Muhammad Azriansyah 09011281320006 Keamanan Jaringan Komputer

Analisis Payload Malware dengan Windows dan Linux

Malware (Malicious Software) adalah suatu program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer. Malware dapat menginfeksi banyak komputer dengan masuk melalui email, download internet, atau program yang terinfeksi.

Malware bisa menyebabkan kerusakan pada sistem komputer dan memungkinkan juga terjadi pencurian data / informasi. Hal yang pada umumnya terjadi penyebab malware adalah mendownload software dari tempat ilegal yang disisipan malware. Malware mencakup virus, worm, trojan horse, sebagian besar rootkit, spyware, adware yang tidak jujur, serta software-software lain yang berbahaya dan tidak diinginkan oleh pengguna PC.

Pada website sendiri terkadang bisa terjangkit malware, hal ini bisa terjadi jika pengguna melakukan download theme website secara ilegal, hal itu dapat menyebabkan data dan informasi yang ada di website jebol, terkadang juga bisa menyebabkan server website menjadi down karena aktifitas yang mencurigakan tersebut.

Hal yang harus dilakukan untuk mencegah malware adalah tidak melakukan aktifitas ilegal, sebagai contoh tidak melakukan download resource dan aplikasi di situs yang tidak terverifikasi atau ilegal, hal ini karena biasanya peluang adanya virus malware lebih besar terjangkit pada suatu aplikasi yang diunduh di website tersebut.

TUGAS

Lakukan analisis terhadap 2 file payload tersebut

1. payload.exe

2. payload2.exe

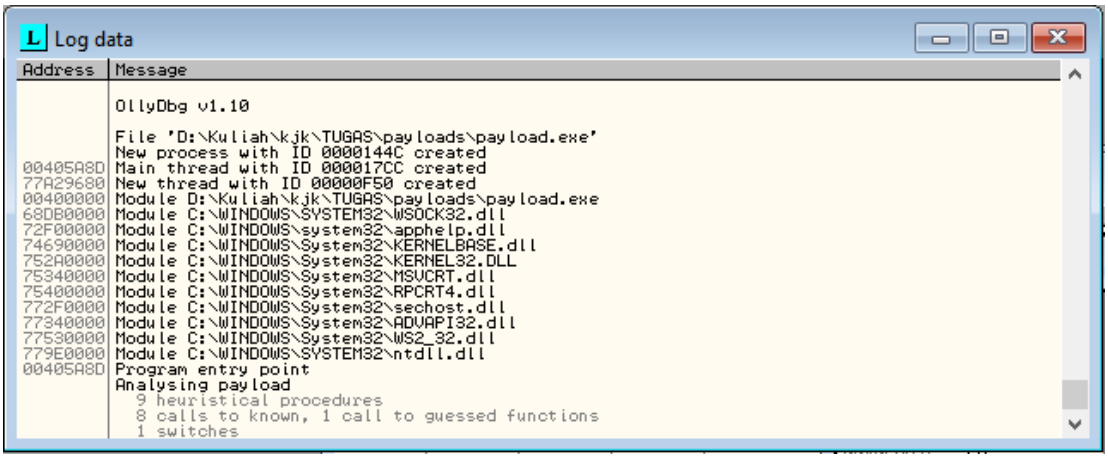
analisis, proses kerja dan skema dari payload tersebut, menggunakan tools:

1. ghex,hexdump,strings (linux)

