National Forensic Sciences University

School of Cyber security and Digital Forensics

Subject: CTMSCS S2 P3 Malware Analysis

(TA-II Assignment)

Submitted to: Mr. Dharmesh Dave and Mr. Parag Rughani

Submitted by: Disha Sharma (2401030020014)

Submission Date: 03/04/2025

INDEX

- Sample 01 - Sample 05

  1) PE Header information

  2) PE Section information

  3) Strings analysis to identify any suspicious.

  4) Imports / Exports analysis.

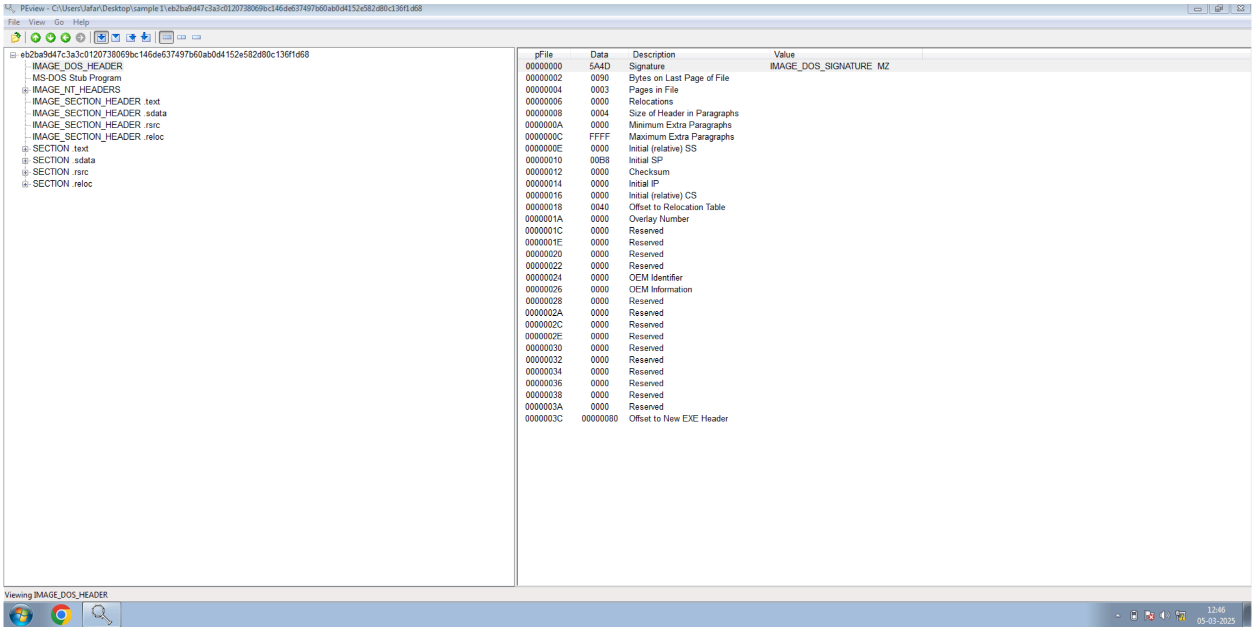
  5) Is the file packed/obfuscated? If yes then try to find its packer name.

  6) If GUI then identifies its resources.

  7) What is the file trying to do with the use of any suspicious functions / dlls?

SAMPLE 01 - SYRIAN MALWARE

1. PE Header Information



PEview - C:\Users\Jafar\Desktop\sample 1\eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68

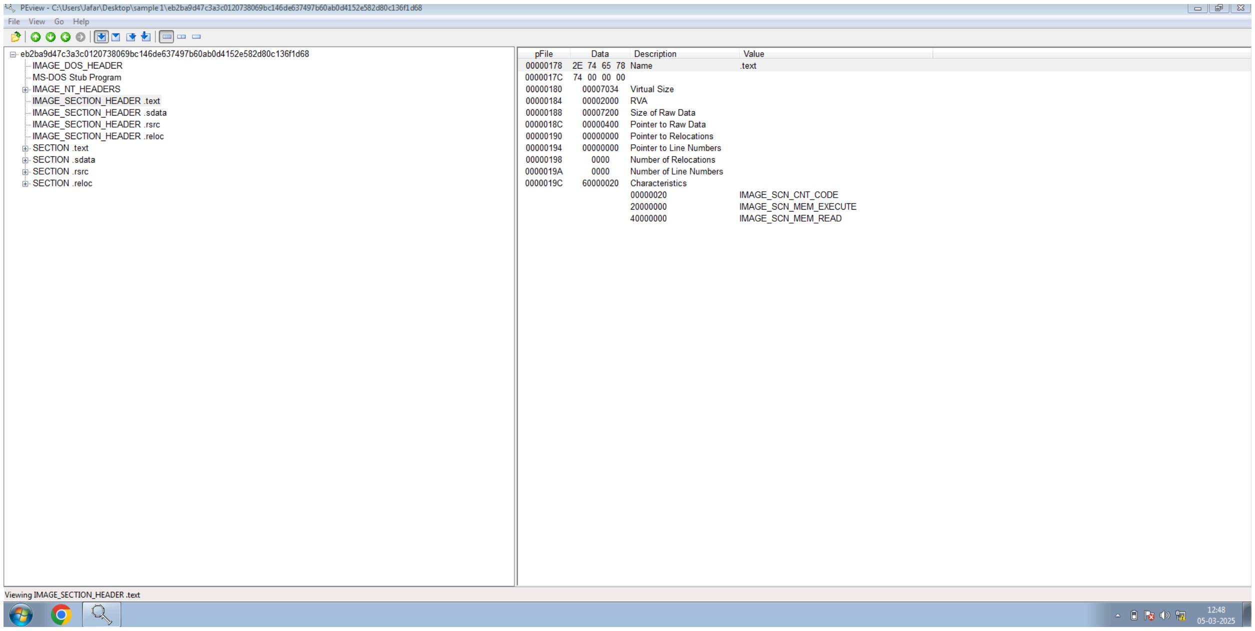
```
⊟ eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
  ⊞ IMAGE_NT_HEADERS
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .sdata
    IMAGE_SECTION_HEADER .rsrc
    IMAGE_SECTION_HEADER .reloc
  ⊞ SECTION .text
  ⊞ SECTION .sdata
  ⊞ SECTION .rsrc
  ⊞ SECTION .reloc
```

pFile	Data	Description	Value
00000000	5A4D	Signature	IMAGE_DOS_SIGNATURE MZ
00000002	0090	Bytes on Last Page of File	
00000004	0003	Pages in File	
00000006	0000	Relocations	
00000008	0004	Size of Header in Paragraphs	
0000000A	0000	Minimum Extra Paragraphs	
0000000C	FFFF	Maximum Extra Paragraphs	
0000000E	0000	Initial (relative) SS	
00000010	00B8	Initial SP	
00000012	0000	Checksum	
00000014	0000	Initial IP	
00000016	0000	Initial (relative) CS	
00000018	0040	Offset to Relocation Table	
0000001A	0000	Overlay Number	
0000001C	0000	Reserved	
0000001E	0000	Reserved	
00000020	0000	Reserved	
00000022	0000	Reserved	
00000024	0000	OEM Identifier	
00000026	0000	OEM Information	
00000028	0000	Reserved	
0000002A	0000	Reserved	
0000002C	0000	Reserved	
0000002E	0000	Reserved	
00000030	0000	Reserved	
00000032	0000	Reserved	
00000034	0000	Reserved	
00000036	0000	Reserved	
00000038	0000	Reserved	
0000003A	0000	Reserved	
0000003C	00000080	Offset to New EXE Header	

Viewing IMAGE_DOS_HEADER

The MS DOS header, now discontinued, provides the aforementioned information. However, significant details can be found from the NT headers and section headers.

2. PE Section Headers

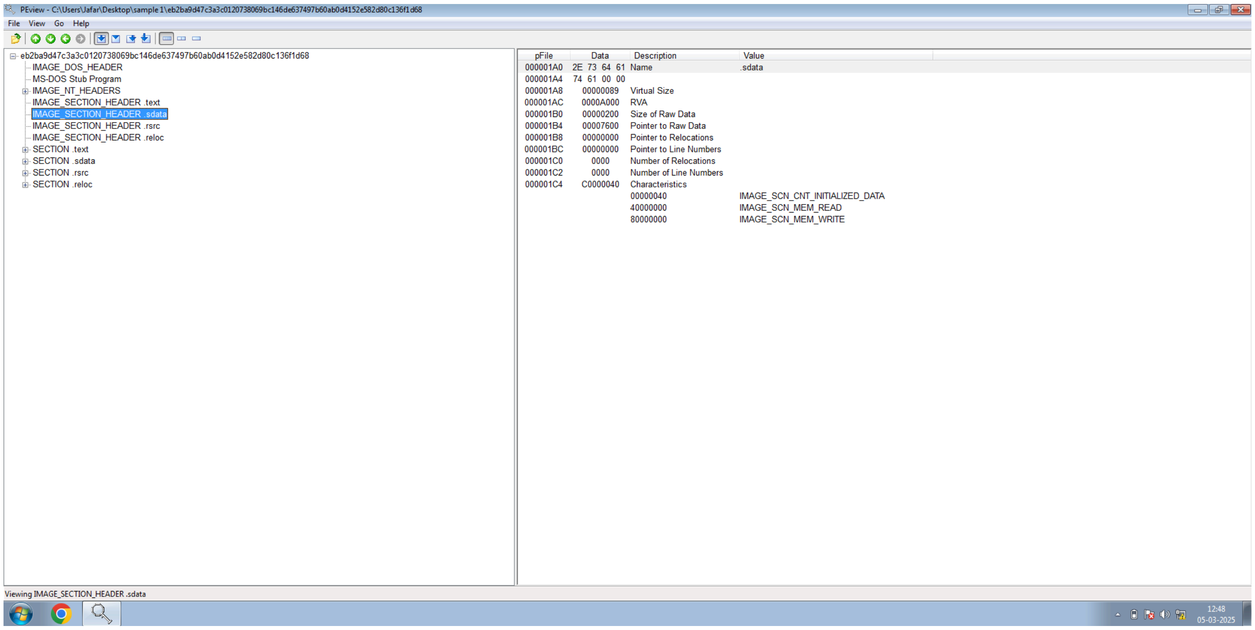


PEview - C:\Users\Jafar\Desktop\sample 1\eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68

```
⊟ eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
  ⊞ IMAGE_NT_HEADERS
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .sdata
    IMAGE_SECTION_HEADER .rsrc
    IMAGE_SECTION_HEADER .reloc
  ⊞ SECTION .text
  ⊞ SECTION .sdata
  ⊞ SECTION .rsrc
  ⊞ SECTION .reloc
```

pFile	Data	Description	Value
00000178	2E 74 65 78	Name	.text
0000017C	74 00 00 00		
00000180	00007034	Virtual Size	
00000184	00002000	RVA	
00000188	00007200	Size of Raw Data	
0000018C	00000400	Pointer to Raw Data	
00000190	00000000	Pointer to Relocations	
00000194	00000000	Pointer to Line Numbers	
00000198	0000	Number of Relocations	
0000019A	0000	Number of Line Numbers	
0000019C	60000020	Characteristics	
		00000020	IMAGE_SCN_CNT_CODE
		20000000	IMAGE_SCN_MEM_EXECUTE
		40000000	IMAGE_SCN_MEM_READ

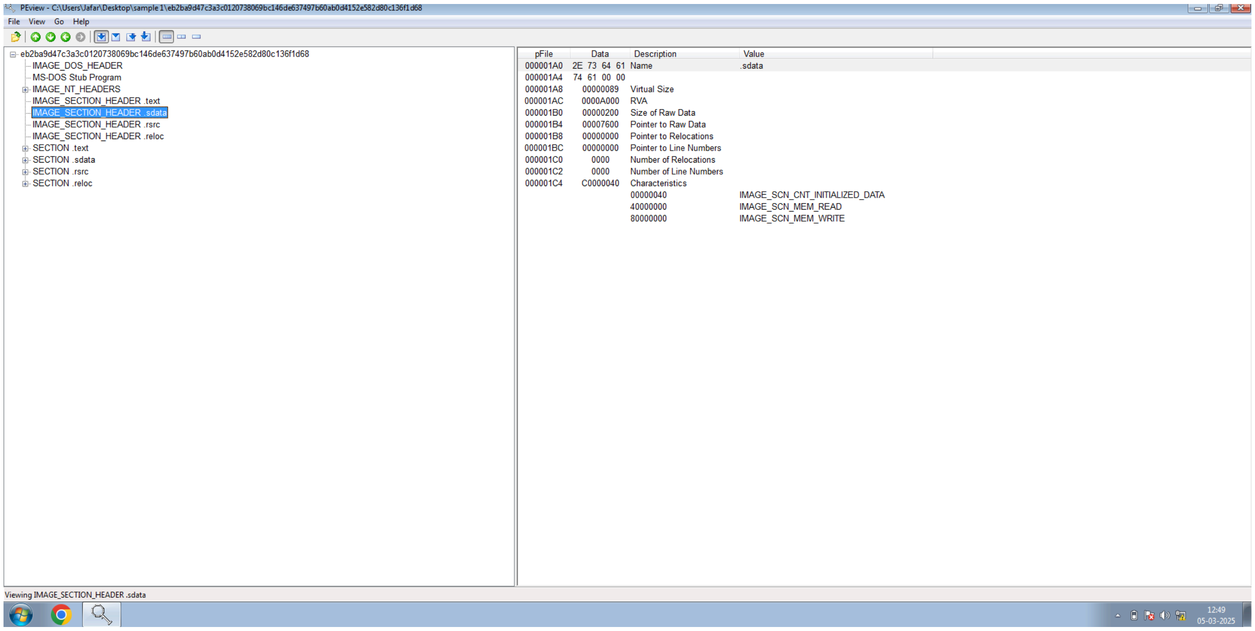
Viewing IMAGE_SECTION_HEADER .text


PEview - C:\Users\Jafar\Desktop\sample 1\eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68
File View Go Help
12:48
05-03-2025

```
eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
  + IMAGE_NT_HEADERS
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .sdata
    IMAGE_SECTION_HEADER .rsrc
    IMAGE_SECTION_HEADER .reloc
  + SECTION .text
  + SECTION .sdata
  + SECTION .rsrc
  + SECTION .reloc
```

```
pFile       Data          Description               Value
000001A0    2E 73 64 61   Name                      .sdata
000001A4    74 61 00 00
000001A8    00000089      Virtual Size
000001AC    0000A000      RVA
000001B0    00000200      Size of Raw Data
000001B4    00007600      Pointer to Raw Data
000001B8    00000000      Pointer to Relocations
000001BC    00000000      Pointer to Line Numbers
000001C0    0000          Number of Relocations
000001C2    0000          Number of Line Numbers
000001C4    C0000040      Characteristics
                          00000040                  IMAGE_SCN_CNT_INITIALIZED_DATA
                          40000000                  IMAGE_SCN_MEM_READ
                          80000000                  IMAGE_SCN_MEM_WRITE
```

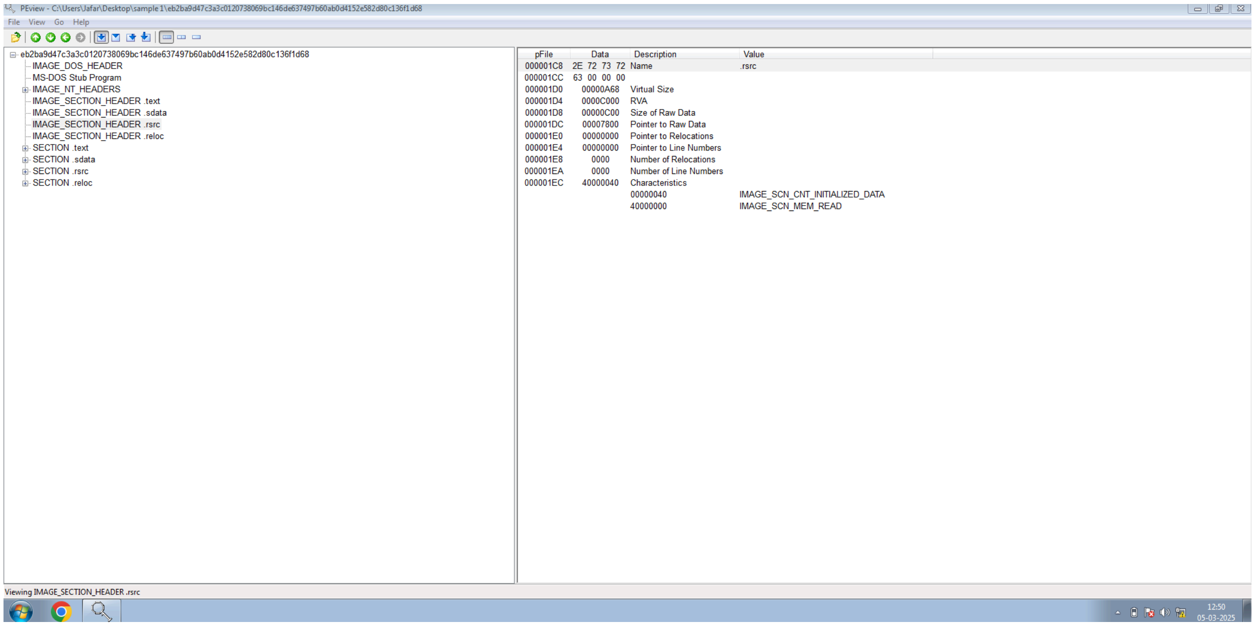
Viewing IMAGE_SECTION_HEADER .sdata


PEview - C:\Users\Jafar\Desktop\sample 1\eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68
File View Go Help
12:49
05-03-2025

```
eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
  + IMAGE_NT_HEADERS
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .sdata
    IMAGE_SECTION_HEADER .rsrc
    IMAGE_SECTION_HEADER .reloc
  + SECTION .text
  + SECTION .sdata
  + SECTION .rsrc
  + SECTION .reloc
```

```
pFile       Data          Description               Value
000001A0    2E 73 64 61   Name                      .sdata
000001A4    74 61 00 00
000001A8    00000089      Virtual Size
000001AC    0000A000      RVA
000001B0    00000200      Size of Raw Data
000001B4    00007600      Pointer to Raw Data
000001B8    00000000      Pointer to Relocations
000001BC    00000000      Pointer to Line Numbers
000001C0    0000          Number of Relocations
000001C2    0000          Number of Line Numbers
000001C4    C0000040      Characteristics
                          00000040                  IMAGE_SCN_CNT_INITIALIZED_DATA
                          40000000                  IMAGE_SCN_MEM_READ
                          80000000                  IMAGE_SCN_MEM_WRITE
```

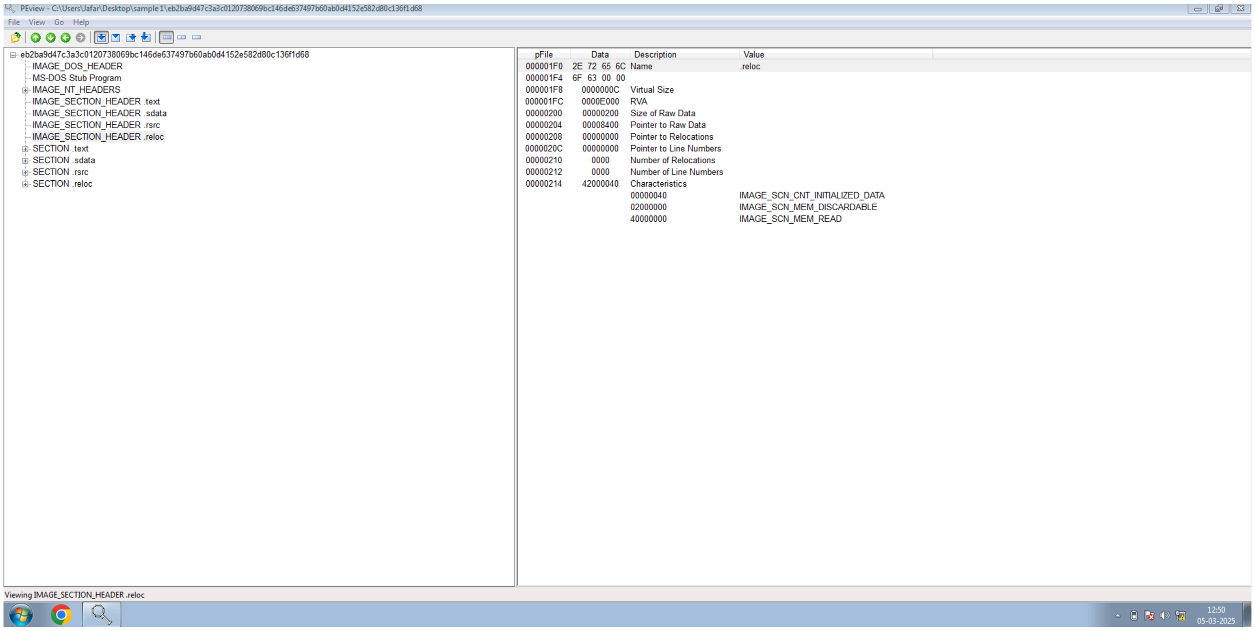
Viewing IMAGE_SECTION_HEADER .sdata


PEview - C:\Users\Jafar\Desktop\sample 1\eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68
File View Go Help
12:50
05-03-2025

```
eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
  + IMAGE_NT_HEADERS
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .sdata
    IMAGE_SECTION_HEADER .rsrc
    IMAGE_SECTION_HEADER .reloc
  + SECTION .text
  + SECTION .sdata
  + SECTION .rsrc
  + SECTION .reloc
```

```
pFile      Data          Description               Value
000001C8   2E 72 73 72   Name                      .rsrc
000001CC   63 00 00 00
000001D0     00000A68    Virtual Size
000001D4     0000C000    RVA
000001D8     00000C00    Size of Raw Data
000001DC     00007800    Pointer to Raw Data
000001E0     00000000    Pointer to Relocations
000001E4     00000000    Pointer to Line Numbers
000001E8       0000      Number of Relocations
000001EA       0000      Number of Line Numbers
000001EC     40000040    Characteristics
                         00000040                  IMAGE_SCN_CNT_INITIALIZED_DATA
                         40000000                  IMAGE_SCN_MEM_READ
```

