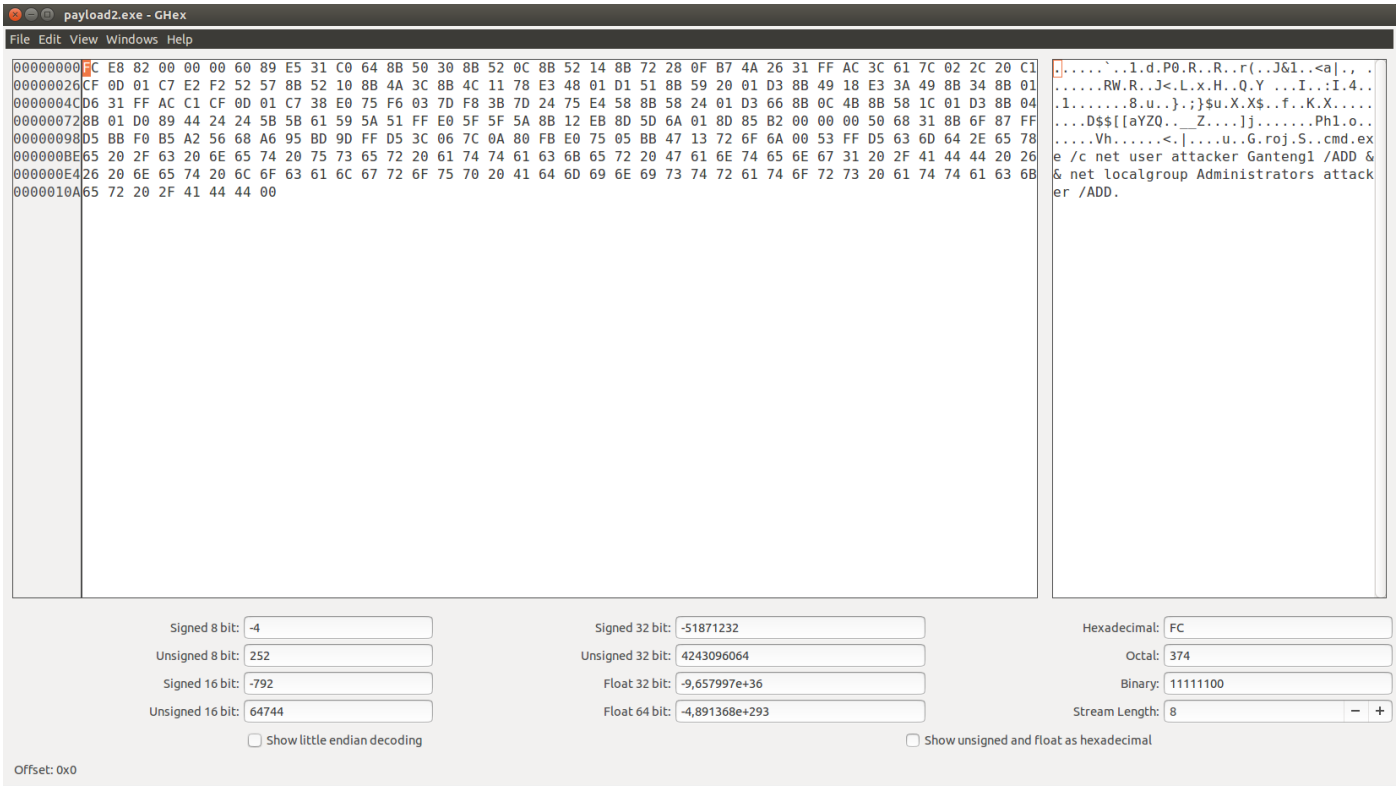

Figure 21

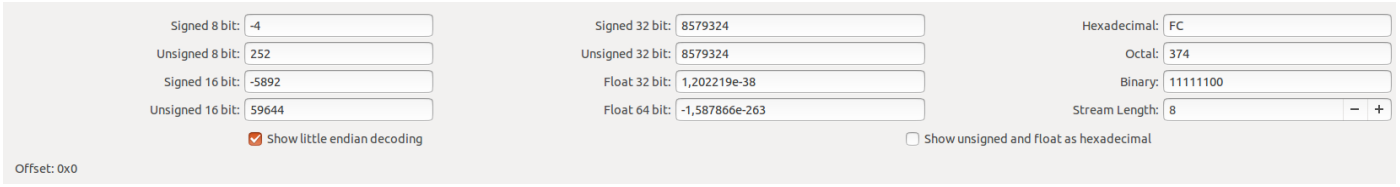

Figure 22

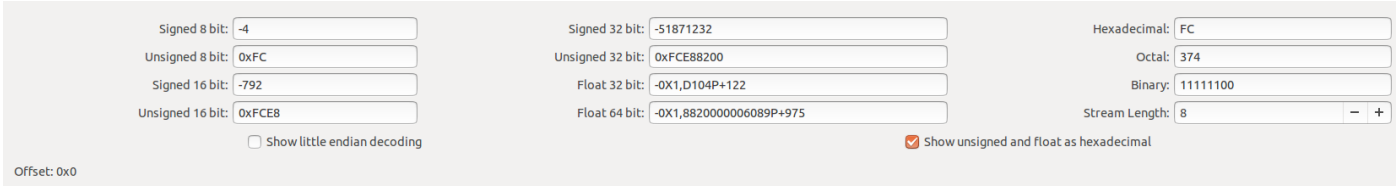

Figure 23

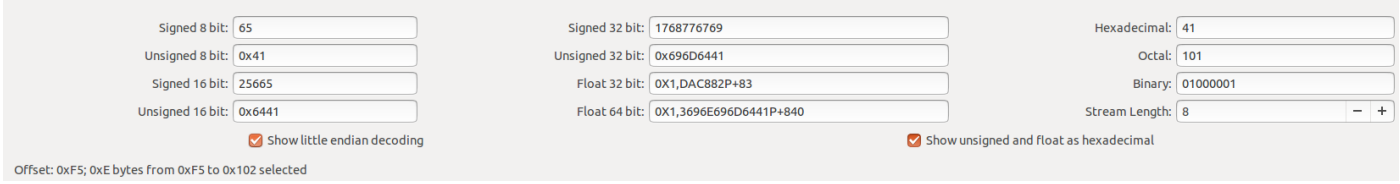

Figure 24

Pada (Figure 18) diketahui bahwa program "payload2.exe" executable pada beberapa modul di komputer victim, yaitu pada ntvdm, sfc_os, sfc, KERNELBA, SHLWAPI, RPCRT4, IMM32, SHELL32, kernel32, USP10, sechost, GDI32, msvort, USER32, ntdll, LPK, ADVAPI32. Melihat dari modul-modul yang executable seperti USER32 dan juga melihat dari displayed string “Administrator attacker” pada sky dum (Figure 21) malware payload2.exe ini dapat melakukan manipulasi atau eksploitasi system administrator pada komputer victim.

Daftar Pustaka

- Anonim, 2013, Apa itu Socket dan apa Fungsinya dalam Jaringan?, [online], (http://akfive.blogspot.co.id/2013/04/apa-itu-socket-dan-apa-fungsinya-dalam.html, diakses tanggal 5 April 2017)
- Anonim, 2014, Perbedaan Malware, Virus, Trojan, Spyware, dan Worm, [online], (https://www.maxmanroe.com/perbedaan-malware-virus-trojan-spyware-dan-worm.html, diakses tanggal 5 April 2017)
- Anonim, 2015, Cara mencegah dan menghapus virus dan malware lainnya, [online], (https://support.microsoft.com/id-id/help/129972/how-to-prevent-and-remove-viruses-and-other-malware, diakses tanggal 5 April 2017)