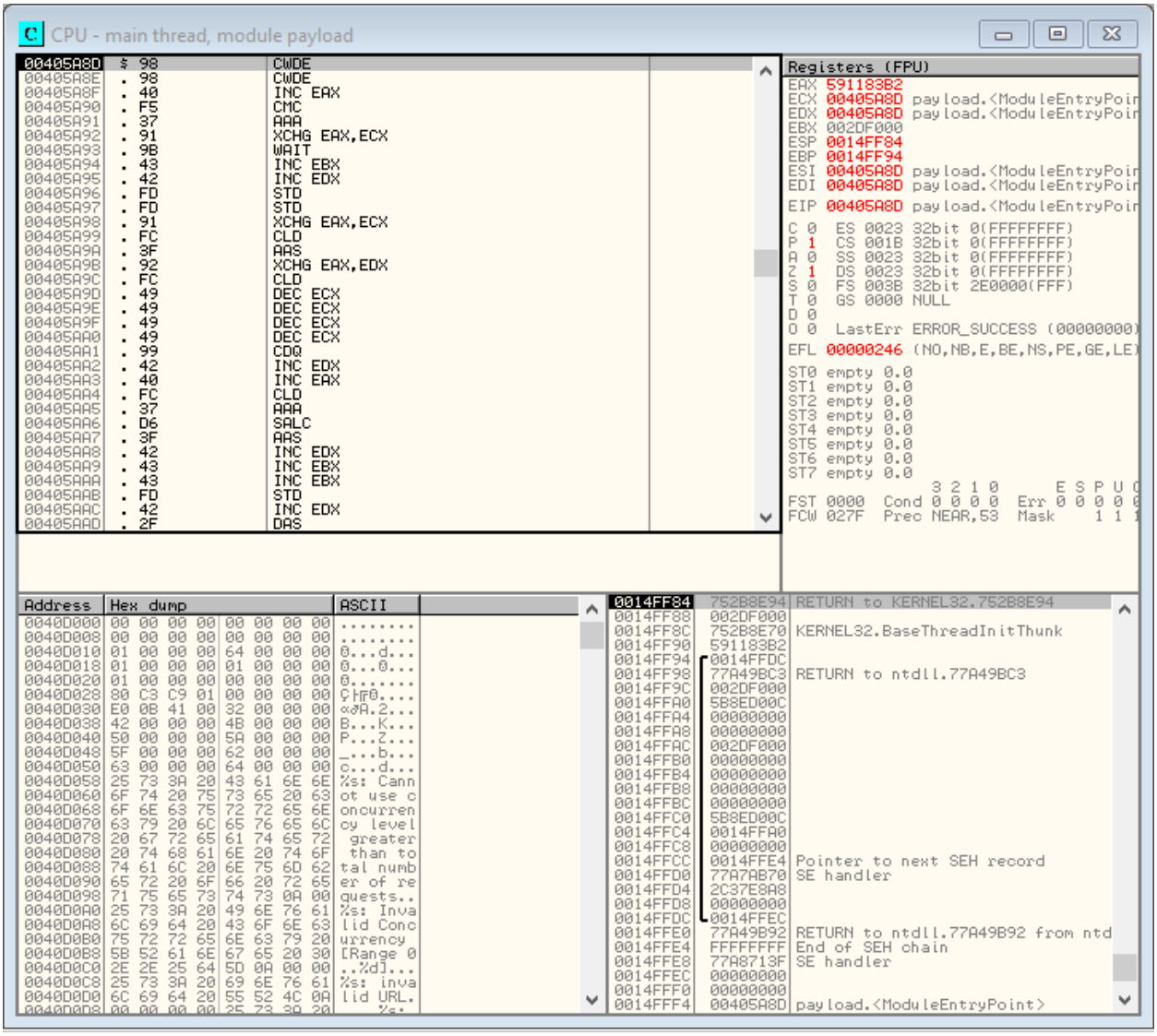
2. ollydbg(win),ida pro(linux,win)