Viewing IMAGE_SECTION_HEADER .rsrc


PEview - C:\Users\Jafar\Desktop\sample 1\eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68
File View Go Help
12:50
05-03-2025

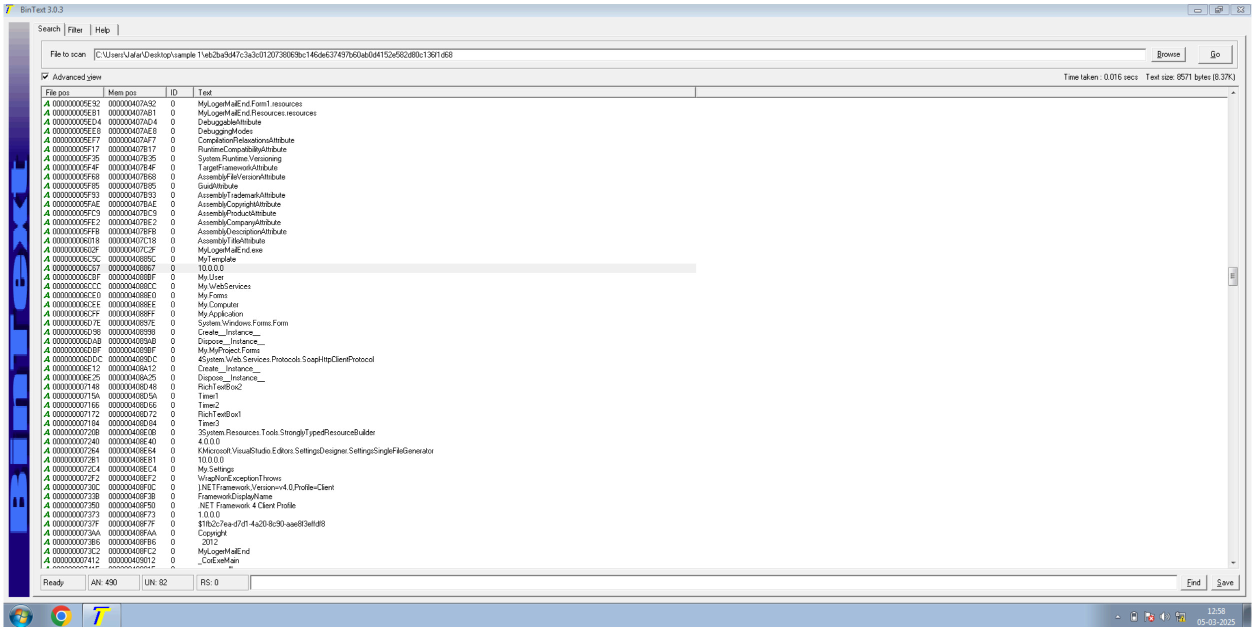
```
eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
  + IMAGE_NT_HEADERS
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .sdata
    IMAGE_SECTION_HEADER .rsrc
    IMAGE_SECTION_HEADER .reloc
  + SECTION .text
  + SECTION .sdata
  + SECTION .rsrc
  + SECTION .reloc
```

```
pFile      Data          Description               Value
000001F0   2E 72 65 6C   Name                      .reloc
000001F4   6F 63 00 00
000001F8     0000000C    Virtual Size
000001FC     0000E000    RVA
00000200     00000200    Size of Raw Data
00000204     00008400    Pointer to Raw Data
00000208     00000000    Pointer to Relocations
0000020C     00000000    Pointer to Line Numbers
00000210       0000      Number of Relocations
00000212       0000      Number of Line Numbers
00000214     42000040    Characteristics
                         00000040                  IMAGE_SCN_CNT_INITIALIZED_DATA
                         02000000                  IMAGE_SCN_MEM_DISCARDABLE
                         40000000                  IMAGE_SCN_MEM_READ
```

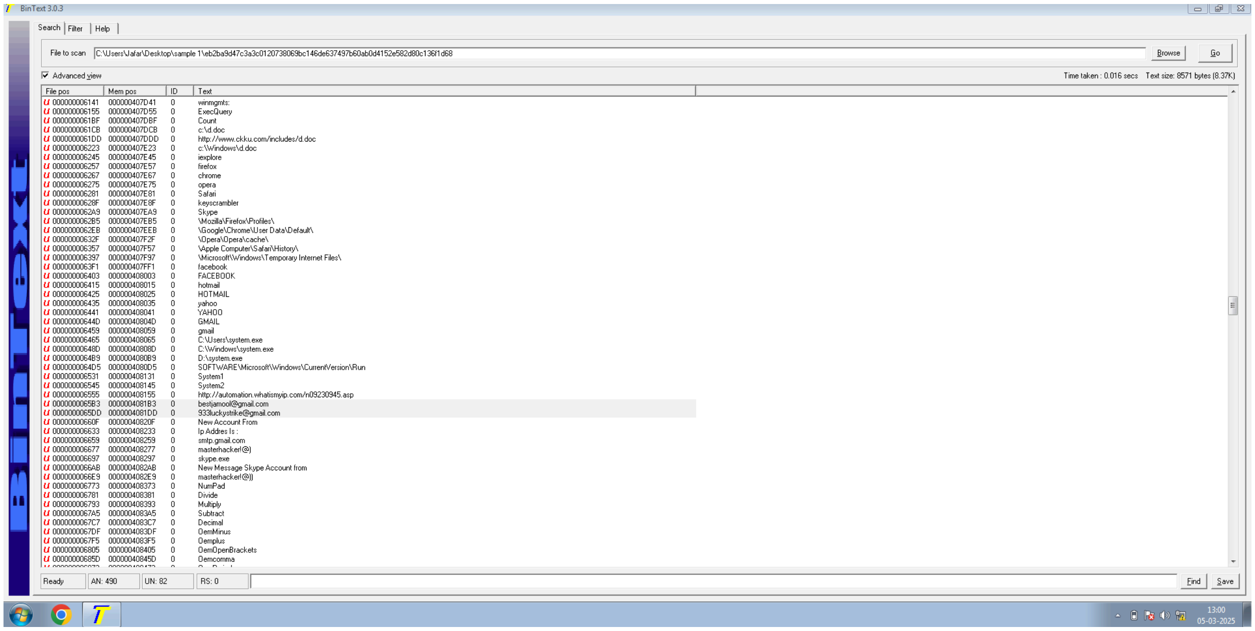
Viewing IMAGE_SECTION_HEADER .reloc

The section headers provide useful information about the 4 sections of the PE file and their associated details like Virtual Size and Size of Raw Data.

3. String Analysis



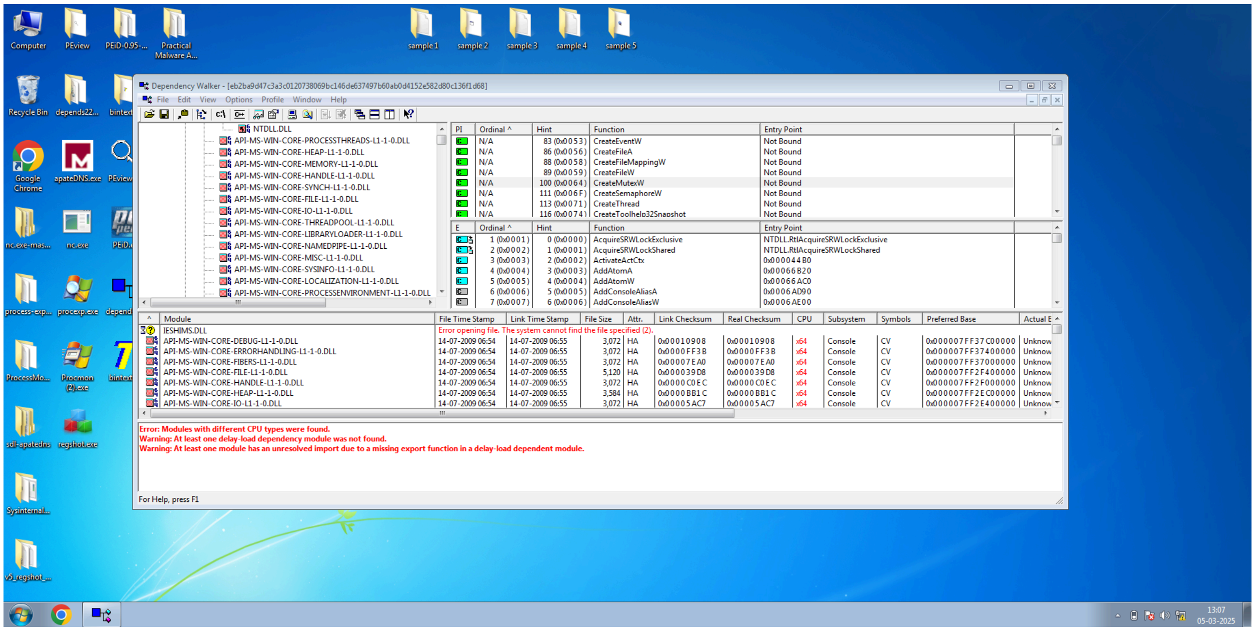
```
File to scan  C:\Users\Jafar\Desktop\sample 1\eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68
☑ Advanced view                          Time taken : 0.016 secs   Text size: 8571 bytes (8.37K)
File pos      Mem pos       ID  Text
A 000000005E92  000000407A92  0   MyLogerMailEnd.Form1.resources
A 000000005EB1  000000407AB1  0   MyLogerMailEnd.Resources.resources
A 000000005ED4  000000407AD4  0   DebuggableAttribute
A 000000005EE8  000000407AE8  0   DebuggingModes
A 000000005EF7  000000407AF7  0   CompilationRelaxationsAttribute
A 000000005F17  000000407B17  0   RuntimeCompatibilityAttribute
A 000000005F35  000000407B35  0   System.Runtime.Versioning
A 000000005F4F  000000407B4F  0   TargetFrameworkAttribute
A 000000005F68  000000407B68  0   AssemblyFileVersionAttribute
A 000000005F85  000000407B85  0   GuidAttribute
A 000000005F93  000000407B93  0   AssemblyTrademarkAttribute
A 000000005FAE  000000407BAE  0   AssemblyCopyrightAttribute
A 000000005FC9  000000407BC9  0   AssemblyProductAttribute
A 000000005FE2  000000407BE2  0   AssemblyCompanyAttribute
A 000000005FFB  000000407BFB  0   AssemblyDescriptionAttribute
A 000000006018  000000407C18  0   AssemblyTitleAttribute
A 00000000602F  000000407C2F  0   MyLogerMailEnd.exe
A 000000006C5C  00000040885C  0   MyTemplate
A 000000006C67  000000408867  0   10.0.0.0
A 000000006CBF  0000004088BF  0   My.User
A 000000006CCC  0000004088CC  0   My.WebServices
A 000000006CE0  0000004088E0  0   My.Forms
A 000000006CEE  0000004088EE  0   My.Computer
A 000000006CFF  0000004088FF  0   My.Application
A 000000006D7E  00000040897E  0   System.Windows.Forms.Form
A 000000006D98  000000408998  0   Create__Instance__
A 000000006DAB  0000004089AB  0   Dispose__Instance__
A 000000006DBF  0000004089BF  0   My.MyProject.Forms
A 000000006DDC  0000004089DC  0   4System.Web.Services.Protocols.SoapHttpClientProtocol
A 000000006E12  000000408A12  0   Create__Instance__
A 000000006E25  000000408A25  0   Dispose__Instance__
A 000000007148  000000408D48  0   RichTextBox2
A 00000000715A  000000408D5A  0   Timer1
A 000000007166  000000408D66  0   Timer2
A 000000007172  000000408D72  0   RichTextBox1
A 000000007184  000000408D84  0   Timer3
A 00000000720B  000000408E0B  0   3System.Resources.Tools.StronglyTypedResourceBuilder
A 000000007240  000000408E40  0   4.0.0.0
A 000000007264  000000408E64  0   KMicrosoft.VisualStudio.Editors.SettingsDesigner.SettingsSingleFileGenerator
A 0000000072B1  000000408EB1  0   10.0.0.0
A 0000000072C4  000000408EC4  0   My.Settings
A 0000000072F2  000000408EF2  0   WrapNonExceptionThrows
A 00000000730C  000000408F0C  0   ).NETFramework,Version=v4.0,Profile=Client
A 00000000733B  000000408F3B  0   FrameworkDisplayName
A 000000007350  000000408F50  0   .NET Framework 4 Client Profile
A 000000007373  000000408F73  0   1.0.0.0
A 00000000737F  000000408F7F  0   $1fb2c7ea-d7d1-4a20-8c90-aae8f3effdf8
A 0000000073AA  000000408FAA  0   Copyright
A 0000000073B6  000000408FB6  0    2012
A 0000000073C2  000000408FC2  0   MyLogerMailEnd
A 000000007412  000000409012  0   _CorExeMain
Ready   AN: 490   UN: 82   RS: 0
```



```
File to scan  C:\Users\Jafar\Desktop\sample 1\eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68
☑ Advanced view                          Time taken : 0.016 secs   Text size: 8571 bytes (8.37K)
File pos      Mem pos       ID  Text
U 000000006141  000000407D41  0   winmgmts:
U 000000006155  000000407D55  0   ExecQuery
U 0000000061BF  000000407DBF  0   Count
U 0000000061CB  000000407DCB  0   c:\d.doc
U 0000000061DD  000000407DDD  0   http://www.ckku.com/includes/d.doc
U 000000006223  000000407E23  0   c:\Windows\d.doc
U 000000006245  000000407E45  0   iexplore
U 000000006257  000000407E57  0   firefox
U 000000006267  000000407E67  0   chrome
U 000000006275  000000407E75  0   opera
U 000000006281  000000407E81  0   Safari
U 00000000628F  000000407E8F  0   keyscrambler
U 0000000062A9  000000407EA9  0   Skype
U 0000000062B5  000000407EB5  0   \Mozilla\Firefox\Profiles\
U 0000000062EB  000000407EEB  0   \Google\Chrome\User Data\Default\
U 00000000632F  000000407F2F  0   \Opera\Opera\cache\
U 000000006357  000000407F57  0   \Apple Computer\Safari\History\
U 000000006397  000000407F97  0   \Microsoft\Windows\Temporary Internet Files\
U 0000000063F1  000000407FF1  0   facebook
U 000000006403  000000408003  0   FACEBOOK
U 000000006415  000000408015  0   hotmail
U 000000006425  000000408025  0   HOTMAIL
U 000000006435  000000408035  0   yahoo
U 000000006441  000000408041  0   YAHOO
U 00000000644D  00000040804D  0   GMAIL
U 000000006459  000000408059  0   gmail
U 000000006465  000000408065  0   C:\Users\system.exe
U 00000000648D  00000040808D  0   C:\Windows\system.exe
U 0000000064B9  0000004080B9  0   D:\system.exe
U 0000000064D5  0000004080D5  0   SOFTWARE\Microsoft\Windows\CurrentVersion\Run
U 000000006531  000000408131  0   System1
U 000000006545  000000408145  0   System2
U 000000006555  000000408155  0   http://automation.whatismyip.com/n09230945.asp
U 0000000065B3  0000004081B3  0   bestjamool@gmail.com
U 0000000065DD  0000004081DD  0   933luckystrike@gmail.com
U 00000000660F  00000040820F  0   New Account From
U 000000006633  000000408233  0   Ip Addres Is :
U 000000006659  000000408259  0   smtp.gmail.com
U 000000006677  000000408277  0   masterhacker!@)
U 000000006697  000000408297  0   skype.exe
U 0000000066AB  0000004082AB  0   New Message Skype Account from
U 0000000066E9  0000004082E9  0   masterhacker!@))
U 000000006773  000000408373  0   NumPad
U 000000006781  000000408381  0   Divide
U 000000006793  000000408393  0   Multiply
U 0000000067A5  0000004083A5  0   Subtract
U 0000000067C7  0000004083C7  0   Decimal
U 0000000067DF  0000004083DF  0   OemMinus
U 0000000067F5  0000004083F5  0   Oemplus
U 000000006805  000000408405  0   OemOpenBrackets
U 00000000685D  00000040845D  0   Oemcomma
Ready   AN: 490   UN: 82   RS: 0
```

The strings contain an IP address possibly used to connect to the attacker's machine along with suspicious windows functions like GetProcAddress and LoadLibrary.

4. Imports/Exports Analysis



Dependency Walker - [eb2ba9d47c3a3c0120738069bc146de637497b60ab0d4152e582d80c136f1d68]

```
NTDLL.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-0.DLL
API-MS-WIN-CORE-HEAP-L1-1-0.DLL
API-MS-WIN-CORE-MEMORY-L1-1-0.DLL
API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
API-MS-WIN-CORE-SYNCH-L1-1-0.DLL
API-MS-WIN-CORE-FILE-L1-1-0.DLL
API-MS-WIN-CORE-IO-L1-1-0.DLL
API-MS-WIN-CORE-THREADPOOL-L1-1-0.DLL
API-MS-WIN-CORE-LIBRARYLOADER-L1-1-0.DLL
API-MS-WIN-CORE-NAMEDPIPE-L1-1-0.DLL
API-MS-WIN-CORE-MISC-L1-1-0.DLL
API-MS-WIN-CORE-SYSINFO-L1-1-0.DLL
API-MS-WIN-CORE-LOCALIZATION-L1-1-0.DLL
API-MS-WIN-CORE-PROCESSENVIRONMENT-L1-1-0.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	83 (0x0053)	CreateEventW	Not Bound
C	N/A	86 (0x0056)	CreateFileA	Not Bound
C	N/A	88 (0x0058)	CreateFileMappingW	Not Bound
C	N/A	89 (0x0059)	CreateFileW	Not Bound
C	N/A	100 (0x0064)	CreateMutexW	Not Bound
C	N/A	111 (0x006F)	CreateSemaphoreW	Not Bound
C	N/A	113 (0x0071)	CreateThread	Not Bound
C	N/A	116 (0x0074)	CreateToolhelp32Snapshot	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
C	2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
C	3 (0x0003)	2 (0x0002)	ActivateActCtx	0x000044B0
C	4 (0x0004)	3 (0x0003)	AddAtomA	0x00066B20
C	5 (0x0005)	4 (0x0004)	AddAtomW	0x00066AC0
C	6 (0x0006)	5 (0x0005)	AddConsoleAliasA	0x0006AD90
C	7 (0x0007)	6 (0x0006)	AddConsoleAliasW	0x0006AE00

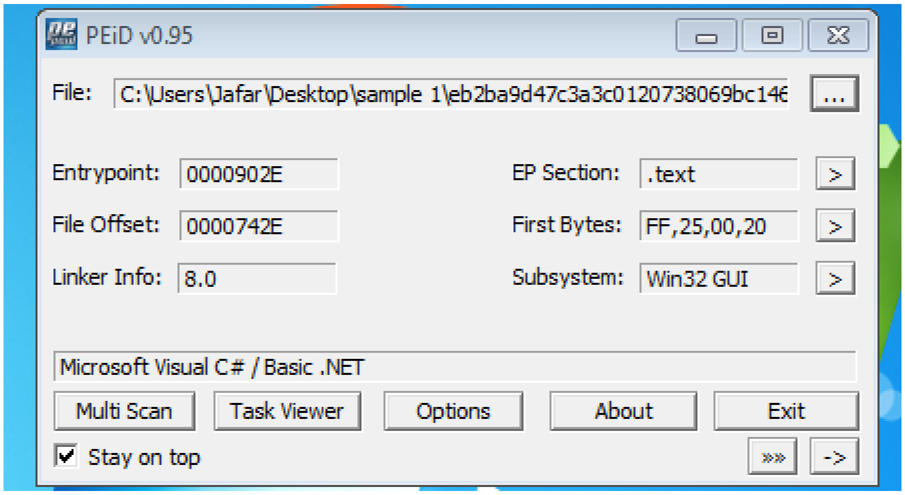
^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual E
?	IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).										
	API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00010908	0x00010908	x64	Console	CV	0x000007FF37C00000	Unknow
	API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000FF3B	0x0000FF3B	x64	Console	CV	0x000007FF37400000	Unknow
	API-MS-WIN-CORE-FIBERS-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00007EA0	0x00007EA0	x64	Console	CV	0x000007FF37000000	Unknow
	API-MS-WIN-CORE-FILE-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	5,120	HA	0x000039D8	0x000039D8	x64	Console	CV	0x000007FF2F400000	Unknow
	API-MS-WIN-CORE-HANDLE-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000C0EC	0x0000C0EC	x64	Console	CV	0x000007FF2F000000	Unknow
	API-MS-WIN-CORE-HEAP-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,584	HA	0x0000BB1C	0x0000BB1C	x64	Console	CV	0x000007FF2EC00000	Unknow
	API-MS-WIN-CORE-IO-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00005AC7	0x00005AC7	x64	Console	CV	0x000007FF2E400000	Unknow

```
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```

For Help, press F1

The imported DLLs use functions to create mutexes (mutual exclusion objects) that show the possibility of the file being a malware.

5. Is the file packed/obfuscated?



File: C:\Users\Jafar\Desktop\sample 1\eb2ba9d47c3a3c0120738069bc14€

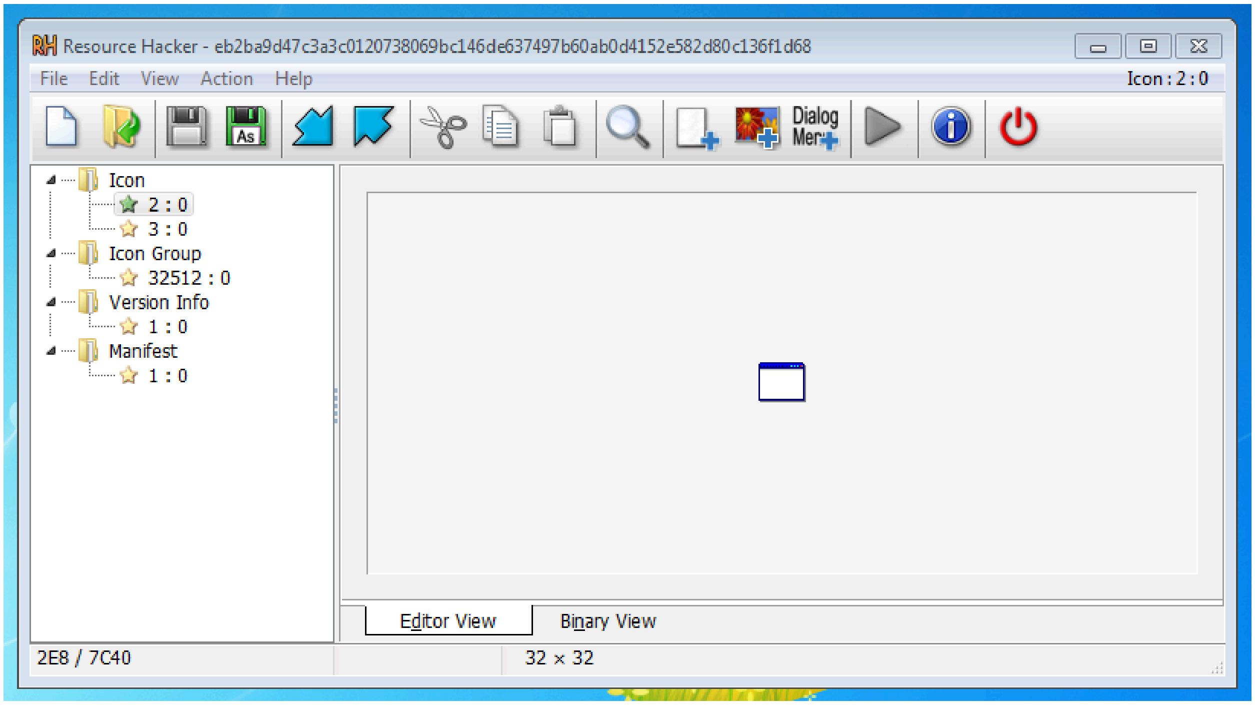
Entrypoint:	0000902E	EP Section:	.text
File Offset:	0000742E	First Bytes:	FF,25,00,20
Linker Info:	8.0	Subsystem:	Win32 GUI

Microsoft Visual C# / Basic .NET

☑ Stay on top

The file is not packed.

6. If GUI, then identify its resources



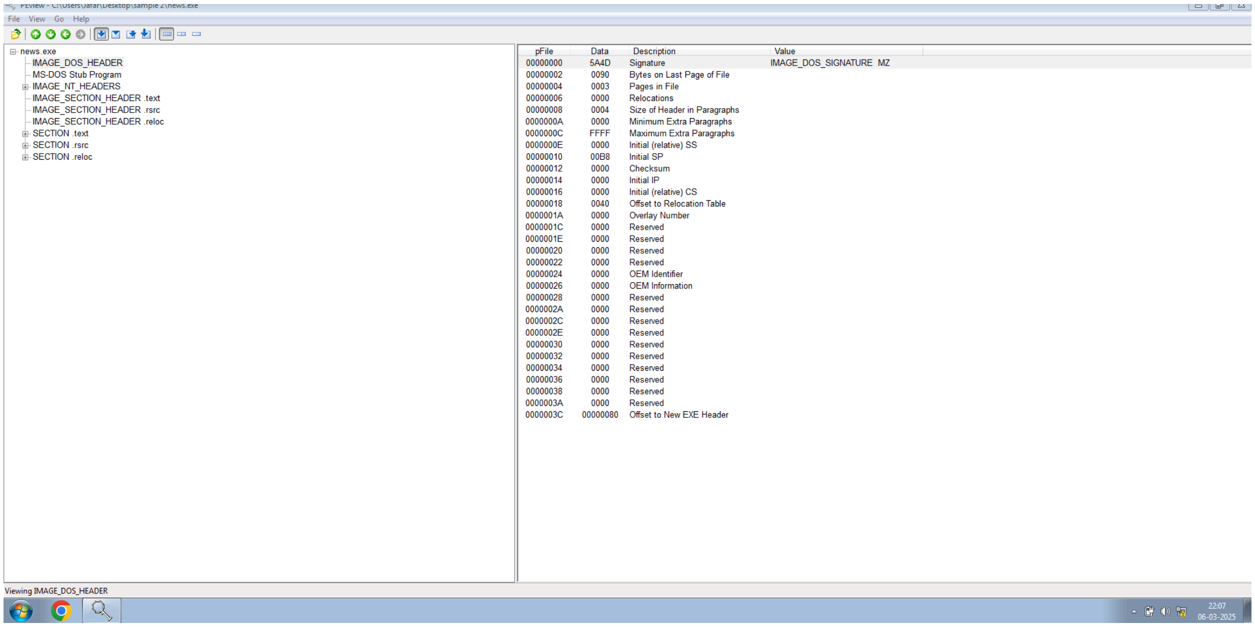
Resource Hacker does not provide much information about the functionality of the malware.

7. What is the file trying to do?

The potential malware file is trying to communicate with an external machine and transfer files or sensitive information. It is able to track the infected system's processes using mutexes and is modifying them simultaneously.

SAMPLE 02 - SYRIAN MALWARE

1. PE Header Information



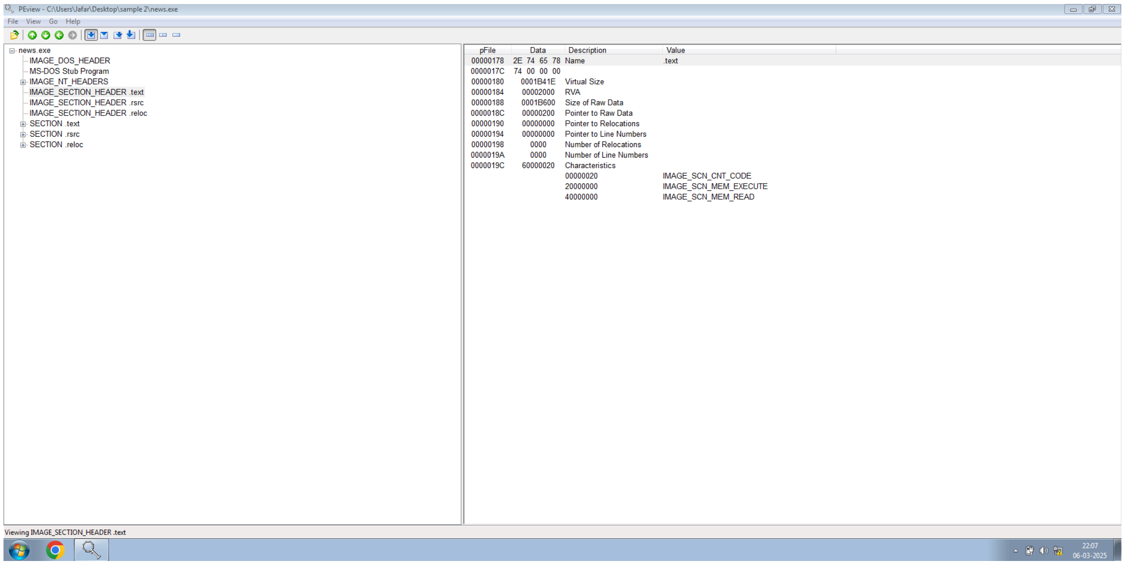
```
news.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .reloc
  SECTION .text
  SECTION .rsrc
  SECTION .reloc
```

```
pFile     Data      Description                   Value
00000000  5A4D      Signature                     IMAGE_DOS_SIGNATURE  MZ
00000002  0090      Bytes on Last Page of File
00000004  0003      Pages in File
00000006  0000      Relocations
00000008  0004      Size of Header in Paragraphs
0000000A  0000      Minimum Extra Paragraphs
0000000C  FFFF      Maximum Extra Paragraphs
0000000E  0000      Initial (relative) SS
00000010  00B8      Initial SP
00000012  0000      Checksum
00000014  0000      Initial IP
00000016  0000      Initial (relative) CS
00000018  0040      Offset to Relocation Table
0000001A  0000      Overlay Number
0000001C  0000      Reserved
0000001E  0000      Reserved
00000020  0000      Reserved
00000022  0000      Reserved
00000024  0000      OEM Identifier
00000026  0000      OEM Information
00000028  0000      Reserved
0000002A  0000      Reserved
0000002C  0000      Reserved
0000002E  0000      Reserved
00000030  0000      Reserved
00000032  0000      Reserved
00000034  0000      Reserved
00000036  0000      Reserved
00000038  0000      Reserved
0000003A  0000      Reserved
0000003C  00000080  Offset to New EXE Header
```

Viewing IMAGE_DOS_HEADER

The MS DOS header, now discontinued, provides the aforementioned information. However, significant details can be found from the NT headers and section headers.

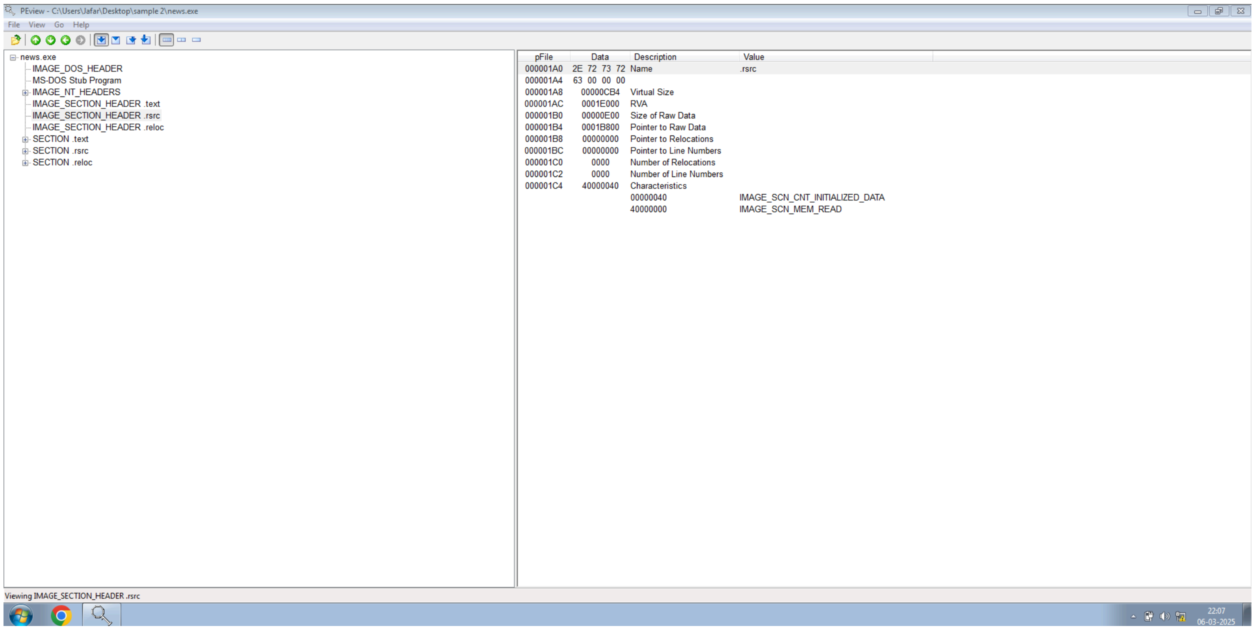
2. PE Section Headers



```
news.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .reloc
  SECTION .text
  SECTION .rsrc
  SECTION .reloc
```

```
pFile     Data          Description              Value
00000178  2E 74 65 78   Name                     .text
0000017C  74 00 00 00
00000180  0001B41E      Virtual Size
00000184  00002000      RVA
00000188  0001B600      Size of Raw Data
0000018C  00000200      Pointer to Raw Data
00000190  00000000      Pointer to Relocations
00000194  00000000      Pointer to Line Numbers
00000198  0000          Number of Relocations
0000019A  0000          Number of Line Numbers
0000019C  60000020      Characteristics
                        00000020                 IMAGE_SCN_CNT_CODE
                        20000000                 IMAGE_SCN_MEM_EXECUTE
                        40000000                 IMAGE_SCN_MEM_READ
```

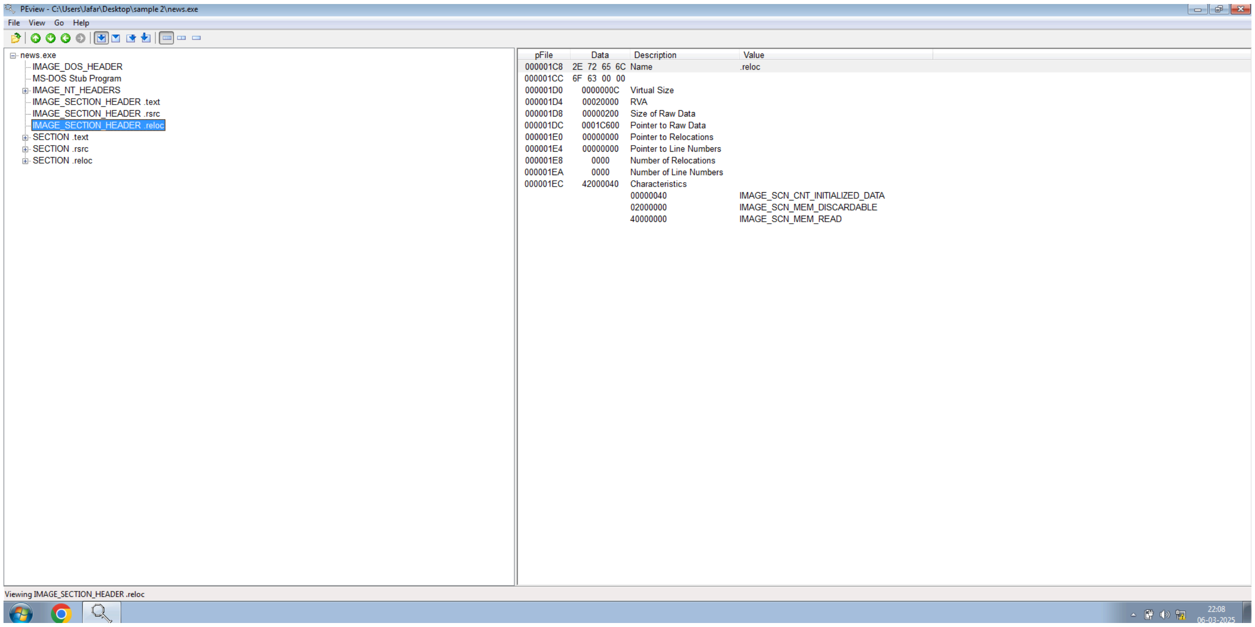
Viewing IMAGE_SECTION_HEADER .text



```
news.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .reloc
  SECTION .text
  SECTION .rsrc
  SECTION .reloc
```

```
pFile     Data         Description              Value
000001A0  2E 72 73 72  Name                     .rsrc
000001A4  63 00 00 00
000001A8   00000CB4    Virtual Size
000001AC   0001E000    RVA
000001B0   00000E00    Size of Raw Data
000001B4   0001B800    Pointer to Raw Data
000001B8   00000000    Pointer to Relocations
000001BC   00000000    Pointer to Line Numbers
000001C0     0000      Number of Relocations
000001C2     0000      Number of Line Numbers
000001C4   40000040    Characteristics
                       00000040                 IMAGE_SCN_CNT_INITIALIZED_DATA
                       40000000                 IMAGE_SCN_MEM_READ
```

Viewing IMAGE_SECTION_HEADER .rsrc



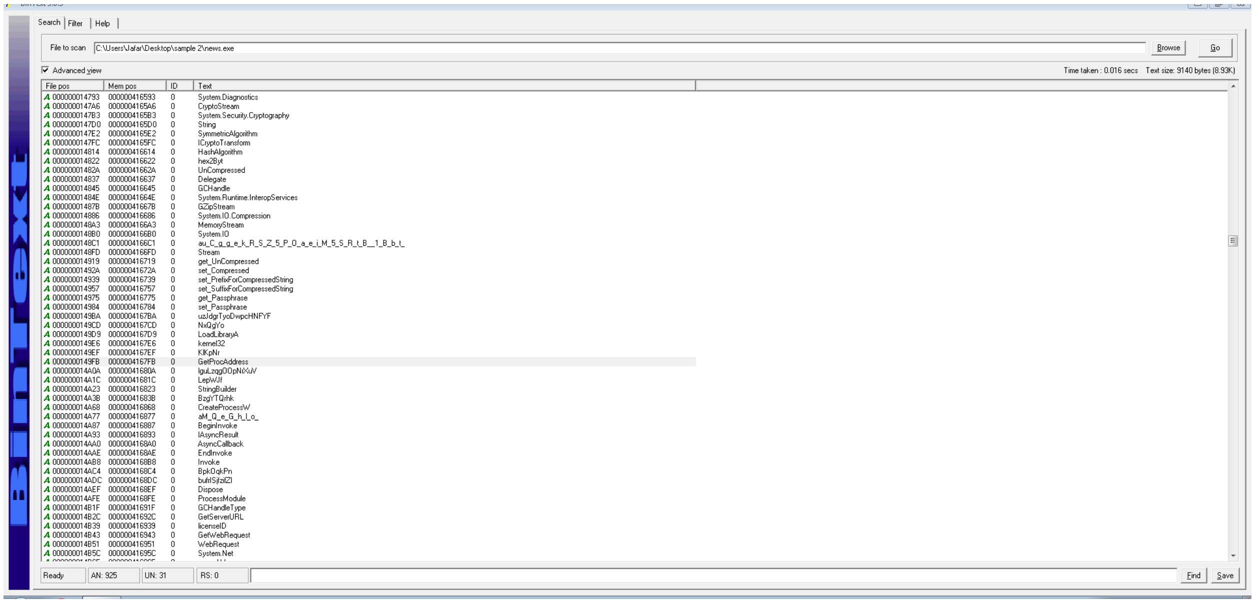
```
news.exe
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rsrc
  IMAGE_SECTION_HEADER .reloc
  SECTION .text
  SECTION .rsrc
  SECTION .reloc
```

```
pFile     Data         Description              Value
000001C8  2E 72 65 6C  Name                     .reloc
000001CC  6F 63 00 00
000001D0   0000000C    Virtual Size
000001D4   00020000    RVA
000001D8   00000200    Size of Raw Data
000001DC   0001C600    Pointer to Raw Data
000001E0   00000000    Pointer to Relocations
000001E4   00000000    Pointer to Line Numbers
000001E8     0000      Number of Relocations
000001EA     0000      Number of Line Numbers
000001EC   42000040    Characteristics
                       00000040                 IMAGE_SCN_CNT_INITIALIZED_DATA
                       02000000                 IMAGE_SCN_MEM_DISCARDABLE
                       40000000                 IMAGE_SCN_MEM_READ
```

Viewing IMAGE_SECTION_HEADER .reloc

The section headers provide useful information about the 4 sections of the PE file and their associated details like Virtual Size and Size of Raw Data.