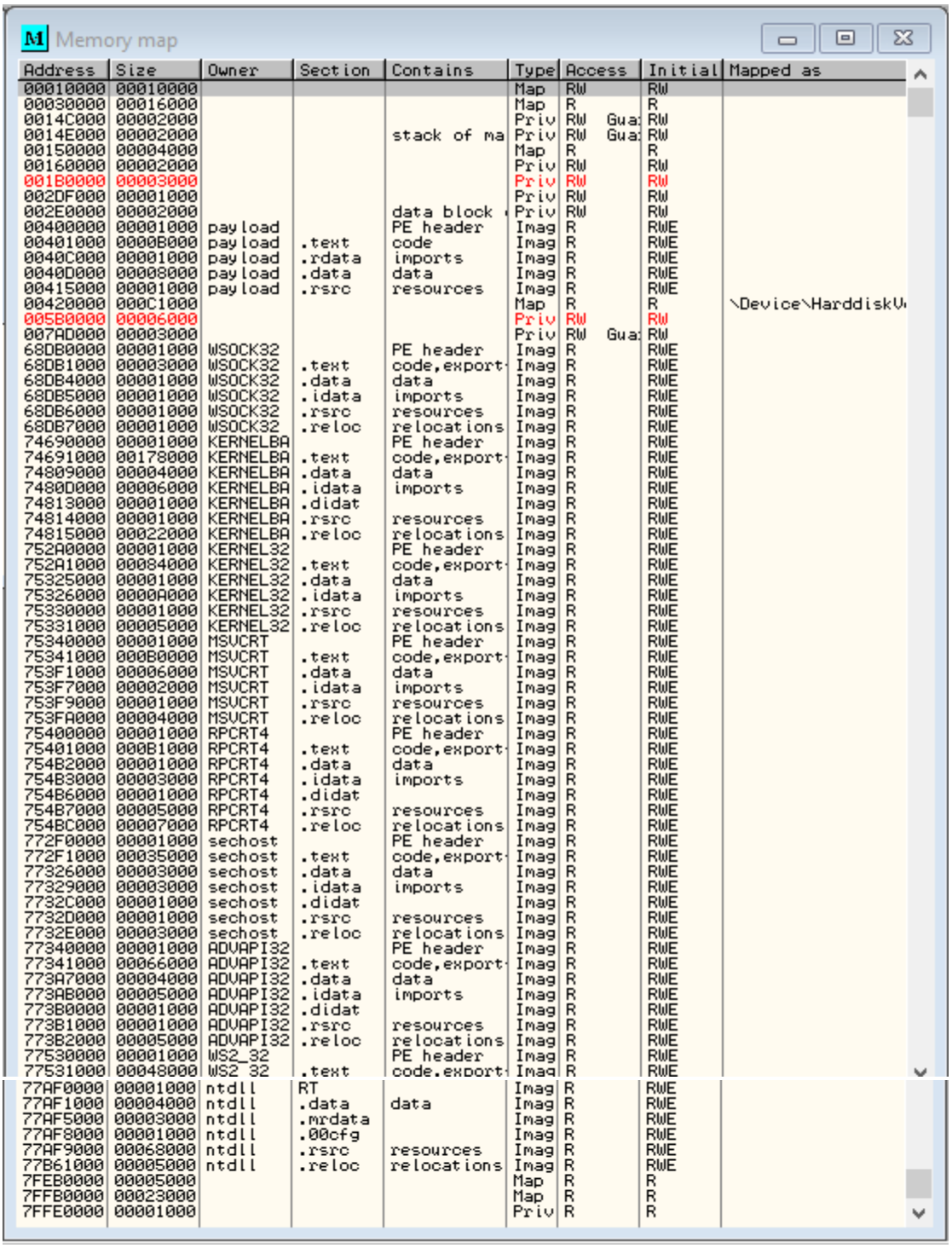
Untuk analisis dinamis lanjut, tool yang digunakan adalah OllyDbg. Ada dua macam cara melakukan debugging dengan OllyDbg, menjalankan program dengan debugger dan menempelkan (attach) debugger pada program yang sedang berjalan.