3. String Analysis



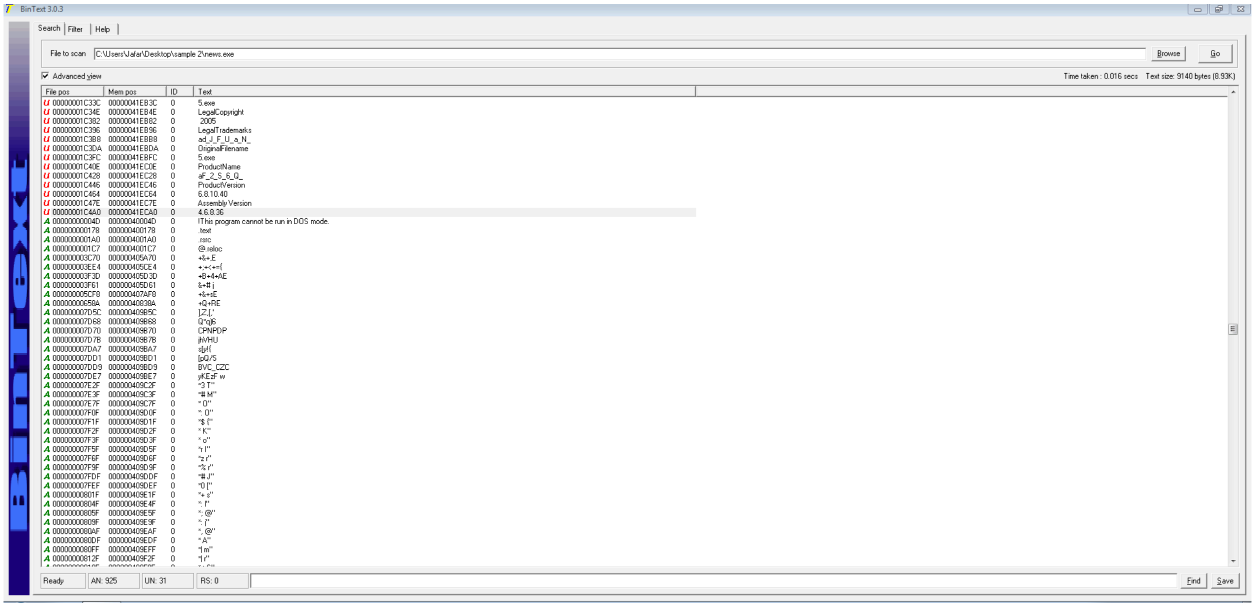
File to scan: C:\Users\Jafar\Desktop\sample 2\news.exe

☑ Advanced view

Time taken : 0.016 secs   Text size: 9140 bytes (8.93K)

```
File pos        Mem pos         ID   Text
A 000000014793  000000416593    0    System.Diagnostics
A 0000000147A6  0000004165A6    0    CryptoStream
A 0000000147B3  0000004165B3    0    System.Security.Cryptography
A 0000000147D0  0000004165D0    0    String
A 0000000147E2  0000004165E2    0    SymmetricAlgorithm
A 0000000147FC  0000004165FC    0    ICryptoTransform
A 000000014814  000000416614    0    HashAlgorithm
A 000000014822  000000416622    0    hex2Byt
A 00000001482A  00000041662A    0    UnCompressed
A 000000014837  000000416637    0    Delegate
A 000000014845  000000416645    0    GCHandle
A 00000001484E  00000041664E    0    System.Runtime.InteropServices
A 00000001487B  00000041667B    0    GZipStream
A 000000014886  000000416686    0    System.IO.Compression
A 0000000148A3  0000004166A3    0    MemoryStream
A 0000000148B0  0000004166B0    0    System.IO
A 0000000148C1  0000004166C1    0    au_C_g_g_e_k_R_S_Z_5_P_0_a_e_i_M_5_S_R_t_B__1_B_b_t_
A 0000000148FD  0000004166FD    0    Stream
A 000000014919  000000416719    0    get_UnCompressed
A 00000001492A  00000041672A    0    set_Compressed
A 000000014939  000000416739    0    set_PrefixForCompressedString
A 000000014957  000000416757    0    set_SuffixForCompressedString
A 000000014975  000000416775    0    get_Passphrase
A 000000014984  000000416784    0    set_Passphrase
A 0000000149BA  0000004167BA    0    uzJdgrTyoDwpcHNFYF
A 0000000149CD  0000004167CD    0    NxQgYo
A 0000000149D9  0000004167D9    0    LoadLibraryA
A 0000000149E6  0000004167E6    0    kernel32
A 0000000149EF  0000004167EF    0    KIKpNr
A 0000000149FB  0000004167FB    0    GetProcAddress
A 000000014A0A  00000041680A    0    IguLzqgOOpNrXuV
A 000000014A1C  00000041681C    0    LepWJf
A 000000014A23  000000416823    0    StringBuilder
A 000000014A3B  00000041683B    0    BzgYTQrhk
A 000000014A68  000000416868    0    CreateProcessW
A 000000014A77  000000416877    0    aM_Q_e_G_h_l_o_
A 000000014A87  000000416887    0    BeginInvoke
A 000000014A93  000000416893    0    IAsyncResult
A 000000014AA0  0000004168A0    0    AsyncCallback
A 000000014AAE  0000004168AE    0    EndInvoke
A 000000014AB8  0000004168B8    0    Invoke
A 000000014AC4  0000004168C4    0    BpkOqkPn
A 000000014ADC  0000004168DC    0    bufrlSjfzifZI
A 000000014AEF  0000004168EF    0    Dispose
A 000000014AFE  0000004168FE    0    ProcessModule
A 000000014B1F  00000041691F    0    GCHandleType
A 000000014B2C  00000041692C    0    GetServerURL
A 000000014B39  000000416939    0    licenseID
A 000000014B43  000000416943    0    GetWebRequest
A 000000014B51  000000416951    0    WebRequest
A 000000014B5C  00000041695C    0    System.Net
```

Ready | AN: 925 | UN: 31 | RS: 0



File to scan: C:\Users\Jafar\Desktop\sample 2\news.exe

☑ Advanced view

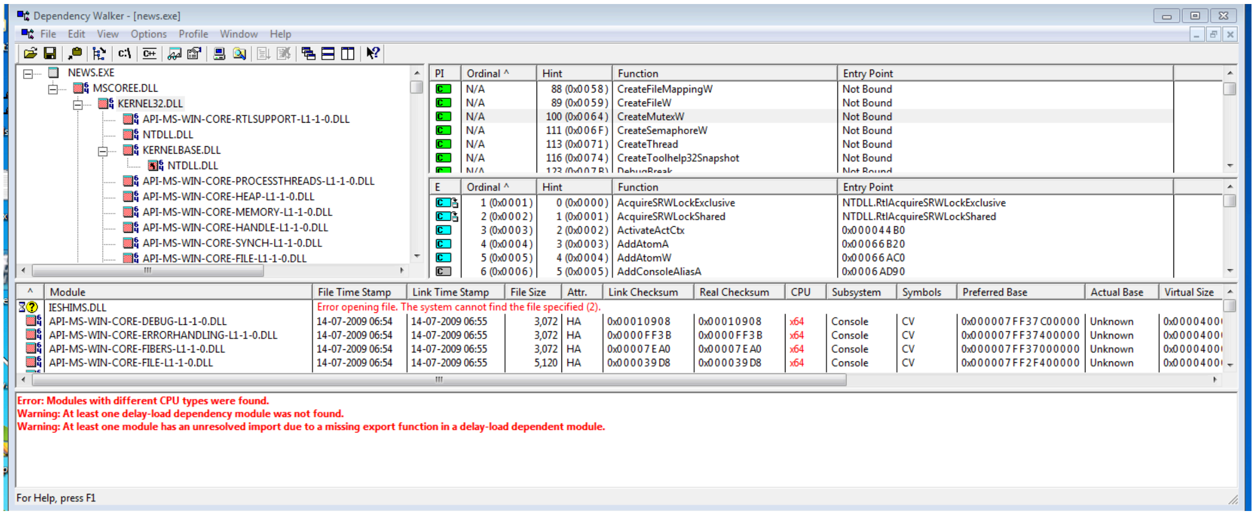
Time taken : 0.016 secs   Text size: 9140 bytes (8.93K)

```
File pos        Mem pos         ID   Text
U 00000001C33C  00000041EB3C    0    5.exe
U 00000001C34E  00000041EB4E    0    LegalCopyright
U 00000001C382  00000041EB82    0     2005
U 00000001C396  00000041EB96    0    LegalTrademarks
U 00000001C3B8  00000041EBB8    0    ad_J_F_U_a_N_
U 00000001C3DA  00000041EBDA    0    OriginalFilename
U 00000001C3FC  00000041EBFC    0    5.exe
U 00000001C40E  00000041EC0E    0    ProductName
U 00000001C428  00000041EC28    0    aF_2_S_6_Q_
U 00000001C446  00000041EC46    0    ProductVersion
U 00000001C464  00000041EC64    0    6.8.10.40
U 00000001C47E  00000041EC7E    0    Assembly Version
U 00000001C4A0  00000041ECA0    0    4.6.8.36
A 00000000004D  00000040004D    0    !This program cannot be run in DOS mode.
A 000000000178  000000400178    0    .text
A 0000000001A0  0000004001A0    0    .rsrc
A 0000000001C7  0000004001C7    0    @.reloc
A 000000003C70  000000405A70    0    +&+,E
A 000000003EE4  000000405CE4    0    +;+<+={
A 000000003F3D  000000405D3D    0    +B+4+AE
A 000000003F61  000000405D61    0    &+# j
A 000000005CF8  000000407AF8    0    +&+sE
A 00000000658A  00000040838A    0    +Q+RE
A 000000007D5C  000000409B5C    0    ]Z,[,'
A 000000007D68  000000409B68    0    Q*q]6
A 000000007D70  000000409B70    0    CPNPDP
A 000000007D7B  000000409B7B    0    jhVHU
A 000000007DA7  000000409BA7    0    s[y!{
A 000000007DD1  000000409BD1    0    [pQ/S
A 000000007DD9  000000409BD9    0    BVC_CZC
A 000000007DE7  000000409BE7    0    yKEzF w
A 000000007E2F  000000409C2F    0    *3 T"
A 000000007E3F  000000409C3F    0    *# M"
A 000000007E7F  000000409C7F    0    * 0"
A 000000007F0F  000000409D0F    0    *: 0"
A 000000007F1F  000000409D1F    0    *$ {"
A 000000007F2F  000000409D2F    0    * K"
A 000000007F3F  000000409D3F    0    * o"
A 000000007F5F  000000409D5F    0    *r l"
A 000000007F6F  000000409D6F    0    *z r"
A 000000007F9F  000000409D9F    0    *% r"
A 000000007FDF  000000409DDF    0    *# J"
A 000000007FEF  000000409DEF    0    *0 ["
A 00000000801F  000000409E1F    0    *+ s"
A 00000000804F  000000409E4F    0    *: l"
A 00000000805F  000000409E5F    0    *; @"
A 00000000809F  000000409E9F    0    *: j"
A 0000000080AF  000000409EAF    0    *, @"
A 0000000080DF  000000409EDF    0    * A"
A 0000000080FF  000000409EFF    0    *| m"
A 00000000812F  000000409F2F    0    *| r"
```

Ready | AN: 925 | UN: 31 | RS: 0

The strings contain an IP address possibly used to connect to the attacker’s machine along with suspicious windows functions like GetProcAddress and LoadLibrary.

4. Imports/Exports Information



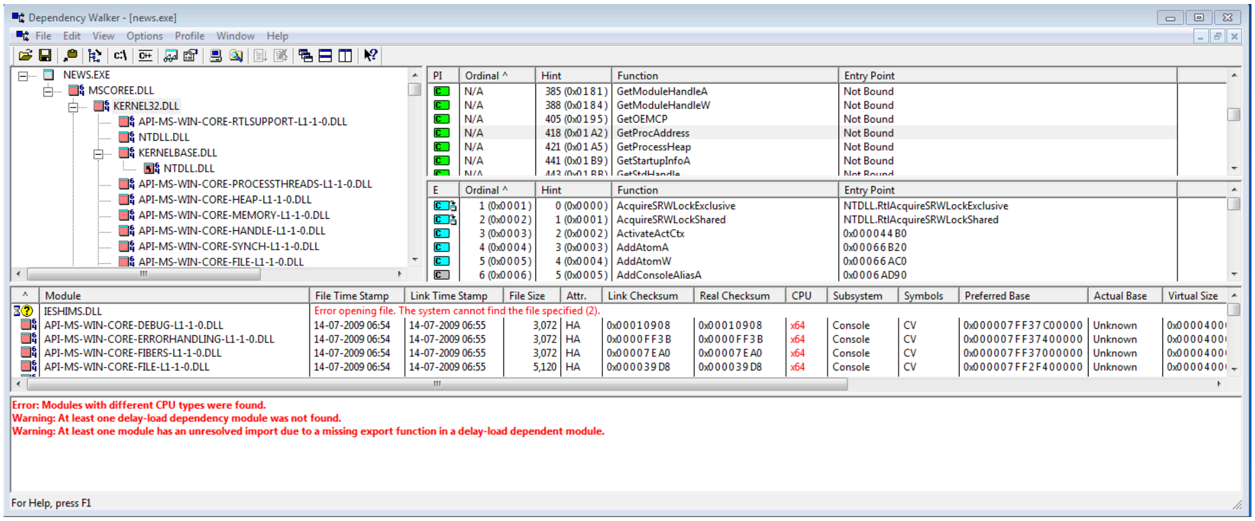
```
NEWS.EXE
  MSCOREE.DLL
    KERNEL32.DLL
      API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
      NTDLL.DLL
      KERNELBASE.DLL
        NTDLL.DLL
      API-MS-WIN-CORE-PROCESSTHREADS-L1-1-0.DLL
      API-MS-WIN-CORE-HEAP-L1-1-0.DLL
      API-MS-WIN-CORE-MEMORY-L1-1-0.DLL
      API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
      API-MS-WIN-CORE-SYNCH-L1-1-0.DLL
      API-MS-WIN-CORE-FILE-L1-1-0.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	88 (0x0058)	CreateFileMappingW	Not Bound
C	N/A	89 (0x0059)	CreateFileW	Not Bound
C	N/A	100 (0x0064)	CreateMutexW	Not Bound
C	N/A	111 (0x006F)	CreateSemaphoreW	Not Bound
C	N/A	113 (0x0071)	CreateThread	Not Bound
C	N/A	116 (0x0074)	CreateToolhelp32Snapshot	Not Bound
C	N/A	123 (0x007B)	DebugBreak	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
C	2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
C	3 (0x0003)	2 (0x0002)	ActivateActCtx	0x000044B0
C	4 (0x0004)	3 (0x0003)	AddAtomA	0x00066B20
C	5 (0x0005)	4 (0x0004)	AddAtomW	0x00066AC0
C	6 (0x0006)	5 (0x0005)	AddConsoleAliasA	0x0006AD90

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
⧗?	IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).											
	API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00010908	0x00010908	x64	Console	CV	0x000007FF37C00000	Unknown	0x0004000
	API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000FF3B	0x0000FF3B	x64	Console	CV	0x000007FF37400000	Unknown	0x0004000
	API-MS-WIN-CORE-FIBERS-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00007EA0	0x00007EA0	x64	Console	CV	0x000007FF37000000	Unknown	0x0004000
	API-MS-WIN-CORE-FILE-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	5,120	HA	0x000039D8	0x000039D8	x64	Console	CV	0x000007FF2F400000	Unknown	0x0004000

```
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```



```
NEWS.EXE
  MSCOREE.DLL
    KERNEL32.DLL
      API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
      NTDLL.DLL
      KERNELBASE.DLL
        NTDLL.DLL
      API-MS-WIN-CORE-PROCESSTHREADS-L1-1-0.DLL
      API-MS-WIN-CORE-HEAP-L1-1-0.DLL
      API-MS-WIN-CORE-MEMORY-L1-1-0.DLL
      API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
      API-MS-WIN-CORE-SYNCH-L1-1-0.DLL
      API-MS-WIN-CORE-FILE-L1-1-0.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	385 (0x0181)	GetModuleHandleA	Not Bound
C	N/A	388 (0x0184)	GetModuleHandleW	Not Bound
C	N/A	405 (0x0195)	GetOEMCP	Not Bound
C	N/A	418 (0x01A2)	GetProcAddress	Not Bound
C	N/A	421 (0x01A5)	GetProcessHeap	Not Bound
C	N/A	441 (0x01B9)	GetStartupInfoA	Not Bound
C	N/A	443 (0x01BB)	GetStdHandle	Not Bound

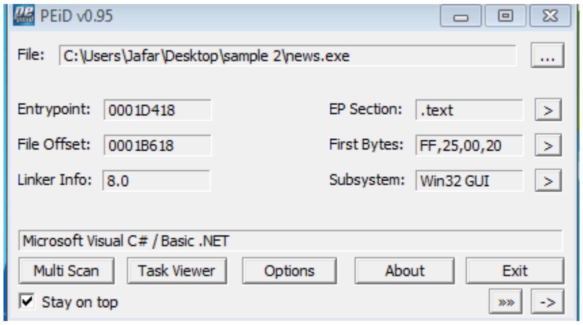
E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
C	2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
C	3 (0x0003)	2 (0x0002)	ActivateActCtx	0x000044B0
C	4 (0x0004)	3 (0x0003)	AddAtomA	0x00066B20
C	5 (0x0005)	4 (0x0004)	AddAtomW	0x00066AC0
C	6 (0x0006)	5 (0x0005)	AddConsoleAliasA	0x0006AD90

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
⧗?	IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).											
	API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00010908	0x00010908	x64	Console	CV	0x000007FF37C00000	Unknown	0x0004000
	API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000FF3B	0x0000FF3B	x64	Console	CV	0x000007FF37400000	Unknown	0x0004000
	API-MS-WIN-CORE-FIBERS-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00007EA0	0x00007EA0	x64	Console	CV	0x000007FF37000000	Unknown	0x0004000
	API-MS-WIN-CORE-FILE-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	5,120	HA	0x000039D8	0x000039D8	x64	Console	CV	0x000007FF2F400000	Unknown	0x0004000

```
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```

The imported DLLs use functions to create mutexes (mutual exclusion objects) that show the possibility of the file being a malware.

5. Is the file packed/obfuscated?



File: C:\Users\Jafar\Desktop\sample 2\news.exe

Entrypoint: 0001D418

EP Section: .text

File Offset: 0001B618

First Bytes: FF,25,00,20

Linker Info: 8.0

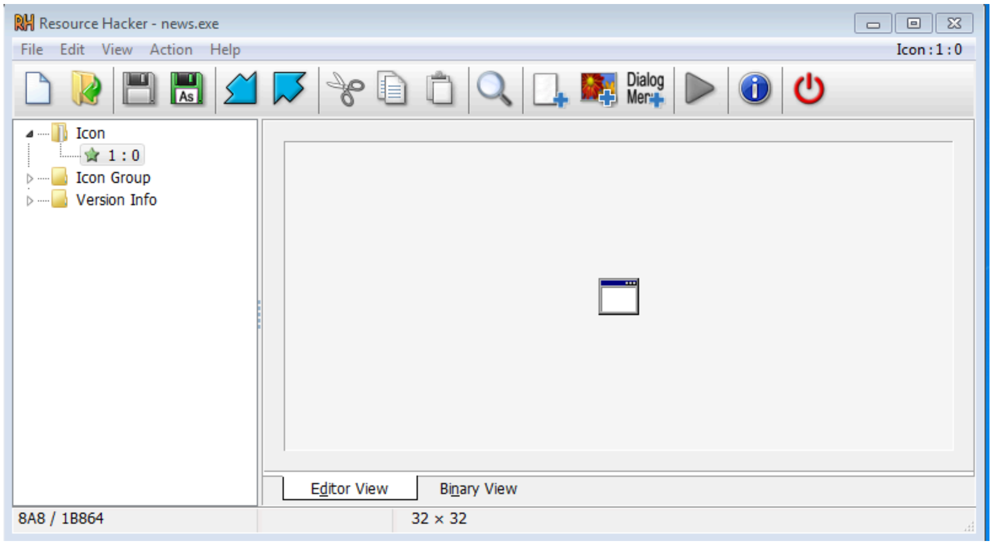
Subsystem: Win32 GUI

Microsoft Visual C# / Basic .NET

☑ Stay on top

No the file is not packed.

6. If GUI, then analyse its resources



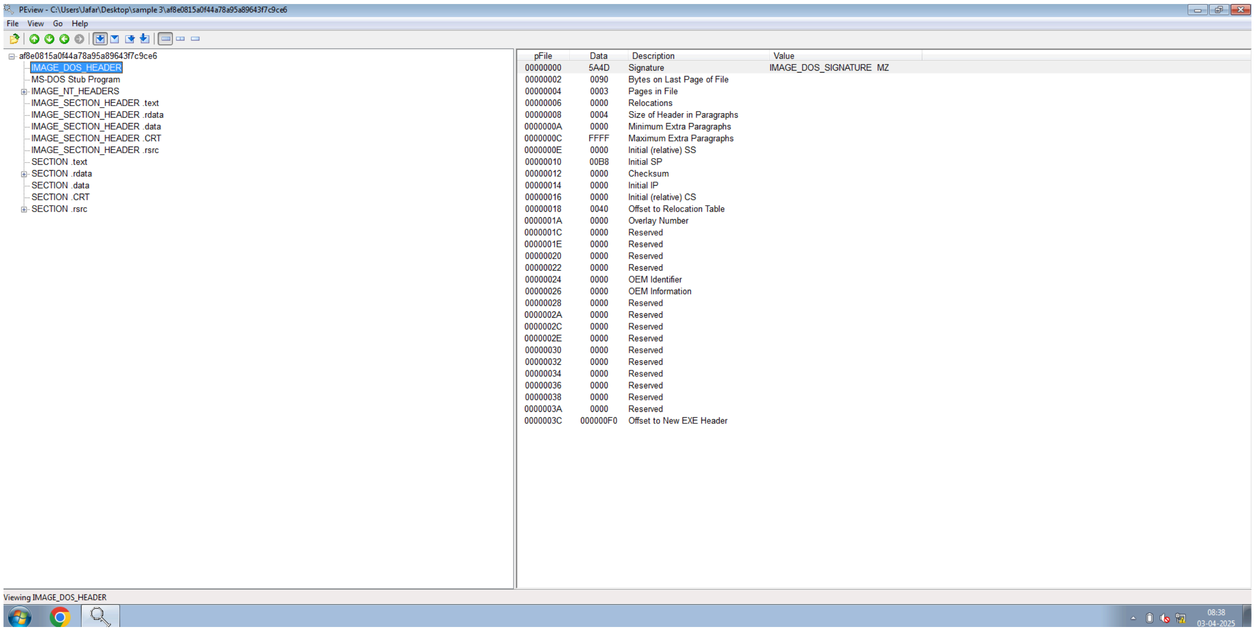
No useful information was retrieved from Resource Hacker.

7. What is the file trying to do?

The potential malware file is trying to communicate with an external machine and transfer files or sensitive information. It is able to track the infected system’s processes using mutexes and is modifying them simultaneously.

SAMPLE 03 - SYRIAN MALWARE

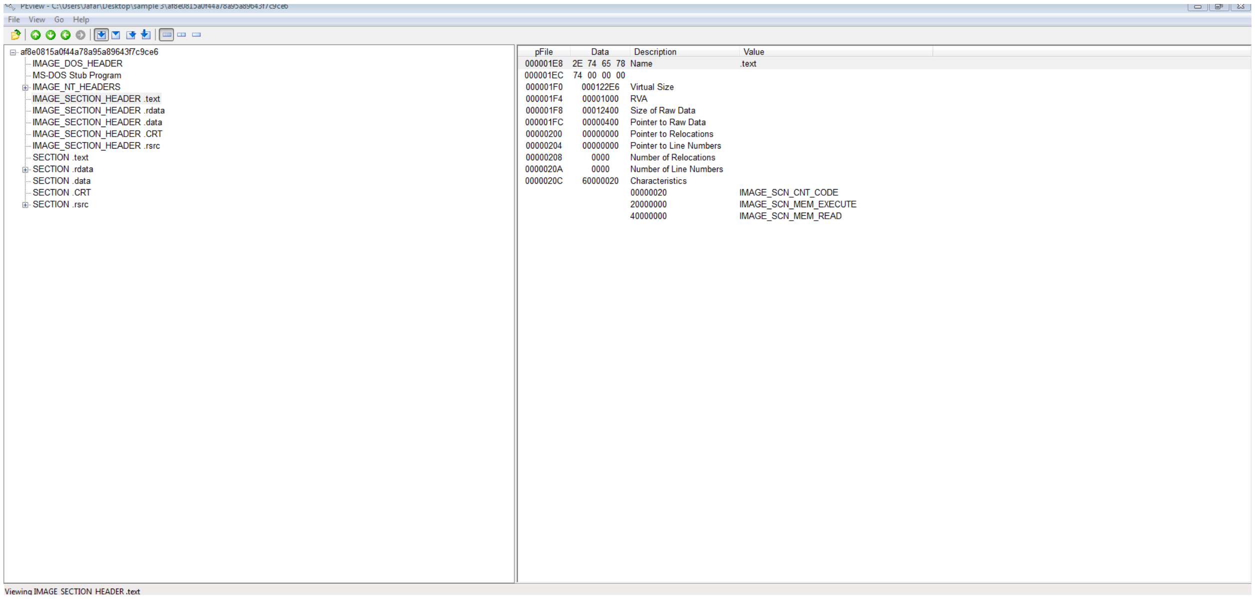
1. PE Header Information


PEview - C:\Users\Jafar\Desktop\sample 3\af8e0815a0f44a78a95a89643f7c9ce6
File View Go Help
af8e0815a0f44a78a95a89643f7c9ce6
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .CRT
IMAGE_SECTION_HEADER .rsrc
SECTION .text
SECTION .rdata
SECTION .data
SECTION .CRT
SECTION .rsrc
Viewing IMAGE_DOS_HEADER
08:38
03-04-2025

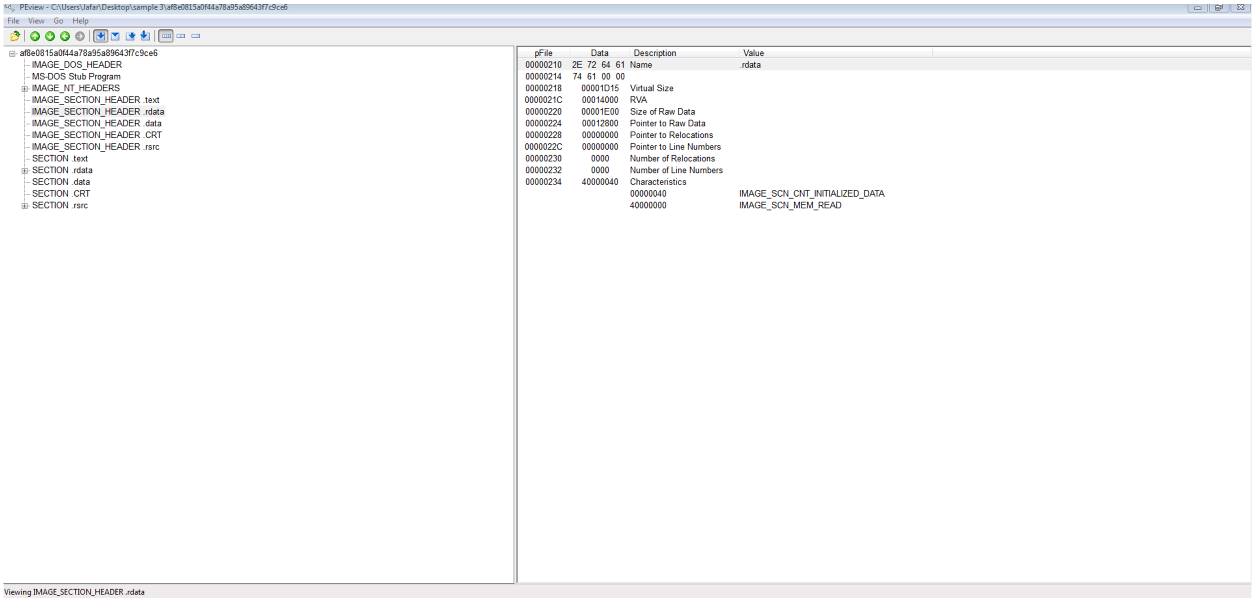
```
pFile     Data      Description                    Value
00000000  5A4D      Signature                      IMAGE_DOS_SIGNATURE  MZ
00000002  0090      Bytes on Last Page of File
00000004  0003      Pages in File
00000006  0000      Relocations
00000008  0004      Size of Header in Paragraphs
0000000A  0000      Minimum Extra Paragraphs
0000000C  FFFF      Maximum Extra Paragraphs
0000000E  0000      Initial (relative) SS
00000010  00B8      Initial SP
00000012  0000      Checksum
00000014  0000      Initial IP
00000016  0000      Initial (relative) CS
00000018  0040      Offset to Relocation Table
0000001A  0000      Overlay Number
0000001C  0000      Reserved
0000001E  0000      Reserved
00000020  0000      Reserved
00000022  0000      Reserved
00000024  0000      OEM Identifier
00000026  0000      OEM Information
00000028  0000      Reserved
0000002A  0000      Reserved
0000002C  0000      Reserved
0000002E  0000      Reserved
00000030  0000      Reserved
00000032  0000      Reserved
00000034  0000      Reserved
00000036  0000      Reserved
00000038  0000      Reserved
0000003A  0000      Reserved
0000003C  000000F0  Offset to New EXE Header
```

The MS DOS header, now discontinued, provides the aforementioned information. However, significant details can be found from the NT headers and section headers.

2. PE Section Headers


PEview - C:\Users\Jafar\Desktop\sample 3\af8e0815a0f44a78a95a89643f7c9ce6
File View Go Help
af8e0815a0f44a78a95a89643f7c9ce6
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .CRT
IMAGE_SECTION_HEADER .rsrc
SECTION .text
SECTION .rdata
SECTION .data
SECTION .CRT
SECTION .rsrc
Viewing IMAGE_SECTION_HEADER .text

```
pFile     Data         Description               Value
000001E8  2E 74 65 78  Name                      .text
000001EC  74 00 00 00
000001F0  000122E6     Virtual Size
000001F4  00001000     RVA
000001F8  00012400     Size of Raw Data
000001FC  00000400     Pointer to Raw Data
00000200  00000000     Pointer to Relocations
00000204  00000000     Pointer to Line Numbers
00000208  0000         Number of Relocations
0000020A  0000         Number of Line Numbers
0000020C  60000020     Characteristics
                       00000020                  IMAGE_SCN_CNT_CODE
                       20000000                  IMAGE_SCN_MEM_EXECUTE
                       40000000                  IMAGE_SCN_MEM_READ
```

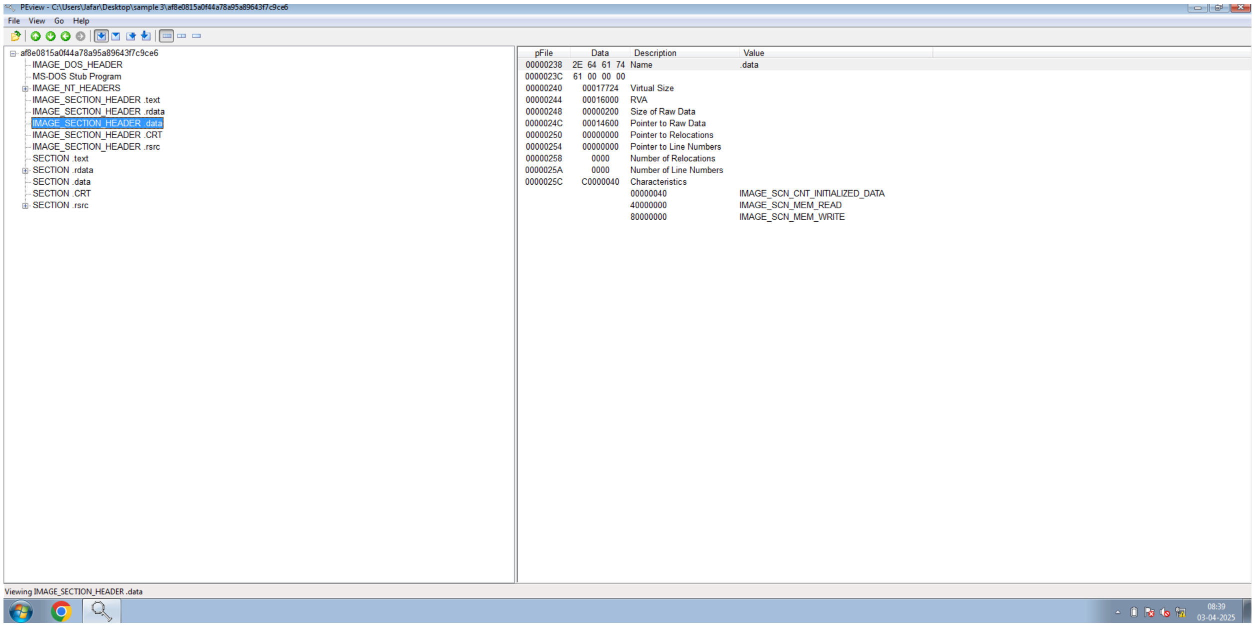


PEview - C:\Users\Jafar\Desktop\sample 3\af8e0815a0f44a78a95a89643f7c9ce6

```
af8e0815a0f44a78a95a89643f7c9ce6
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .CRT
  IMAGE_SECTION_HEADER .rsrc
  SECTION .text
  SECTION .rdata
  SECTION .data
  SECTION .CRT
  SECTION .rsrc
```

```
pFile     Data         Description              Value
00000210  2E 72 64 61  Name                     .rdata
00000214  74 61 00 00
00000218  00001D15     Virtual Size
0000021C  00014000     RVA
00000220  00001E00     Size of Raw Data
00000224  00012800     Pointer to Raw Data
00000228  00000000     Pointer to Relocations
0000022C  00000000     Pointer to Line Numbers
00000230  0000         Number of Relocations
00000232  0000         Number of Line Numbers
00000234  40000040     Characteristics
                       00000040                 IMAGE_SCN_CNT_INITIALIZED_DATA
                       40000000                 IMAGE_SCN_MEM_READ
```

Viewing IMAGE_SECTION_HEADER .rdata

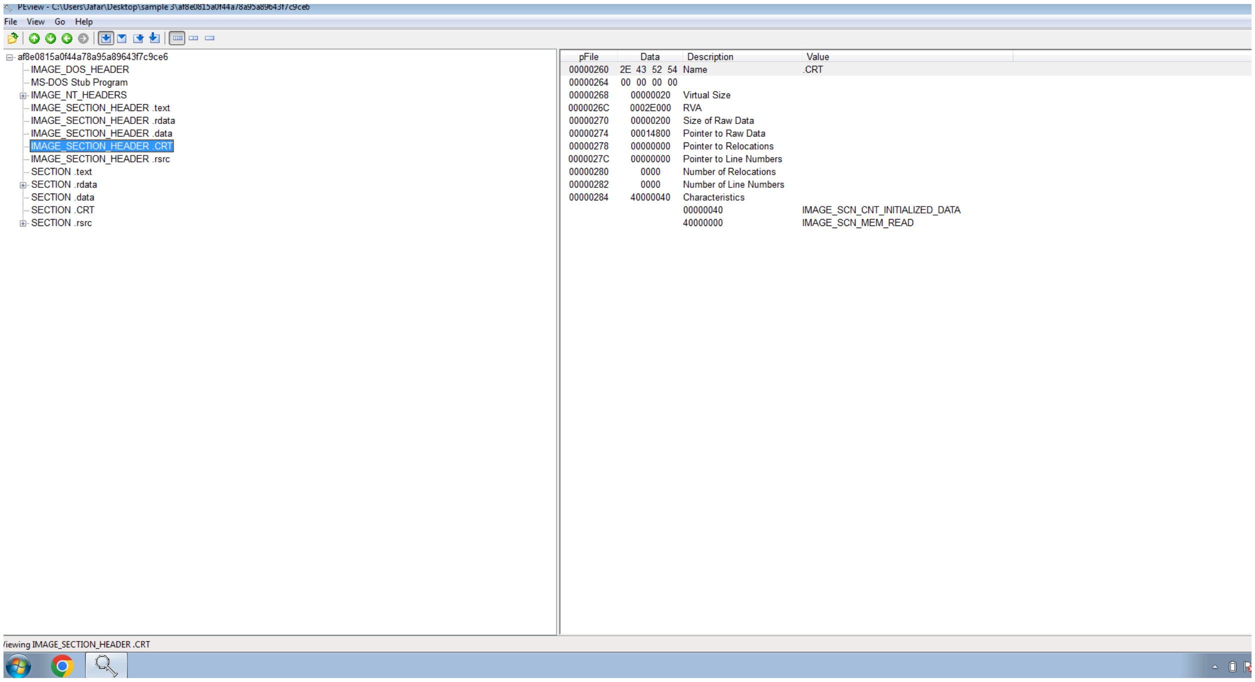


PEview - C:\Users\Jafar\Desktop\sample 3\af8e0815a0f44a78a95a89643f7c9ce6

```
af8e0815a0f44a78a95a89643f7c9ce6
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .CRT
  IMAGE_SECTION_HEADER .rsrc
  SECTION .text
  SECTION .rdata
  SECTION .data
  SECTION .CRT
  SECTION .rsrc
```

```
pFile     Data         Description              Value
00000238  2E 64 61 74  Name                     .data
0000023C  61 00 00 00
00000240  00017724     Virtual Size
00000244  00016000     RVA
00000248  00000200     Size of Raw Data
0000024C  00014600     Pointer to Raw Data
00000250  00000000     Pointer to Relocations
00000254  00000000     Pointer to Line Numbers
00000258  0000         Number of Relocations
0000025A  0000         Number of Line Numbers
0000025C  C0000040     Characteristics
                       00000040                 IMAGE_SCN_CNT_INITIALIZED_DATA
                       40000000                 IMAGE_SCN_MEM_READ
                       80000000                 IMAGE_SCN_MEM_WRITE
```

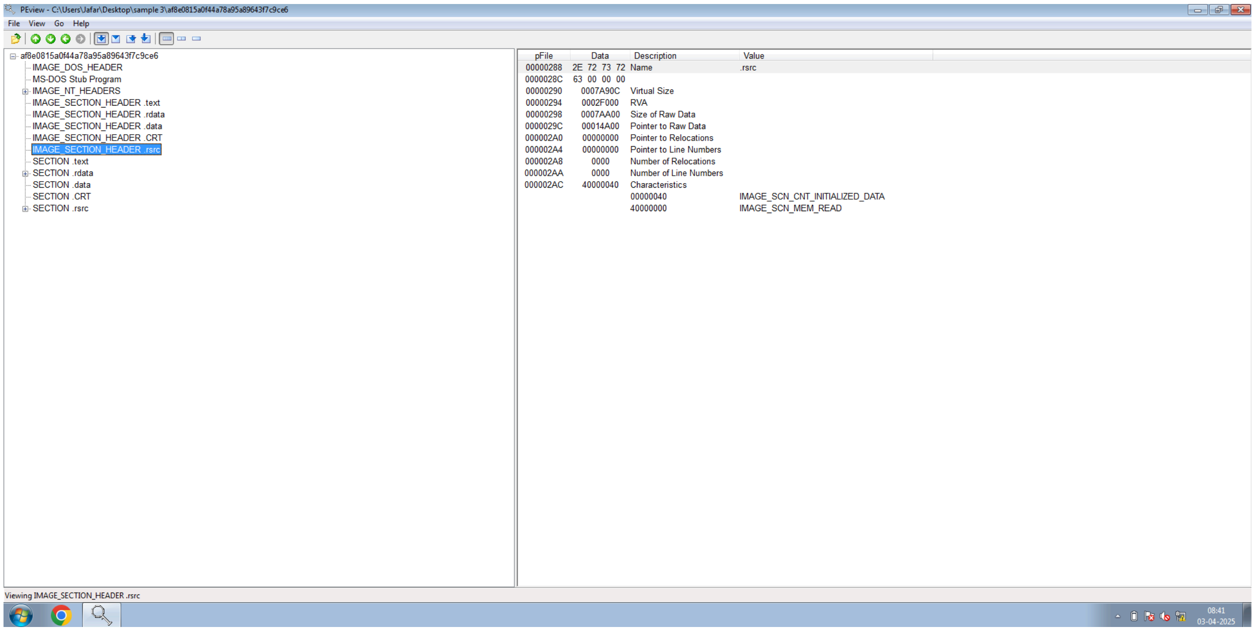
Viewing IMAGE_SECTION_HEADER .data


PEview - C:\Users\Jafar\Desktop\sample 3\af8e0815a0f44a78a95a89643f7c9ce6
File View Go Help

```
af8e0815a0f44a78a95a89643f7c9ce6
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .CRT
  IMAGE_SECTION_HEADER .rsrc
  SECTION .text
  SECTION .rdata
  SECTION .data
  SECTION .CRT
  SECTION .rsrc
```

```
pFile      Data          Description              Value
00000260   2E 43 52 54   Name                     .CRT
00000264   00 00 00 00
00000268   00000020      Virtual Size
0000026C   0002E000      RVA
00000270   00000200      Size of Raw Data
00000274   00014800      Pointer to Raw Data
00000278   00000000      Pointer to Relocations
0000027C   00000000      Pointer to Line Numbers
00000280   0000          Number of Relocations
00000282   0000          Number of Line Numbers
00000284   40000040      Characteristics
                         00000040                 IMAGE_SCN_CNT_INITIALIZED_DATA
                         40000000                 IMAGE_SCN_MEM_READ
```

Viewing IMAGE_SECTION_HEADER .CRT


PEview - C:\Users\Jafar\Desktop\sample 3\af8e0815a0f44a78a95a89643f7c9ce6
File View Go Help
08:41
03-04-2025

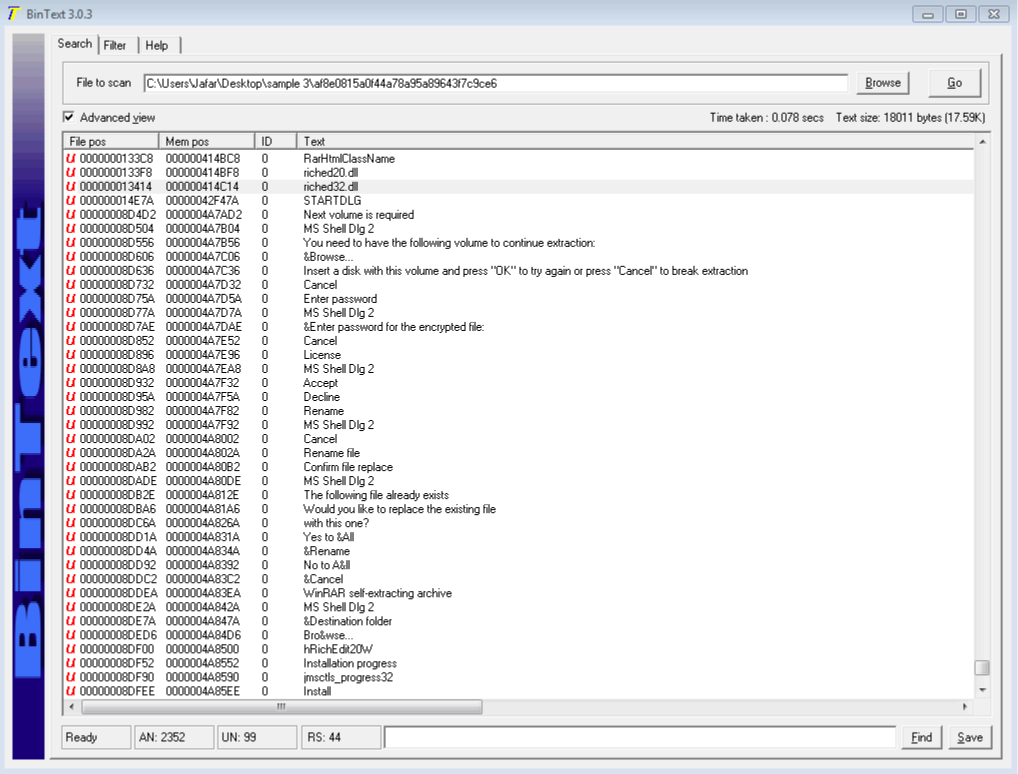
```
af8e0815a0f44a78a95a89643f7c9ce6
  IMAGE_DOS_HEADER
  MS-DOS Stub Program
  IMAGE_NT_HEADERS
  IMAGE_SECTION_HEADER .text
  IMAGE_SECTION_HEADER .rdata
  IMAGE_SECTION_HEADER .data
  IMAGE_SECTION_HEADER .CRT
  IMAGE_SECTION_HEADER .rsrc
  SECTION .text
  SECTION .rdata
  SECTION .data
  SECTION .CRT
  SECTION .rsrc
```

```
pFile      Data          Description              Value
00000288   2E 72 73 72   Name                     .rsrc
0000028C   63 00 00 00
00000290   0007A90C      Virtual Size
00000294   0002F000      RVA
00000298   0007AA00      Size of Raw Data
0000029C   00014A00      Pointer to Raw Data
000002A0   00000000      Pointer to Relocations
000002A4   00000000      Pointer to Line Numbers
000002A8   0000          Number of Relocations
000002AA   0000          Number of Line Numbers
000002AC   40000040      Characteristics
                         00000040                 IMAGE_SCN_CNT_INITIALIZED_DATA
                         40000000                 IMAGE_SCN_MEM_READ
```

Viewing IMAGE_SECTION_HEADER .rsrc

The section headers provide useful information about the 4 sections of the PE file and their associated details like Virtual Size and Size of Raw Data.