Hasil yang di dapatkan menggunakan tools Ollydbg pada windows



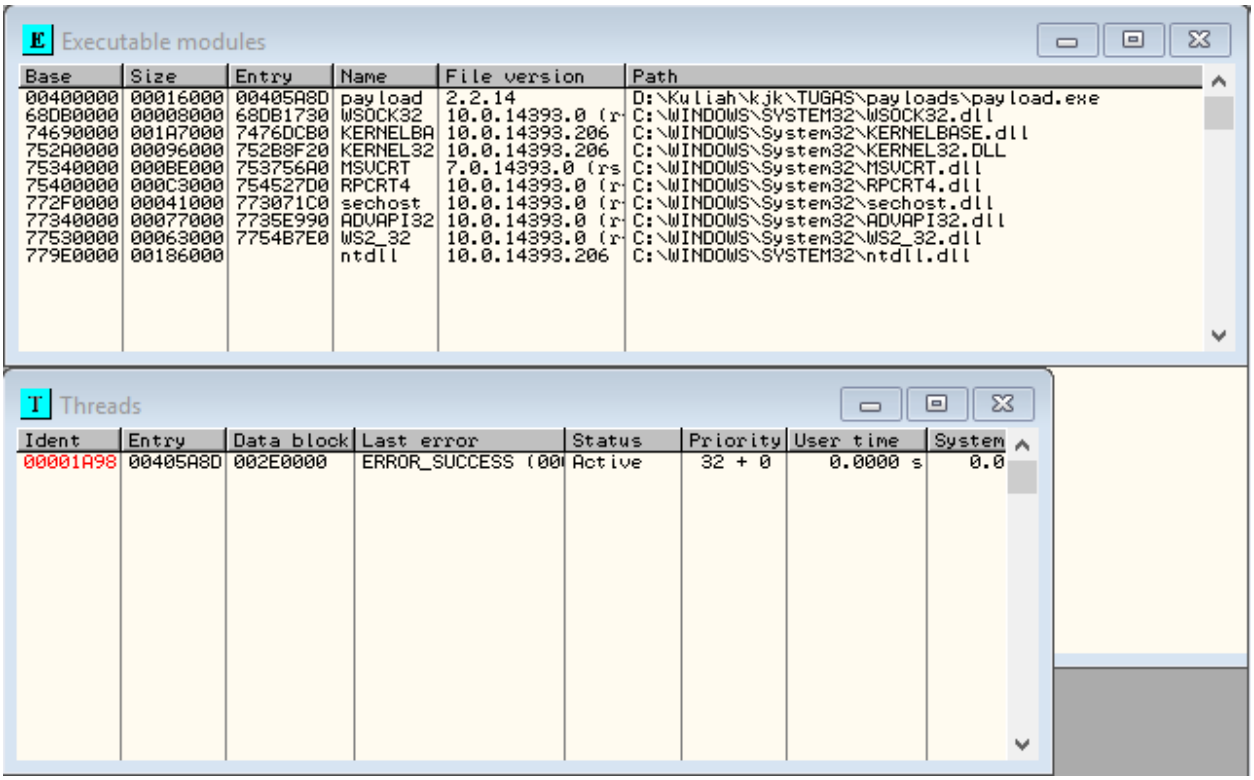
Pada aplikasi Ollydb pada log data ditemukan 9 prosedur heuristik, 8 calls to known, 1 call to guessed functions dan 1 switches.