3. Strings Analysis

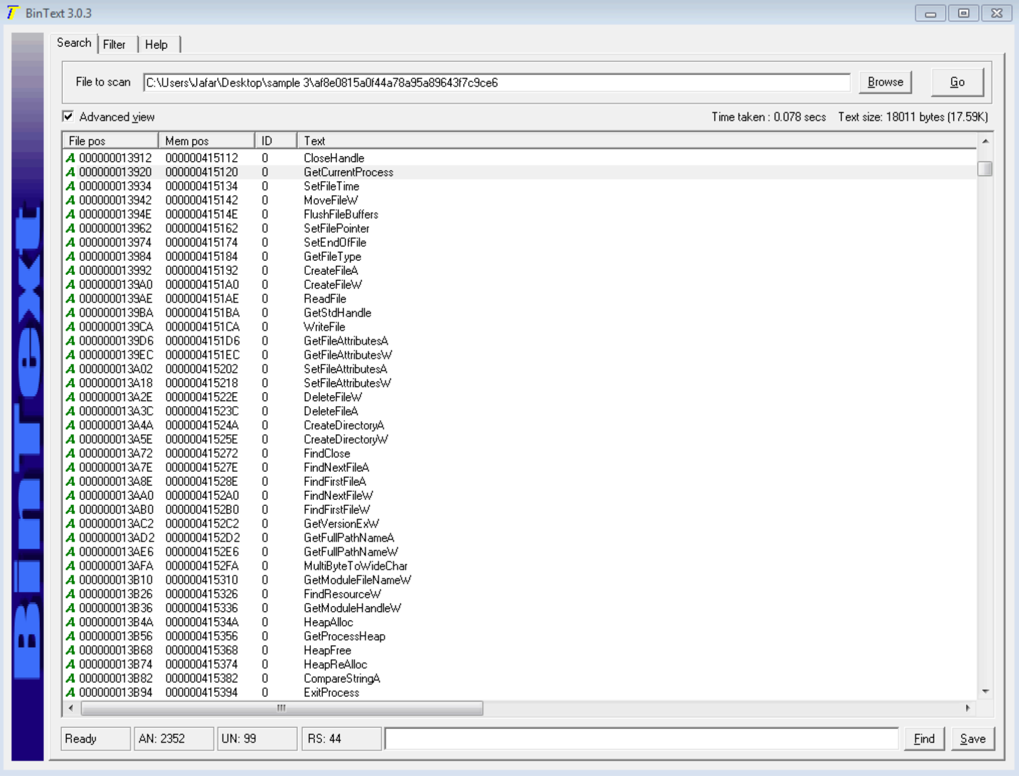


File to scan C:\Users\Jafar\Desktop\sample 3\af8e0815a0f44a78a95a89643f7c9ce6

☑ Advanced view   Time taken : 0.078 secs   Text size: 18011 bytes (17.59K)

```
File pos        Mem pos         ID   Text
U 0000000133C8  000000414BC8    0    RarHtmlClassName
U 0000000133F8  000000414BF8    0    riched20.dll
U 000000013414  000000414C14    0    riched32.dll
U 000000014E7A  00000042F47A    0    STARTDLG
U 00000008D4D2  0000004A7AD2    0    Next volume is required
U 00000008D504  0000004A7B04    0    MS Shell Dlg 2
U 00000008D556  0000004A7B56    0    You need to have the following volume to continue extraction:
U 00000008D606  0000004A7C06    0    &Browse...
U 00000008D636  0000004A7C36    0    Insert a disk with this volume and press "OK" to try again or press "Cancel" to break extraction
U 00000008D732  0000004A7D32    0    Cancel
U 00000008D75A  0000004A7D5A    0    Enter password
U 00000008D77A  0000004A7D7A    0    MS Shell Dlg 2
U 00000008D7AE  0000004A7DAE    0    &Enter password for the encrypted file:
U 00000008D852  0000004A7E52    0    Cancel
U 00000008D896  0000004A7E96    0    License
U 00000008D8A8  0000004A7EA8    0    MS Shell Dlg 2
U 00000008D932  0000004A7F32    0    Accept
U 00000008D95A  0000004A7F5A    0    Decline
U 00000008D982  0000004A7F82    0    Rename
U 00000008D992  0000004A7F92    0    MS Shell Dlg 2
U 00000008DA02  0000004A8002    0    Cancel
U 00000008DA2A  0000004A802A    0    Rename file
U 00000008DAB2  0000004A80B2    0    Confirm file replace
U 00000008DADE  0000004A80DE    0    MS Shell Dlg 2
U 00000008DB2E  0000004A812E    0    The following file already exists
U 00000008DBA6  0000004A81A6    0    Would you like to replace the existing file
U 00000008DC6A  0000004A826A    0    with this one?
U 00000008DD1A  0000004A831A    0    Yes to &All
U 00000008DD4A  0000004A834A    0    &Rename
U 00000008DD92  0000004A8392    0    No to A&ll
U 00000008DDC2  0000004A83C2    0    &Cancel
U 00000008DDEA  0000004A83EA    0    WinRAR self-extracting archive
U 00000008DE2A  0000004A842A    0    MS Shell Dlg 2
U 00000008DE7A  0000004A847A    0    &Destination folder
U 00000008DED6  0000004A84D6    0    Bro&wse...
U 00000008DF00  0000004A8500    0    hRichEdit20W
U 00000008DF52  0000004A8552    0    Installation progress
U 00000008DF90  0000004A8590    0    jmsctls_progress32
U 00000008DFEE  0000004A85EE    0    Install
```

Ready | AN: 2352 | UN: 99 | RS: 44



File to scan C:\Users\Jafar\Desktop\sample 3\af8e0815a0f44a78a95a89643f7c9ce6

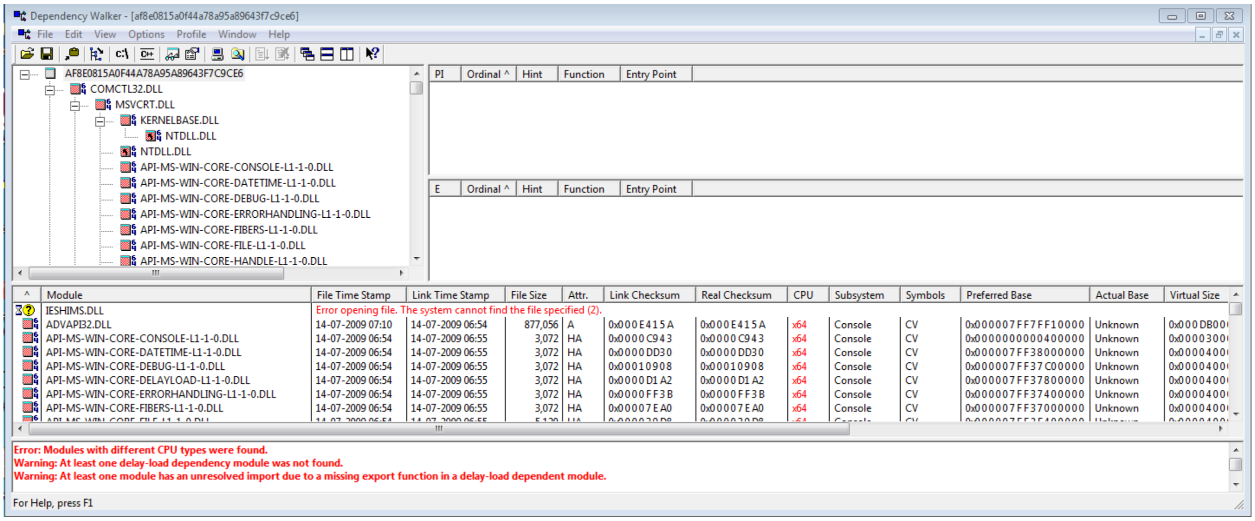
☑ Advanced view   Time taken : 0.078 secs   Text size: 18011 bytes (17.59K)

```
File pos        Mem pos         ID   Text
A 000000013912  000000415112    0    CloseHandle
A 000000013920  000000415120    0    GetCurrentProcess
A 000000013934  000000415134    0    SetFileTime
A 000000013942  000000415142    0    MoveFileW
A 00000001394E  00000041514E    0    FlushFileBuffers
A 000000013962  000000415162    0    SetFilePointer
A 000000013974  000000415174    0    SetEndOfFile
A 000000013984  000000415184    0    GetFileType
A 000000013992  000000415192    0    CreateFileA
A 0000000139A0  0000004151A0    0    CreateFileW
A 0000000139AE  0000004151AE    0    ReadFile
A 0000000139BA  0000004151BA    0    GetStdHandle
A 0000000139CA  0000004151CA    0    WriteFile
A 0000000139D6  0000004151D6    0    GetFileAttributesA
A 0000000139EC  0000004151EC    0    GetFileAttributesW
A 000000013A02  000000415202    0    SetFileAttributesA
A 000000013A18  000000415218    0    SetFileAttributesW
A 000000013A2E  00000041522E    0    DeleteFileW
A 000000013A3C  00000041523C    0    DeleteFileA
A 000000013A4A  00000041524A    0    CreateDirectoryA
A 000000013A5E  00000041525E    0    CreateDirectoryW
A 000000013A72  000000415272    0    FindClose
A 000000013A7E  00000041527E    0    FindNextFileA
A 000000013A8E  00000041528E    0    FindFirstFileA
A 000000013AA0  0000004152A0    0    FindNextFileW
A 000000013AB0  0000004152B0    0    FindFirstFileW
A 000000013AC2  0000004152C2    0    GetVersionExW
A 000000013AD2  0000004152D2    0    GetFullPathNameA
A 000000013AE6  0000004152E6    0    GetFullPathNameW
A 000000013AFA  0000004152FA    0    MultiByteToWideChar
A 000000013B10  000000415310    0    GetModuleFileNameW
A 000000013B26  000000415326    0    FindResourceW
A 000000013B36  000000415336    0    GetModuleHandleW
A 000000013B4A  00000041534A    0    HeapAlloc
A 000000013B56  000000415356    0    GetProcessHeap
A 000000013B68  000000415368    0    HeapFree
A 000000013B74  000000415374    0    HeapReAlloc
A 000000013B82  000000415382    0    CompareStringA
A 000000013B94  000000415394    0    ExitProcess
```

Ready | AN: 2352 | UN: 99 | RS: 44

New DLLs are being called along with file manipulation functions and mutexes.

4. Imports/Exports Analysis



Dependency Walker - [af8e0815a0f44a78a95a89643f7c9ce6]

```
AF8E0815A0F44A78A95A89643F7C9CE6
  COMCTL32.DLL
    MSVCRT.DLL
      KERNELBASE.DLL
        NTDLL.DLL
      NTDLL.DLL
      API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL
      API-MS-WIN-CORE-DATETIME-L1-1-0.DLL
      API-MS-WIN-CORE-DEBUG-L1-1-0.DLL
      API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL
      API-MS-WIN-CORE-FIBERS-L1-1-0.DLL
      API-MS-WIN-CORE-FILE-L1-1-0.DLL
      API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
```

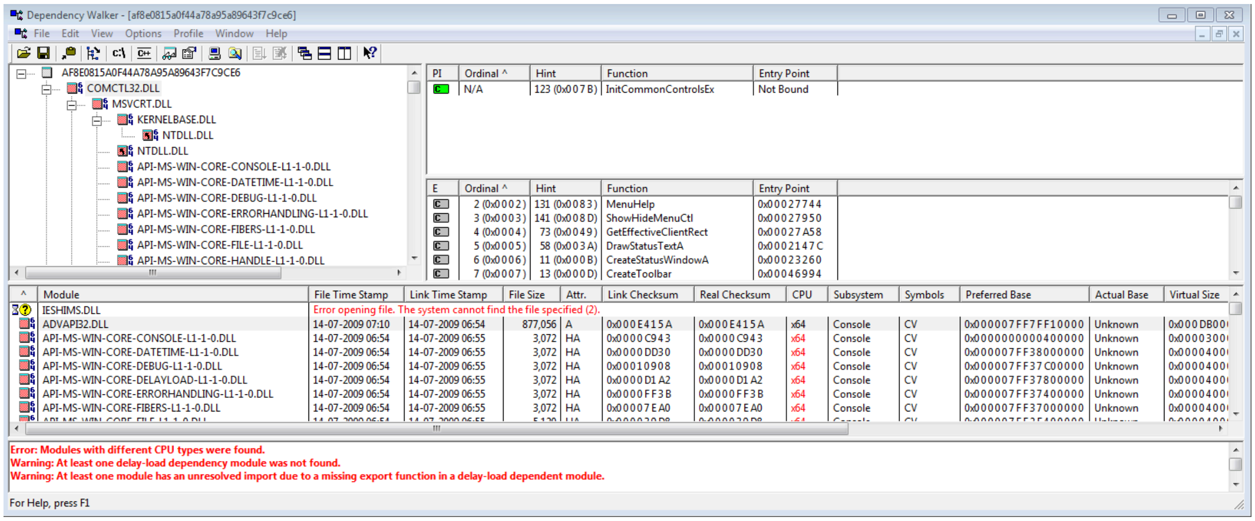
PI	Ordinal ^	Hint	Function	Entry Point

E	Ordinal ^	Hint	Function	Entry Point

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).											
ADVAPI32.DLL	14-07-2009 07:10	14-07-2009 06:54	877,056	A	0x000E415A	0x000E415A	x64	Console	CV	0x000007FF7FF10000	Unknown	0x000DB00
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000C943	0x0000C943	x64	Console	CV	0x0000000000400000	Unknown	0x0000300
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000DD30	0x0000DD30	x64	Console	CV	0x000007FF38000000	Unknown	0x0000400
API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00010908	0x00010908	x64	Console	CV	0x000007FF37C00000	Unknown	0x0000400
API-MS-WIN-CORE-DELAYLOAD-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000D1A2	0x0000D1A2	x64	Console	CV	0x000007FF37800000	Unknown	0x0000400
API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000FF3B	0x0000FF3B	x64	Console	CV	0x000007FF37400000	Unknown	0x0000400
API-MS-WIN-CORE-FIBERS-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00007EA0	0x00007EA0	x64	Console	CV	0x000007FF37000000	Unknown	0x0000400

```
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```

For Help, press F1



Dependency Walker - [af8e0815a0f44a78a95a89643f7c9ce6]

```
AF8E0815A0F44A78A95A89643F7C9CE6
  COMCTL32.DLL
    MSVCRT.DLL
      KERNELBASE.DLL
        NTDLL.DLL
      NTDLL.DLL
      API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL
      API-MS-WIN-CORE-DATETIME-L1-1-0.DLL
      API-MS-WIN-CORE-DEBUG-L1-1-0.DLL
      API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL
      API-MS-WIN-CORE-FIBERS-L1-1-0.DLL
      API-MS-WIN-CORE-FILE-L1-1-0.DLL
      API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
🟩	N/A	123 (0x007B)	InitCommonControlsEx	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
C	2 (0x0002)	131 (0x0083)	MenuHelp	0x00027744
C	3 (0x0003)	141 (0x008D)	ShowHideMenuCtl	0x00027950
C	4 (0x0004)	73 (0x0049)	GetEffectiveClientRect	0x00027A58
C	5 (0x0005)	58 (0x003A)	DrawStatusTextA	0x0002147C
C	6 (0x0006)	11 (0x000B)	CreateStatusWindowA	0x00023260
C	7 (0x0007)	13 (0x000D)	CreateToolbar	0x00046994

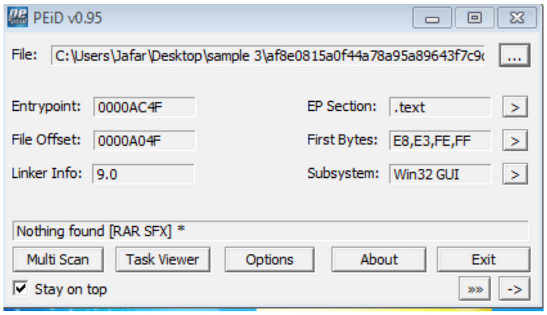
Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).											
ADVAPI32.DLL	14-07-2009 07:10	14-07-2009 06:54	877,056	A	0x000E415A	0x000E415A	x64	Console	CV	0x000007FF7FF10000	Unknown	0x000DB00
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000C943	0x0000C943	x64	Console	CV	0x0000000000400000	Unknown	0x0000300
API-MS-WIN-CORE-DATETIME-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000DD30	0x0000DD30	x64	Console	CV	0x000007FF38000000	Unknown	0x0000400
API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00010908	0x00010908	x64	Console	CV	0x000007FF37C00000	Unknown	0x0000400
API-MS-WIN-CORE-DELAYLOAD-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000D1A2	0x0000D1A2	x64	Console	CV	0x000007FF37800000	Unknown	0x0000400
API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000FF3B	0x0000FF3B	x64	Console	CV	0x000007FF37400000	Unknown	0x0000400
API-MS-WIN-CORE-FIBERS-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00007EA0	0x00007EA0	x64	Console	CV	0x000007FF37000000	Unknown	0x0000400

```
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```

For Help, press F1

Different DLLs are importing NTDLL.dll which is a suspicious indicator of the file being a malware executable.

5. Is the file packed/obfuscated?



PEiD v0.95

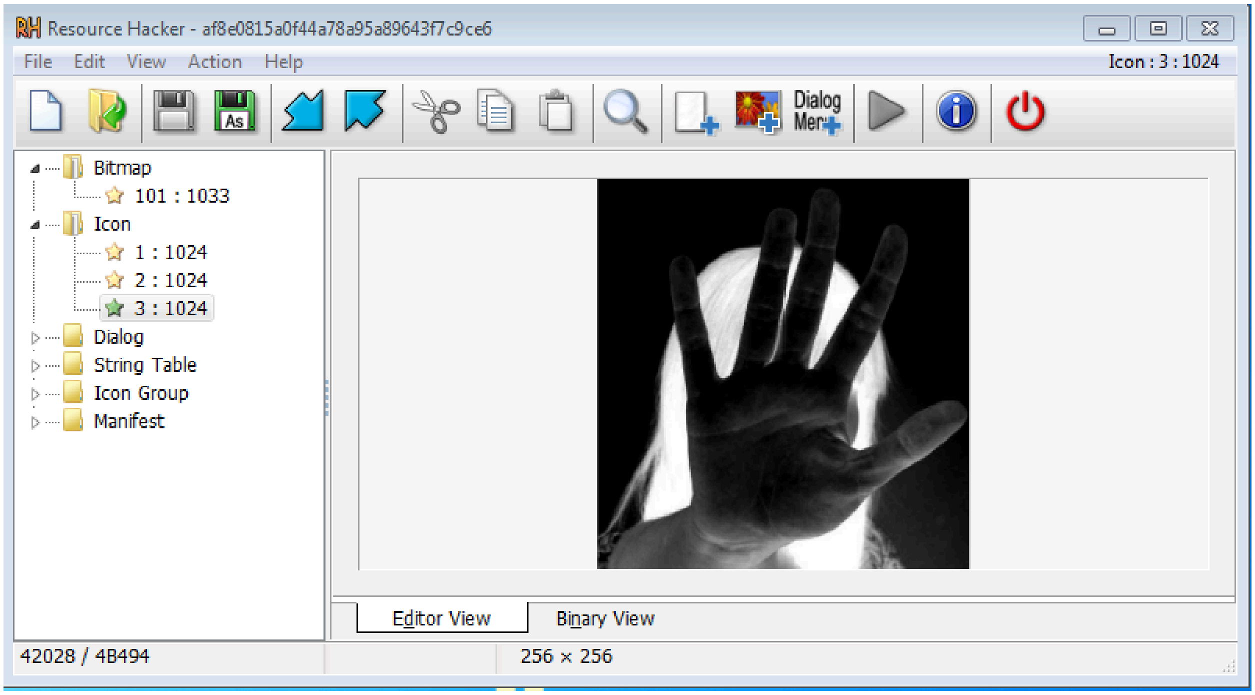
File:	C:\Users\Jafar\Desktop\sample 3\af8e0815a0f44a78a95a89643f7c9		
Entrypoint:	0000AC4F	EP Section:	.text
File Offset:	0000A04F	First Bytes:	E8,E3,FE,FF
Linker Info:	9.0	Subsystem:	Win32 GUI

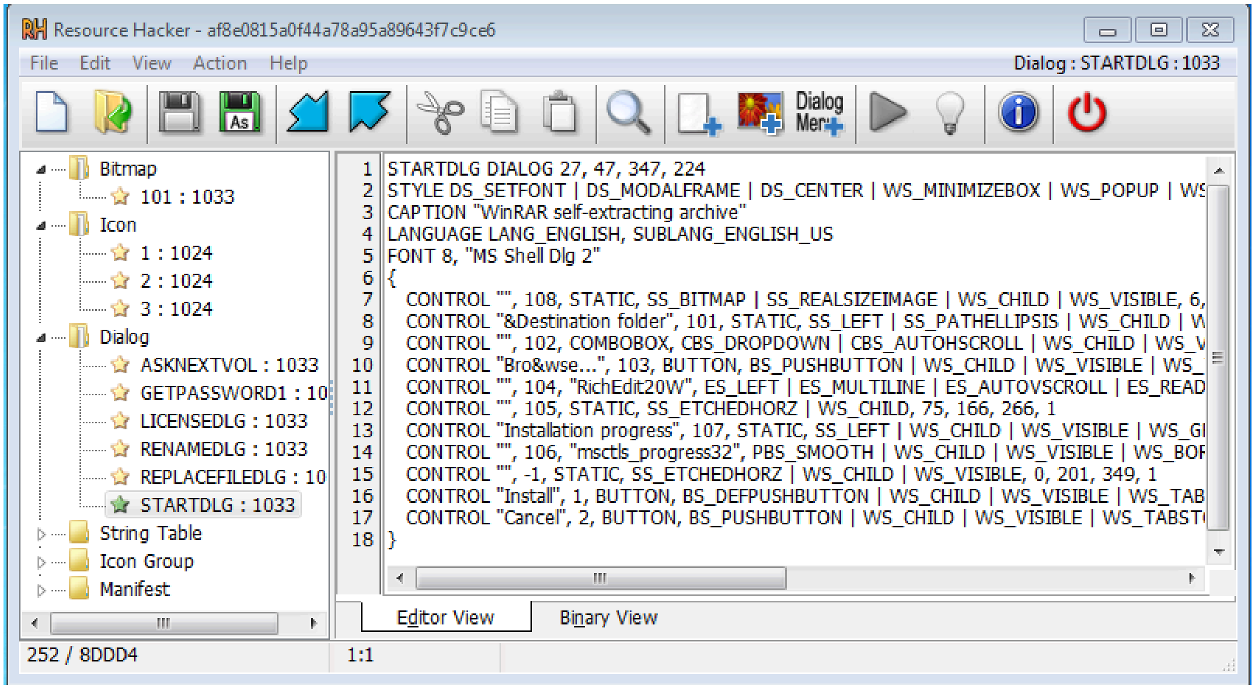
Nothing found [RAR SFX] *

☑ Stay on top

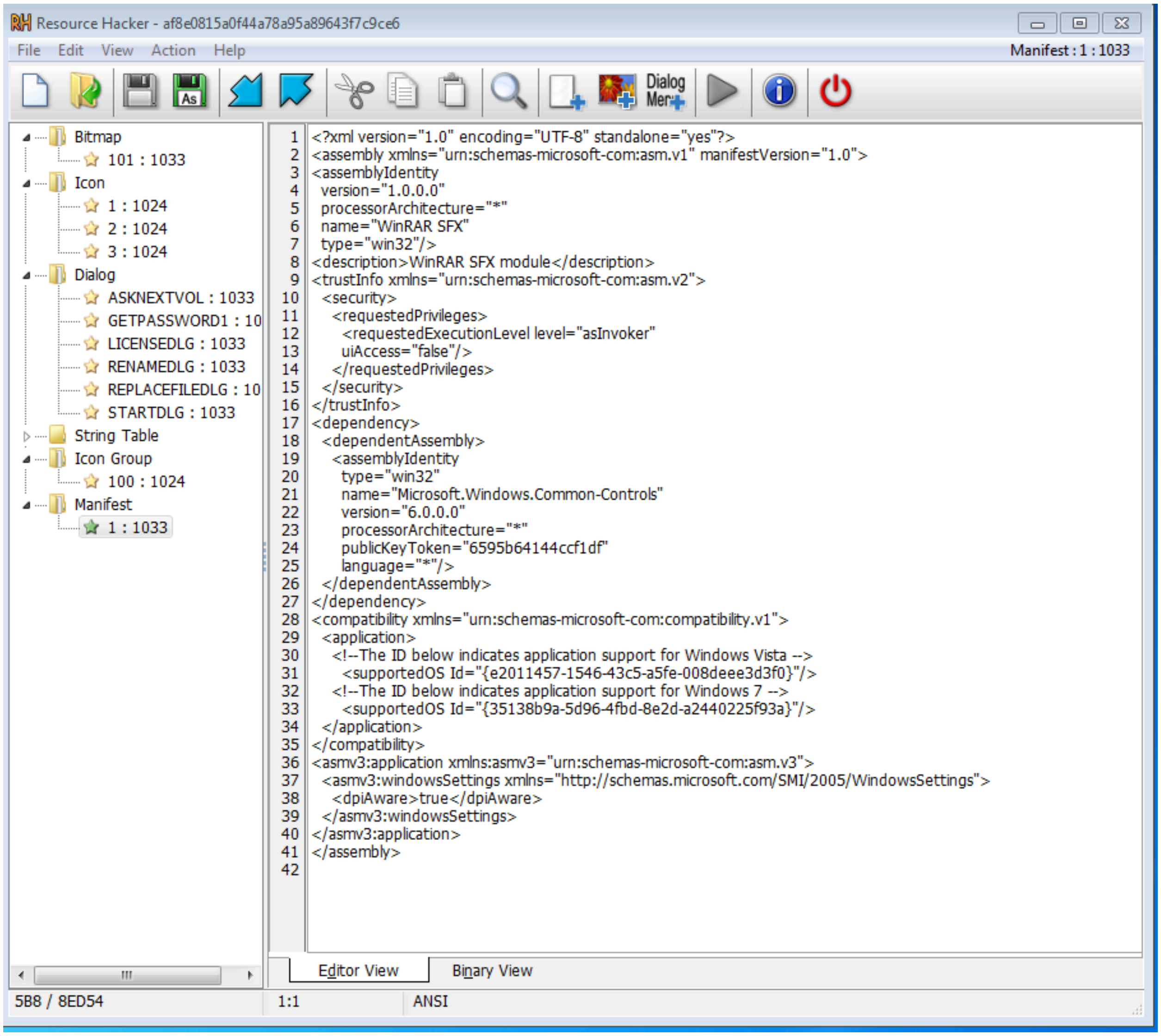
No the file is not packed.

6. If GUI, then analyse its resources.





```
STARTDLG DIALOG 27, 47, 347, 224
STYLE DS_SETFONT | DS_MODALFRAME | DS_CENTER | WS_MINIMIZEBOX | WS_POPUP | WS
CAPTION "WinRAR self-extracting archive"
LANGUAGE LANG_ENGLISH, SUBLANG_ENGLISH_US
FONT 8, "MS Shell Dlg 2"
{
   CONTROL "", 108, STATIC, SS_BITMAP | SS_REALSIZEIMAGE | WS_CHILD | WS_VISIBLE, 6,
   CONTROL "&Destination folder", 101, STATIC, SS_LEFT | SS_PATHELLIPSIS | WS_CHILD | W
   CONTROL "", 102, COMBOBOX, CBS_DROPDOWN | CBS_AUTOHSCROLL | WS_CHILD | WS_V
   CONTROL "Bro&wse...", 103, BUTTON, BS_PUSHBUTTON | WS_CHILD | WS_VISIBLE | WS_
   CONTROL "", 104, "RichEdit20W", ES_LEFT | ES_MULTILINE | ES_AUTOVSCROLL | ES_READ
   CONTROL "", 105, STATIC, SS_ETCHEDHORZ | WS_CHILD, 75, 166, 266, 1
   CONTROL "Installation progress", 107, STATIC, SS_LEFT | WS_CHILD | WS_VISIBLE | WS_GI
   CONTROL "", 106, "msctls_progress32", PBS_SMOOTH | WS_CHILD | WS_VISIBLE | WS_BOF
   CONTROL "", -1, STATIC, SS_ETCHEDHORZ | WS_CHILD | WS_VISIBLE, 0, 201, 349, 1
   CONTROL "Install", 1, BUTTON, BS_DEFPUSHBUTTON | WS_CHILD | WS_VISIBLE | WS_TAB
   CONTROL "Cancel", 2, BUTTON, BS_PUSHBUTTON | WS_CHILD | WS_VISIBLE | WS_TABST
}
```



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
 version="1.0.0.0"
 processorArchitecture="*"
 name="WinRAR SFX"
 type="win32"/>
<description>WinRAR SFX module</description>
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
 <security>
  <requestedPrivileges>
   <requestedExecutionLevel level="asInvoker"
   uiAccess="false"/>
  </requestedPrivileges>
 </security>
</trustInfo>
<dependency>
 <dependentAssembly>
  <assemblyIdentity
   type="win32"
   name="Microsoft.Windows.Common-Controls"
   version="6.0.0.0"
   processorArchitecture="*"
   publicKeyToken="6595b64144ccf1df"
   language="*"/>
 </dependentAssembly>
</dependency>
<compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">
 <application>
  <!--The ID below indicates application support for Windows Vista -->
   <supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}"/>
  <!--The ID below indicates application support for Windows 7 -->
   <supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"/>
 </application>
</compatibility>
<asmv3:application xmlns:asmv3="urn:schemas-microsoft-com:asm.v3">
 <asmv3:windowsSettings xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">
  <dpiAware>true</dpiAware>
 </asmv3:windowsSettings>
</asmv3:application>
</assembly>
```

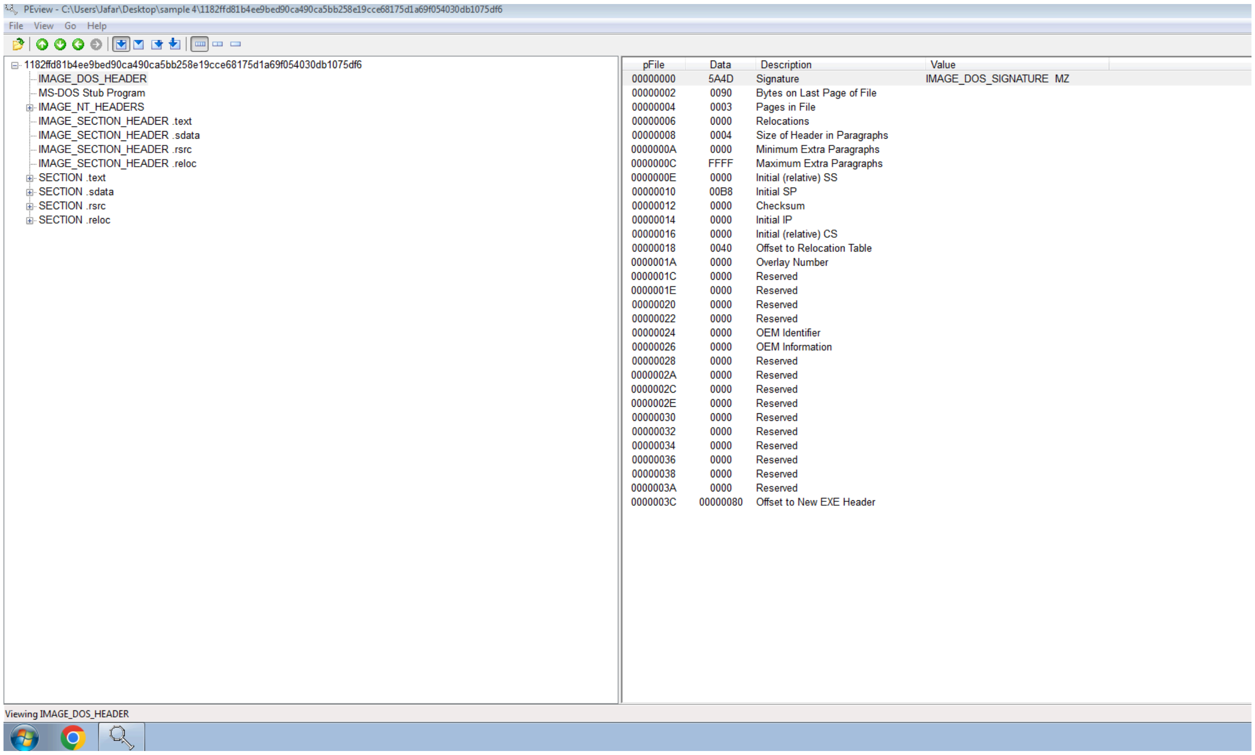
Resource Hacker provides us with an image that seems suspicious along with the manifest file of the executable.

7. What is the file trying to do with suspicious functions?

The file is a potential malware that does file manipulation using functions like CreateFile and DeleteFile repeated;y along with process manipulation using mutexes. No IP address is found, so the possibility of external communication can be ruled out.

SAMPLE 04 - SYRIAN MALWARE

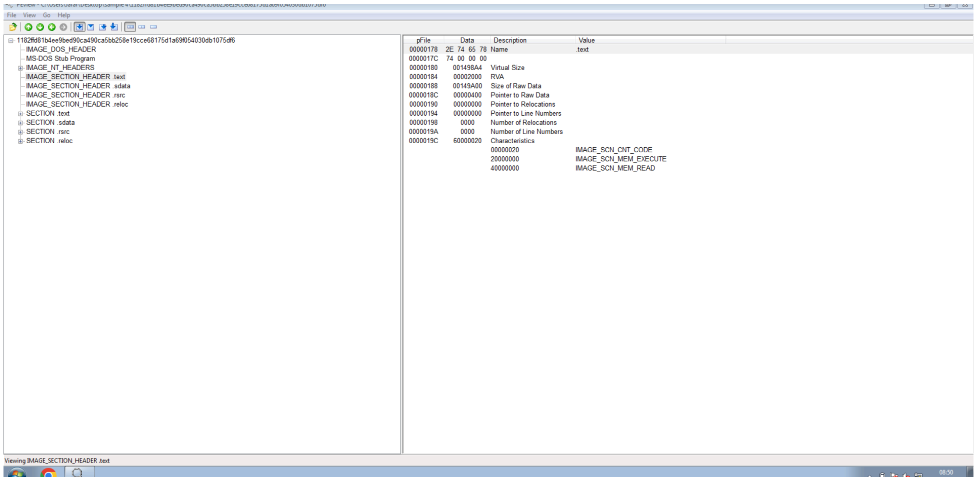
1. PE Header Information



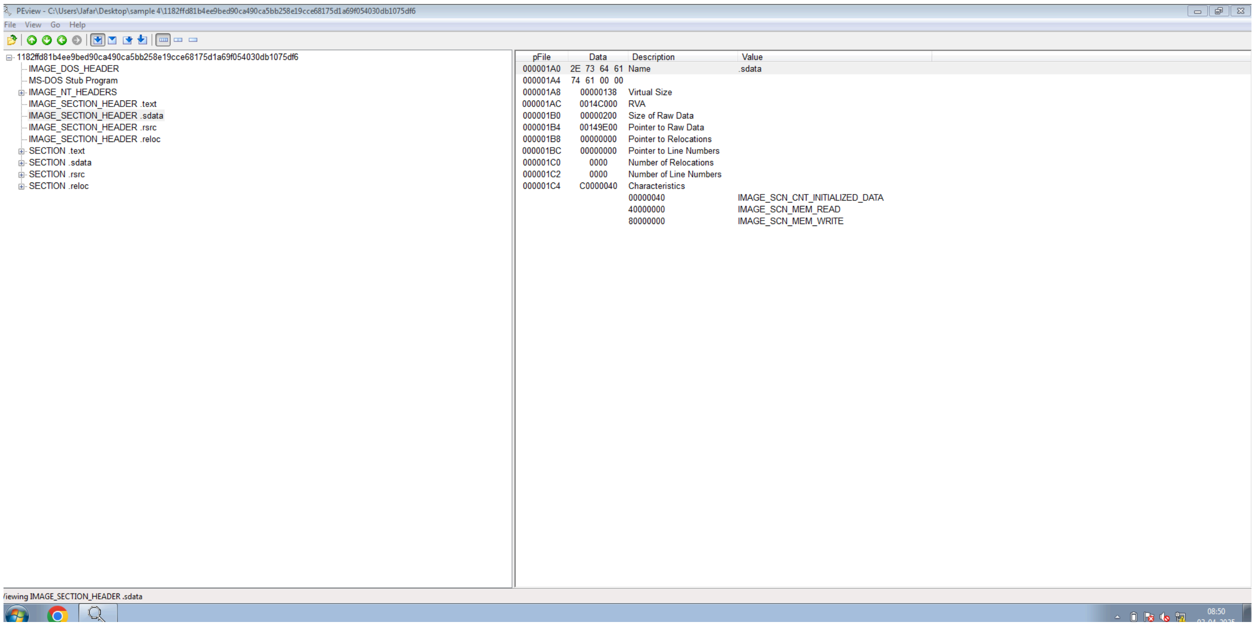
```
PEview - C:\Users\Jafar\Desktop\sample 4\1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1075df6

1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1075df6
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
  + IMAGE_NT_HEADERS
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .sdata
    IMAGE_SECTION_HEADER .rsrc
    IMAGE_SECTION_HEADER .reloc
  + SECTION .text
  + SECTION .sdata
  + SECTION .rsrc
  + SECTION .reloc

pFile      Data      Description                    Value
00000000   5A4D      Signature                      IMAGE_DOS_SIGNATURE  MZ
00000002   0090      Bytes on Last Page of File
00000004   0003      Pages in File
00000006   0000      Relocations
00000008   0004      Size of Header in Paragraphs
0000000A   0000      Minimum Extra Paragraphs
0000000C   FFFF      Maximum Extra Paragraphs
0000000E   0000      Initial (relative) SS
00000010   00B8      Initial SP
00000012   0000      Checksum
00000014   0000      Initial IP
00000016   0000      Initial (relative) CS
00000018   0040      Offset to Relocation Table
0000001A   0000      Overlay Number
0000001C   0000      Reserved
0000001E   0000      Reserved
00000020   0000      Reserved
00000022   0000      Reserved
00000024   0000      OEM Identifier
00000026   0000      OEM Information
00000028   0000      Reserved
0000002A   0000      Reserved
0000002C   0000      Reserved
0000002E   0000      Reserved
00000030   0000      Reserved
00000032   0000      Reserved
00000034   0000      Reserved
00000036   0000      Reserved
00000038   0000      Reserved
0000003A   0000      Reserved
0000003C   00000080  Offset to New EXE Header

Viewing IMAGE_DOS_HEADER
```

The MS DOS header, now discontinued, provides the aforementioned information. However, significant details can be found from the NT headers and section headers.

2. PE Section Headers



```
1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1075df6
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
  + IMAGE_NT_HEADERS
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .sdata
    IMAGE_SECTION_HEADER .rsrc
    IMAGE_SECTION_HEADER .reloc
  + SECTION .text
  + SECTION .sdata
  + SECTION .rsrc
  + SECTION .reloc

pFile      Data          Description                Value
00000178   2E 74 65 78   Name                       .text
0000017C   74 00 00 00
00000180   001498A4      Virtual Size
00000184   00002000      RVA
00000188   00149A00      Size of Raw Data
0000018C   00000400      Pointer to Raw Data
00000190   00000000      Pointer to Relocations
00000194   00000000      Pointer to Line Numbers
00000198   0000          Number of Relocations
0000019A   0000          Number of Line Numbers
0000019C   60000020      Characteristics
                         00000020                   IMAGE_SCN_CNT_CODE
                         20000000                   IMAGE_SCN_MEM_EXECUTE
                         40000000                   IMAGE_SCN_MEM_READ

Viewing IMAGE_SECTION_HEADER .text
```

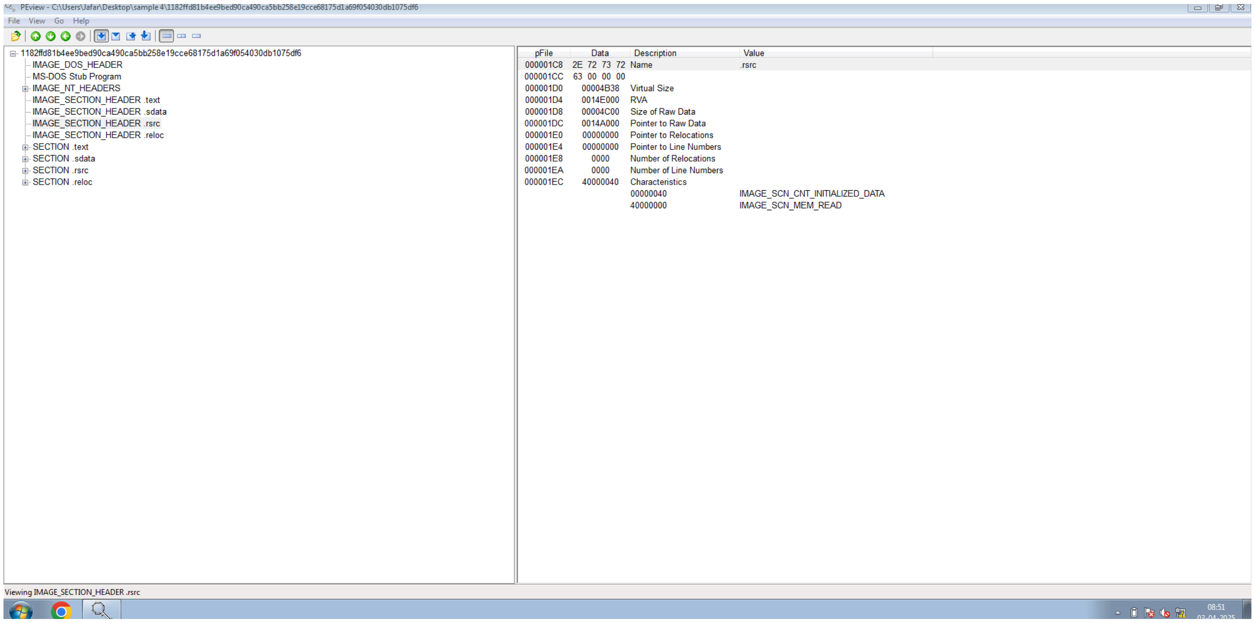


PEview - C:\Users\Jafar\Desktop\sample 4\1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1075df6

```
⊟ 1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1075df6
     IMAGE_DOS_HEADER
     MS-DOS Stub Program
   ⊞ IMAGE_NT_HEADERS
     IMAGE_SECTION_HEADER .text
     IMAGE_SECTION_HEADER .sdata
     IMAGE_SECTION_HEADER .rsrc
     IMAGE_SECTION_HEADER .reloc
   ⊞ SECTION .text
   ⊞ SECTION .sdata
   ⊞ SECTION .rsrc
   ⊞ SECTION .reloc
```

```
pFile      Data          Description              Value
000001A0   2E 73 64 61   Name                     .sdata
000001A4   74 61 00 00
000001A8   00000138      Virtual Size
000001AC   0014C000      RVA
000001B0   00000200      Size of Raw Data
000001B4   00149E00      Pointer to Raw Data
000001B8   00000000      Pointer to Relocations
000001BC   00000000      Pointer to Line Numbers
000001C0   0000          Number of Relocations
000001C2   0000          Number of Line Numbers
000001C4   C0000040      Characteristics
                         00000040                 IMAGE_SCN_CNT_INITIALIZED_DATA
                         40000000                 IMAGE_SCN_MEM_READ
                         80000000                 IMAGE_SCN_MEM_WRITE
```

Viewing IMAGE_SECTION_HEADER .sdata

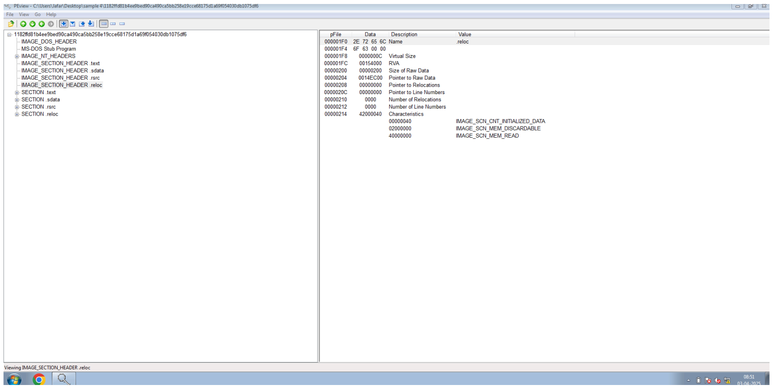


PEview - C:\Users\Jafar\Desktop\sample 4\1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1075df6

```
⊟ 1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1075df6
     IMAGE_DOS_HEADER
     MS-DOS Stub Program
   ⊞ IMAGE_NT_HEADERS
     IMAGE_SECTION_HEADER .text
     IMAGE_SECTION_HEADER .sdata
     IMAGE_SECTION_HEADER .rsrc
     IMAGE_SECTION_HEADER .reloc
   ⊞ SECTION .text
   ⊞ SECTION .sdata
   ⊞ SECTION .rsrc
   ⊞ SECTION .reloc
```

```
pFile      Data          Description              Value
000001C8   2E 72 73 72   Name                     .rsrc
000001CC   63 00 00 00
000001D0   00004B38      Virtual Size
000001D4   0014E000      RVA
000001D8   00004C00      Size of Raw Data
000001DC   0014A000      Pointer to Raw Data
000001E0   00000000      Pointer to Relocations
000001E4   00000000      Pointer to Line Numbers
000001E8   0000          Number of Relocations
000001EA   0000          Number of Line Numbers
000001EC   40000040      Characteristics
                         00000040                 IMAGE_SCN_CNT_INITIALIZED_DATA
                         40000000                 IMAGE_SCN_MEM_READ
```