CPU - main thread, module payload
00405A8D $ 98 CWDE
00405A8E . 98 CWDE
00405A8F . 40 INC EAX
00405A90 . F5 CMC
00405A91 . 37 AAA
00405A92 . 91 XCHG EAX,ECX
00405A93 . 9B WAIT
00405A94 . 43 INC EBX
00405A95 . 42 INC EDX
00405A96 . FD STD
00405A97 . FD STD
00405A98 . 91 XCHG EAX,ECX
00405A99 . FC CLD
00405A9A . 3F AAS
00405A9B . 92 XCHG EAX,EDX
00405A9C . FC CLD
00405A9D . 49 DEC ECX
00405A9E . 49 DEC ECX
00405A9F . 49 DEC ECX
00405AA0 . 49 DEC ECX
00405AA1 . 99 CDQ
00405AA2 . 42 INC EDX
00405AA3 . 40 INC EAX
00405AA4 . FC CLD
00405AA5 . 37 AAA
00405AA6 . D6 SALC
00405AA7 . 3F AAS
00405AA8 . 42 INC EDX
00405AA9 . 43 INC EBX
00405AAA . 43 INC EBX
00405AAB . FD STD
00405AAC . 42 INC EDX
00405AAD . 2F DAS
Registers (FPU)
EAX 591183B2
ECX 00405A8D payload.<ModuleEntryPoin
EDX 00405A8D payload.<ModuleEntryPoin
EBX 002DF000
ESP 0014FF84
EBP 0014FF94
ESI 00405A8D payload.<ModuleEntryPoin
EDI 00405A8D payload.<ModuleEntryPoin
EIP 00405A8D payload.<ModuleEntryPoin
C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 2E0000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
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
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 ....d...
0040D018 01 00 00 00 01 00 00 00 ....0...
0040D020 01 00 00 00 00 00 00 00 ....
0040D028 80 C3 C9 01 00 00 00 00 ....
0040D030 E0 0B 41 00 32 00 00 00 ..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:
0014FF84 752B8E94 RETURN to KERNEL32.752B8E94
0014FF88 002DF000
0014FF8C 752B8E70 KERNEL32.BaseThreadInitThunk
0014FF90 591183B2
0014FF94 0014FFDC
0014FF98 77A49BC3 RETURN to ntdll.77A49BC3
0014FF9C 002DF000
0014FFA0 5B8ED00C
0014FFA4 00000000
0014FFA8 00000000
0014FFAC 002DF000
0014FFB0 00000000
0014FFB4 00000000
0014FFB8 00000000
0014FFBC 00000000
0014FFC0 5B8ED00C
0014FFC4 0014FFA0
0014FFC8 00000000
0014FFCC 0014FFE4 Pointer to next SEH record
0014FFD0 77A7AB70 SE handler
0014FFD4 2C37E8A8
0014FFD8 00000000
0014FFDC 0014FFEC
0014FFE0 77A49B92 RETURN to ntdll.77A49B92 from ntd
0014FFE4 FFFFFFFF End of SEH chain
0014FFE8 77A8713F SE handler
0014FFEC 00000000
0014FFF0 00000000
0014FFF4 00405A8D payload.<ModuleEntryPoint>

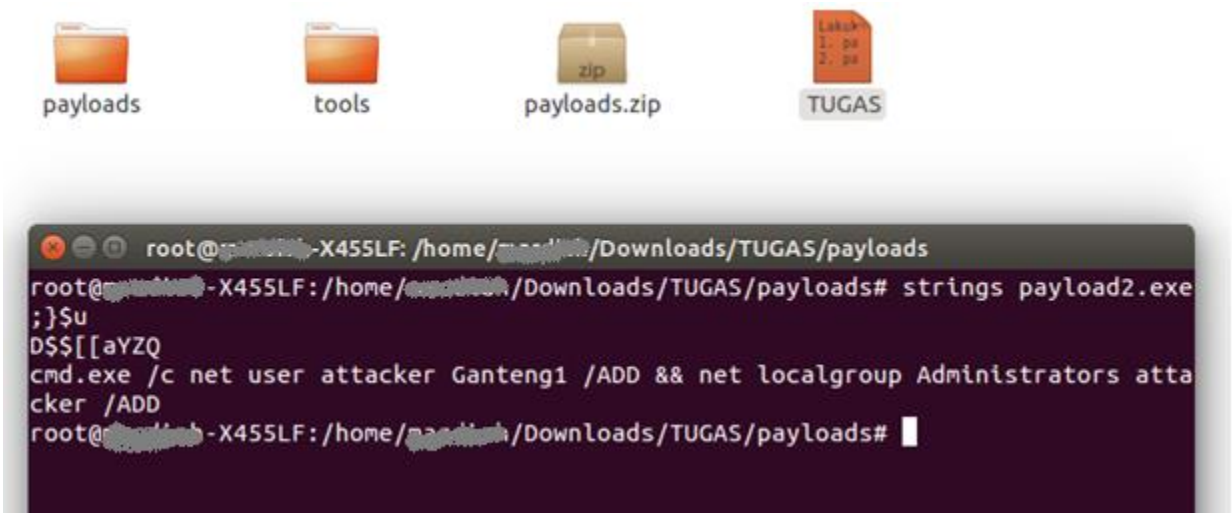


Memory map

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	RW	RW	
00030000	00016000				Map	R	R	
0014C000	00002000				Priv	RW Gua	RW	
0014E000	00002000			stack of ma	Priv	RW Gua	RW	
00150000	00004000				Map	R	R	
00160000	00002000				Priv	RW	RW	
001B0000	00003000				Priv	RW	RW	
002DF000	00001000				Priv	RW	RW	
002E0000	00002000			data block	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	
00420000	000C1000				Map	R	R	\Device\HarddiskV
005B0000	00006000				Priv	RW	RW	
007AD000	00003000				Priv	RW Gua	RW	
68DB0000	00001000	WSOCK32		PE header	Imag	R	RWE	
68DB1000	00003000	WSOCK32	.text	code,export	Imag	R	RWE	
68DB4000	00001000	WSOCK32	.data	data	Imag	R	RWE	
68DB5000	00001000	WSOCK32	.idata	imports	Imag	R	RWE	
68DB6000	00001000	WSOCK32	.rsrc	resources	Imag	R	RWE	
68DB7000	00001000	WSOCK32	.reloc	relocations	Imag	R	RWE	
74690000	00001000	KERNELBA		PE header	Imag	R	RWE	
74691000	00178000	KERNELBA	.text	code,export	Imag	R	RWE	
74809000	00004000	KERNELBA	.data	data	Imag	R	RWE	
7480D000	00006000	KERNELBA	.idata	imports	Imag	R	RWE	
74813000	00001000	KERNELBA	.didat		Imag	R	RWE	
74814000	00001000	KERNELBA	.rsrc	resources	Imag	R	RWE	
74815000	00022000	KERNELBA	.reloc	relocations	Imag	R	RWE	
752A0000	00001000	KERNEL32		PE header	Imag	R	RWE	
752A1000	00084000	KERNEL32	.text	code,export	Imag	R	RWE	
75325000	00001000	KERNEL32	.data	data	Imag	R	RWE	
75326000	0000A000	KERNEL32	.idata	imports	Imag	R	RWE	
75330000	00001000	KERNEL32	.rsrc	resources	Imag	R	RWE	
75331000	00005000	KERNEL32	.reloc	relocations	Imag	R	RWE	
75340000	00001000	MSVCRT		PE header	Imag	R	RWE	
75341000	000B0000	MSVCRT	.text	code,export	Imag	R	RWE	
753F1000	00006000	MSVCRT	.data	data	Imag	R	RWE	
753F7000	00002000	MSVCRT	.idata	imports	Imag	R	RWE	
753F9000	00001000	MSVCRT	.rsrc	resources	Imag	R	RWE	
753FA000	00004000	MSVCRT	.reloc	relocations	Imag	R	RWE	
75400000	00001000	RPCRT4		PE header	Imag	R	RWE	
75401000	000B1000	RPCRT4	.text	code,export	Imag	R	RWE	
754B2000	00001000	RPCRT4	.data	data	Imag	R	RWE	
754B3000	00003000	RPCRT4	.idata	imports	Imag	R	RWE	
754B6000	00001000	RPCRT4	.didat		Imag	R	RWE	
754B7000	00005000	RPCRT4	.rsrc	resources	Imag	R	RWE	
754BC000	00007000	RPCRT4	.reloc	relocations	Imag	R	RWE	
772F0000	00001000	sechost		PE header	Imag	R	RWE	
772F1000	00035000	sechost	.text	code,export	Imag	R	RWE	
77326000	00003000	sechost	.data	data	Imag	R	RWE	
77329000	00003000	sechost	.idata	imports	Imag	R	RWE	
7732C000	00001000	sechost	.didat		Imag	R	RWE	
7732D000	00001000	sechost	.rsrc	resources	Imag	R	RWE	
7732E000	00003000	sechost	.reloc	relocations	Imag	R	RWE	
77340000	00001000	ADVAPI32		PE header	Imag	R	RWE	
77341000	00066000	ADVAPI32	.text	code,export	Imag	R	RWE	
773A7000	00004000	ADVAPI32	.data	data	Imag	R	RWE	
773AB000	00005000	ADVAPI32	.idata	imports	Imag	R	RWE	
773B0000	00001000	ADVAPI32	.didat		Imag	R	RWE	
773B1000	00001000	ADVAPI32	.rsrc	resources	Imag	R	RWE	
773B2000	00005000	ADVAPI32	.reloc	relocations	Imag	R	RWE	
77530000	00001000	WS2_32		PE header	Imag	R	RWE	
77531000	00048000	WS2_32	.text	code,export	Imag	R	RWE	
77AF0000	00001000	ntdll	RT		Imag	R	RWE	
77AF1000	00004000	ntdll	.data	data	Imag	R	RWE	
77AF5000	00003000	ntdll	.mrdata		Imag	R	RWE	
77AF8000	00001000	ntdll	.00cfg		Imag	R	RWE	
77AF9000	00068000	ntdll	.rsrc	resources	Imag	R	RWE	
77B61000	00005000	ntdll	.reloc	relocations	Imag	R	RWE	
7FEB0000	00005000				Map	R	R	
7FFB0000	00023000				Map	R	R	
7FFE0000	00001000				Priv	R	R	

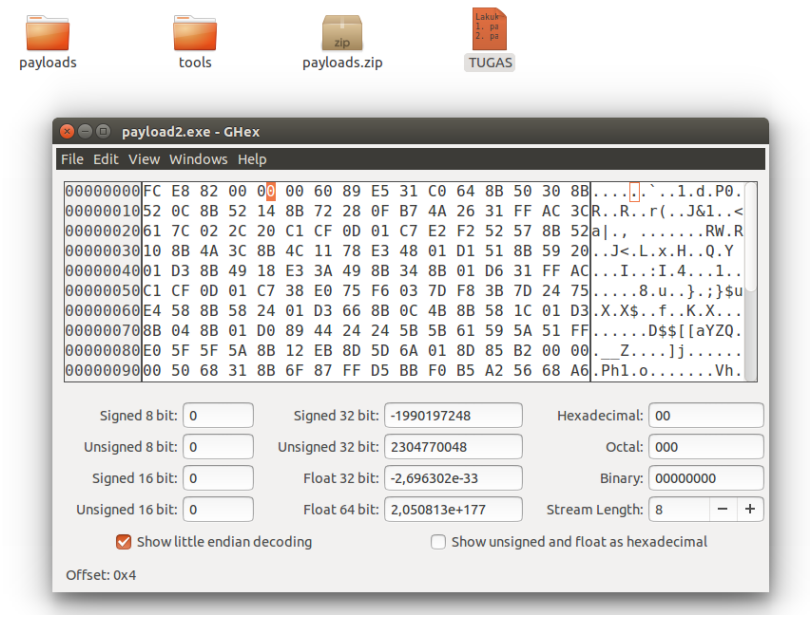


Lakukan analisis strings pada file payload menggunakan command berikut;

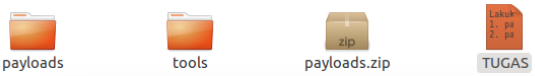


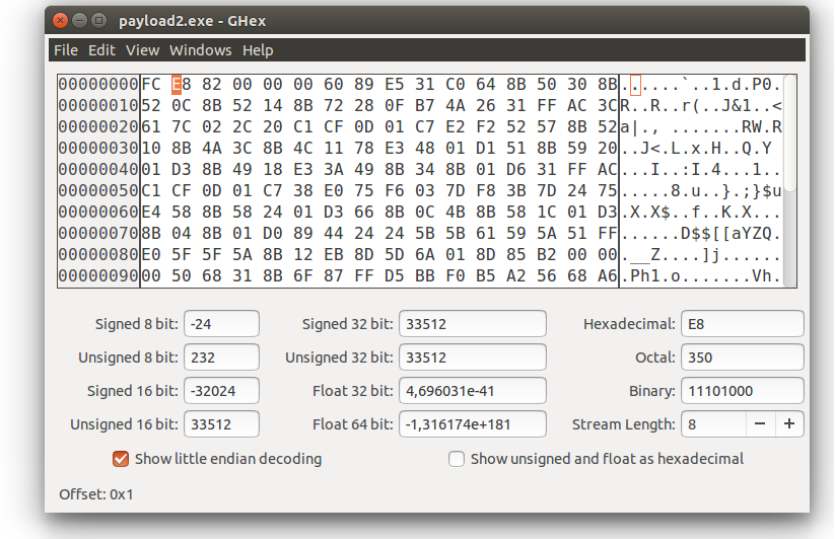
Muhammad Azriansyah 09011281320006 Keamanan Jaringan Komputer

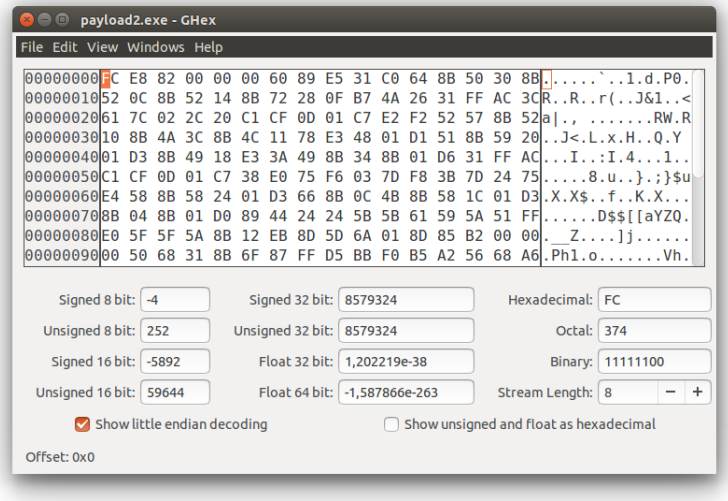
Hasil yang di dapatkan setelah memproses file payload dengan tools Ghex pada linux;



Muhammad Azriansyah 09011281320006 Keamanan Jaringan Komputer



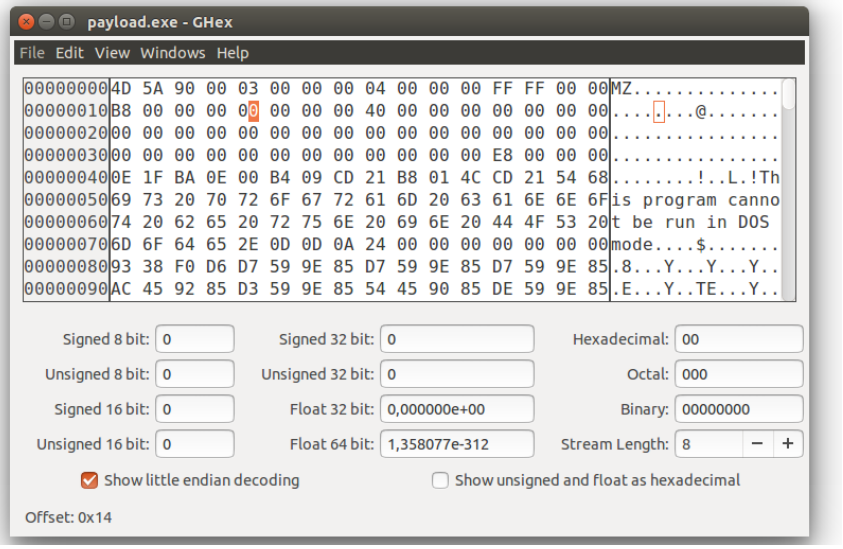




```
ardiah-X455LF: /home/[redacted]/Downloads/TUGAS/payloads
Your code just forked, and you are currently executing in the parent process
Your code just forked, and you are currently executing in the child process
Internal error
The process is not recognized.
The given path contained wildcard characters
The given path is misformatted or contained invalid characters
The given path was above the root path
The given path is incomplete
The given path is relative
The given path is absolute
The specified network mask is invalid.
The specified IP address is invalid.
DSO load failed
No shared memory is currently available
No thread key structure was provided and one was required.
No thread was provided and one was required.
No socket was provided and one was required.
No poll structure was provided and one was required.
No lock was provided and one was required.
No directory was provided and one was required.
No time was provided and one was required.
No process was provided and one was required.
An invalid socket was returned
An invalid date has been provided
A new pool could not be created.
Unrecognized Win32 error code %d
CancelIo
GetCompressedFileSizeA
GetCompressedFileSizeW
ZwQueryInformationFile
GetSecurityInfo
GetNamedSecurityInfoA
GetNamedSecurityInfoW
GetEffectiveRightsFromAclW
ntdll.dll
shell32
ws2_32
mswsock
advapi32
kernel32
root@ardiah-X455LF:/home/[redacted]/Downloads/TUGAS/payloads#
```

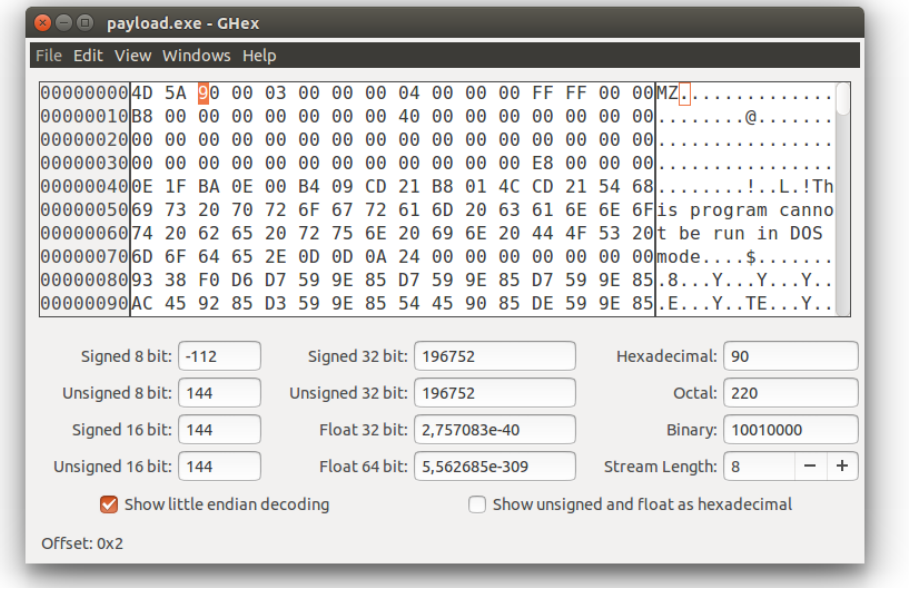

1.png


2.png



exe	DOS MZ executable file format and its descendants (including NE and PE)	0	MZ	4D 5A


1.png




```
4D 5A 90 00 03 00 00 00          MZ......
04 00 00 00 FF FF                ....ÿÿ
ZAP  ZoneAlam data file
```