Viewing IMAGE_SECTION_HEADER .rsrc



PEview - C:\Users\Jafar\Desktop\sample 4\1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1075df6

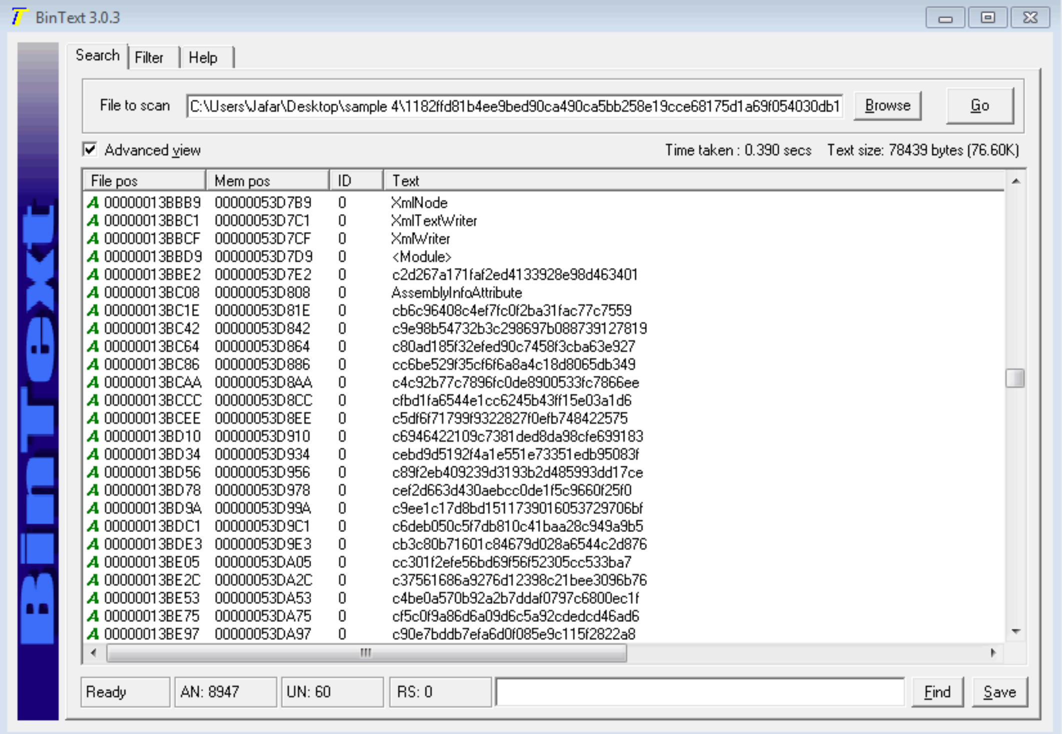
```
⊟ 1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1075df6
     IMAGE_DOS_HEADER
     MS-DOS Stub Program
   ⊞ IMAGE_NT_HEADERS
     IMAGE_SECTION_HEADER .text
     IMAGE_SECTION_HEADER .sdata
     IMAGE_SECTION_HEADER .rsrc
     IMAGE_SECTION_HEADER .reloc
   ⊞ SECTION .text
   ⊞ SECTION .sdata
   ⊞ SECTION .rsrc
   ⊞ SECTION .reloc
```

```
pFile      Data          Description              Value
000001F0   2E 72 65 6C   Name                     .reloc
000001F4   6F 63 00 00
000001F8   0000000C      Virtual Size
000001FC   00154000      RVA
00000200   00000200      Size of Raw Data
00000204   0014EC00      Pointer to Raw Data
00000208   00000000      Pointer to Relocations
0000020C   00000000      Pointer to Line Numbers
00000210   0000          Number of Relocations
00000212   0000          Number of Line Numbers
00000214   42000040      Characteristics
                         00000040                 IMAGE_SCN_CNT_INITIALIZED_DATA
                         02000000                 IMAGE_SCN_MEM_DISCARDABLE
                         40000000                 IMAGE_SCN_MEM_READ
```

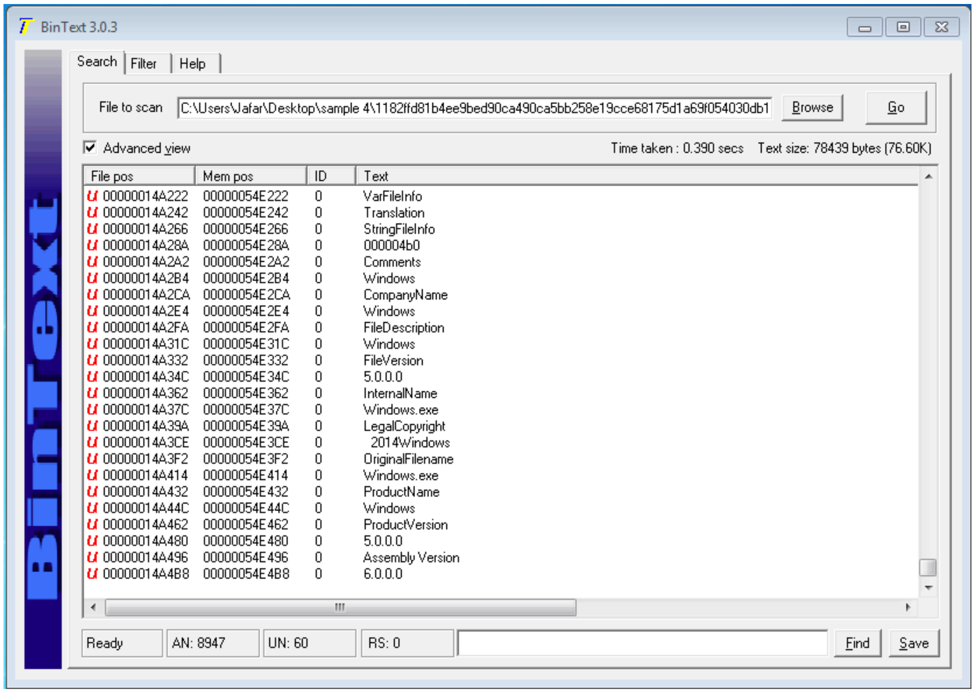
Viewing IMAGE_SECTION_HEADER .reloc

The section headers provide useful information about the 4 sections of the PE file and their associated details like Virtual Size and Size of Raw Data.

3. String Analysis



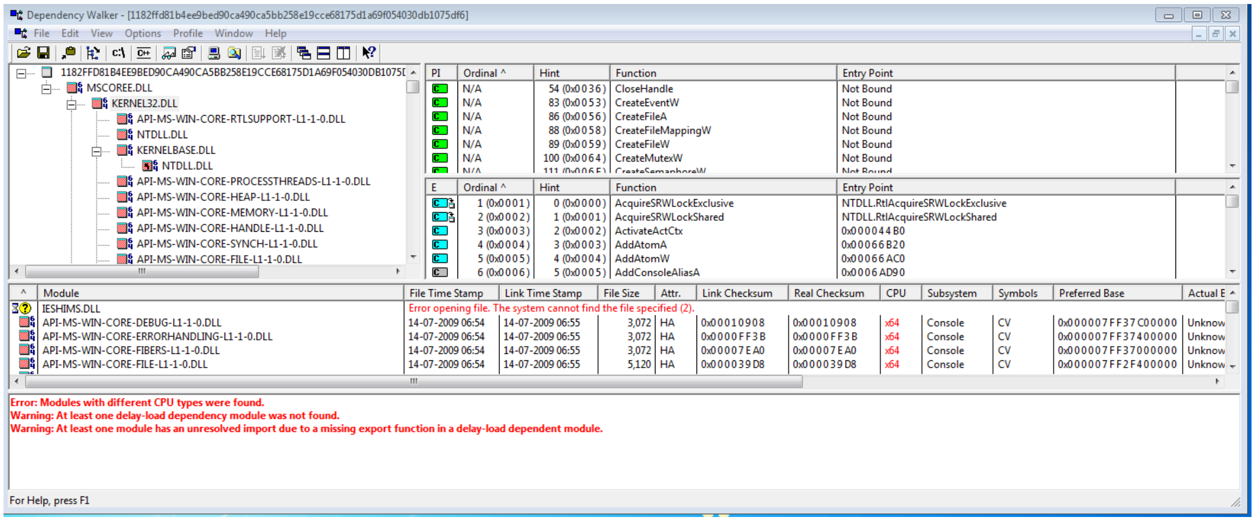
```
File to scan  C:\Users\Jafar\Desktop\sample 4\1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1
☑ Advanced view                                   Time taken : 0.390 secs   Text size: 78439 bytes (76.60K)

File pos          Mem pos           ID    Text
A 00000013BBB9    00000053D7B9      0     XmlNode
A 00000013BBC1    00000053D7C1      0     XmlTextWriter
A 00000013BBCF    00000053D7CF      0     XmlWriter
A 00000013BBD9    00000053D7D9      0     <Module>
A 00000013BBE2    00000053D7E2      0     c2d267a171faf2ed4133928e98d463401
A 00000013BC08    00000053D808      0     AssemblyInfoAttribute
A 00000013BC1E    00000053D81E      0     cb6c96408c4ef7fc0f2ba31fac77c7559
A 00000013BC42    00000053D842      0     c9e98b54732b3c298697b088739127819
A 00000013BC64    00000053D864      0     c80ad185f32efed90c7458f3cba63e927
A 00000013BC86    00000053D886      0     cc6be529f35cf6f6a8a4c18d8065db349
A 00000013BCAA    00000053D8AA      0     c4c92b77c7896fc0de8900533fc7866ee
A 00000013BCCC    00000053D8CC      0     cfbd1fa6544e1cc6245b43ff15e03a1d6
A 00000013BCEE    00000053D8EE      0     c5df6f71799f9322827f0efb748422575
A 00000013BD10    00000053D910      0     c6946422109c7381ded8da98cfe699183
A 00000013BD34    00000053D934      0     cebd9d5192f4a1e551e73351edb95083f
A 00000013BD56    00000053D956      0     c89f2eb409239d3193b2d485993dd17ce
A 00000013BD78    00000053D978      0     cef2d663d430aebcc0de1f5c9660f25f0
A 00000013BD9A    00000053D99A      0     c9ee1c17d8bd1511739016053729706bf
A 00000013BDC1    00000053D9C1      0     c6deb050c5f7db810c41baa28c949a9b5
A 00000013BDE3    00000053D9E3      0     cb3c80b71601c84679d028a6544c2d876
A 00000013BE05    00000053DA05      0     cc301f2efe56bd69f56f52305cc533ba7
A 00000013BE2C    00000053DA2C      0     c37561686a9276d12398c21bee3096b76
A 00000013BE53    00000053DA53      0     c4be0a570b92a2b7ddaf0797c6800ec1f
A 00000013BE75    00000053DA75      0     cf5c0f9a86d6a09d6c5a92cdedcd46ad6
A 00000013BE97    00000053DA97      0     c90e7bddb7efa6d0f085e9c115f2822a8

Ready    AN: 8947    UN: 60    RS: 0
```



```
File to scan  C:\Users\Jafar\Desktop\sample 4\1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1
☑ Advanced view                              Time taken : 0.390 secs   Text size: 78439 bytes (76.60K)

File pos          Mem pos           ID    Text
U 00000014A222    00000054E222      0     VarFileInfo
U 00000014A242    00000054E242      0     Translation
U 00000014A266    00000054E266      0     StringFileInfo
U 00000014A28A    00000054E28A      0     000004b0
U 00000014A2A2    00000054E2A2      0     Comments
U 00000014A2B4    00000054E2B4      0     Windows
U 00000014A2CA    00000054E2CA      0     CompanyName
U 00000014A2E4    00000054E2E4      0     Windows
U 00000014A2FA    00000054E2FA      0     FileDescription
U 00000014A31C    00000054E31C      0     Windows
U 00000014A332    00000054E332      0     FileVersion
U 00000014A34C    00000054E34C      0     5.0.0.0
U 00000014A362    00000054E362      0     InternalName
U 00000014A37C    00000054E37C      0     Windows.exe
U 00000014A39A    00000054E39A      0     LegalCopyright
U 00000014A3CE    00000054E3CE      0       2014Windows
U 00000014A3F2    00000054E3F2      0     OriginalFilename
U 00000014A414    00000054E414      0     Windows.exe
U 00000014A432    00000054E432      0     ProductName
U 00000014A44C    00000054E44C      0     Windows
U 00000014A462    00000054E462      0     ProductVersion
U 00000014A480    00000054E480      0     5.0.0.0
U 00000014A496    00000054E496      0     Assembly Version
U 00000014A4B8    00000054E4B8      0     6.0.0.0

Ready    AN: 8947    UN: 60    RS: 0
```

Strings contain an IP address and a list of hashes probably to files.

4. Imports/Exports Analysis



Dependency Walker - [1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1075df6]

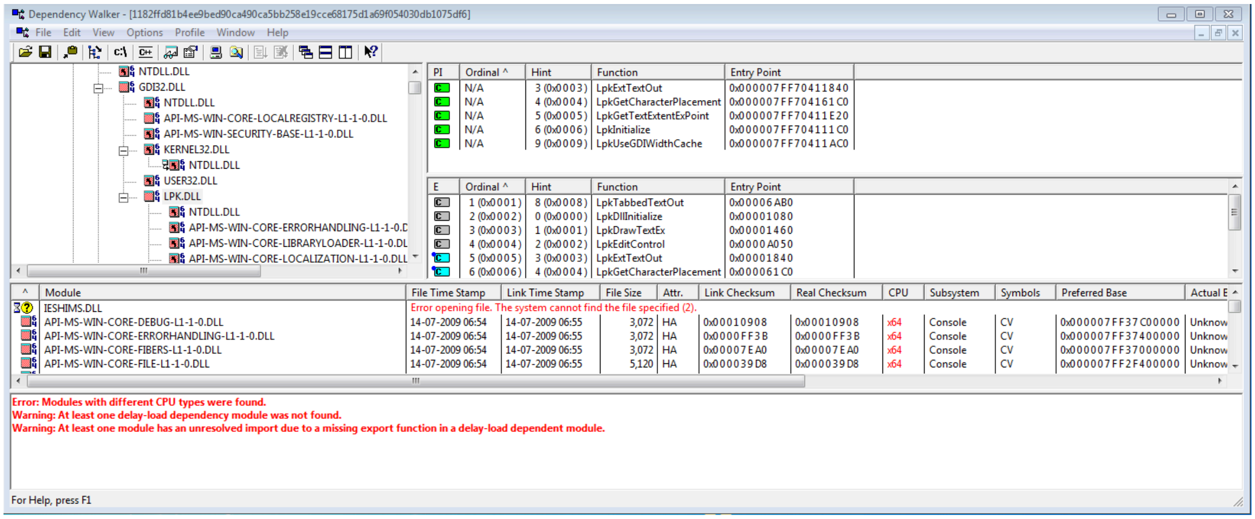
```
1182FFD81B4EE9BED90CA490CA5BB258E19CCE68175D1A69F054030DB1075I
    MSCOREE.DLL
        KERNEL32.DLL
            API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
            NTDLL.DLL
            KERNELBASE.DLL
                NTDLL.DLL
            API-MS-WIN-CORE-PROCESSTHREADS-L1-1-0.DLL
            API-MS-WIN-CORE-HEAP-L1-1-0.DLL
            API-MS-WIN-CORE-MEMORY-L1-1-0.DLL
            API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
            API-MS-WIN-CORE-SYNCH-L1-1-0.DLL
            API-MS-WIN-CORE-FILE-L1-1-0.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	54 (0x0036)	CloseHandle	Not Bound
C	N/A	83 (0x0053)	CreateEventW	Not Bound
C	N/A	86 (0x0056)	CreateFileA	Not Bound
C	N/A	88 (0x0058)	CreateFileMappingW	Not Bound
C	N/A	89 (0x0059)	CreateFileW	Not Bound
C	N/A	100 (0x0064)	CreateMutexW	Not Bound
C	N/A	111 (0x006E)	CreateSemaphoreW	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
C	2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
C	3 (0x0003)	2 (0x0002)	ActivateActCtx	0x000044B0
C	4 (0x0004)	3 (0x0003)	AddAtomA	0x00066B20
C	5 (0x0005)	4 (0x0004)	AddAtomW	0x00066AC0
C	6 (0x0006)	5 (0x0005)	AddConsoleAliasA	0x0006AD90

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual E
⧗?	IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).										
	API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00010908	0x00010908	x64	Console	CV	0x000007FF37C00000	Unknow
	API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000FF3B	0x0000FF3B	x64	Console	CV	0x000007FF37400000	Unknow
	API-MS-WIN-CORE-FIBERS-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00007EA0	0x00007EA0	x64	Console	CV	0x000007FF37000000	Unknow
	API-MS-WIN-CORE-FILE-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	5,120	HA	0x000039D8	0x000039D8	x64	Console	CV	0x000007FF2F400000	Unknow

```
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```



Dependency Walker - [1182ffd81b4ee9bed90ca490ca5bb258e19cce68175d1a69f054030db1075df6]

```
            NTDLL.DLL
        GDI32.DLL
            NTDLL.DLL
            API-MS-WIN-CORE-LOCALREGISTRY-L1-1-0.DLL
            API-MS-WIN-SECURITY-BASE-L1-1-0.DLL
            KERNEL32.DLL
                NTDLL.DLL
            USER32.DLL
            LPK.DLL
                NTDLL.DLL
                API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.D
                API-MS-WIN-CORE-LIBRARYLOADER-L1-1-0.DL
                API-MS-WIN-CORE-LOCALIZATION-L1-1-0.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	3 (0x0003)	LpkExtTextOut	0x000007FF70411840
C	N/A	4 (0x0004)	LpkGetCharacterPlacement	0x000007FF704161C0
C	N/A	5 (0x0005)	LpkGetTextExtentExPoint	0x000007FF70411E20
C	N/A	6 (0x0006)	LpkInitialize	0x000007FF704111C0
C	N/A	9 (0x0009)	LpkUseGDIWidthCache	0x000007FF70411AC0

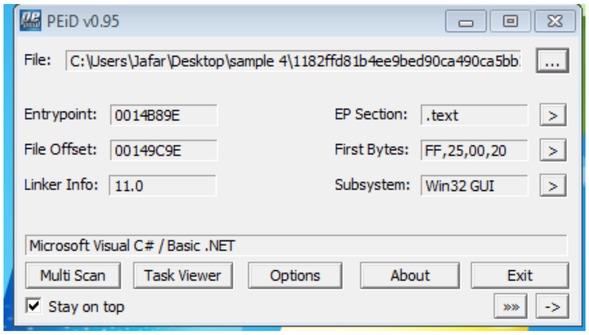
E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	8 (0x0008)	LpkTabbedTextOut	0x00006AB0
C	2 (0x0002)	0 (0x0000)	LpkDllInitialize	0x00001080
C	3 (0x0003)	1 (0x0001)	LpkDrawTextEx	0x00001460
C	4 (0x0004)	2 (0x0002)	LpkEditControl	0x0000A050
C	5 (0x0005)	3 (0x0003)	LpkExtTextOut	0x00001840
C	6 (0x0006)	4 (0x0004)	LpkGetCharacterPlacement	0x000061C0

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual E
⧗?	IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).										
	API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00010908	0x00010908	x64	Console	CV	0x000007FF37C00000	Unknow
	API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000FF3B	0x0000FF3B	x64	Console	CV	0x000007FF37400000	Unknow
	API-MS-WIN-CORE-FIBERS-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00007EA0	0x00007EA0	x64	Console	CV	0x000007FF37000000	Unknow
	API-MS-WIN-CORE-FILE-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	5,120	HA	0x000039D8	0x000039D8	x64	Console	CV	0x000007FF2F400000	Unknow

```
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```

NTDLL is being called by other dlls and file manipulation as well as mutex functions are being called.

5. Is the file packed/obfuscated?



File: C:\Users\Jafar\Desktop\sample 4\1182ffd81b4ee9bed90ca490ca5bb

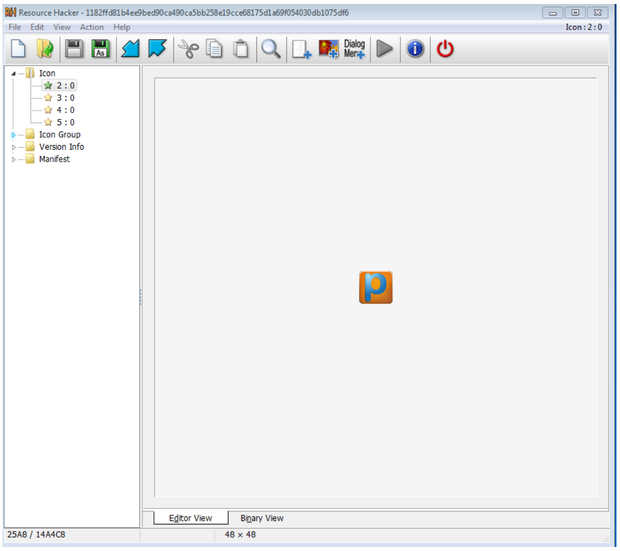
Entrypoint:	0014B89E	EP Section:	.text
File Offset:	00149C9E	First Bytes:	FF,25,00,20
Linker Info:	11.0	Subsystem:	Win32 GUI

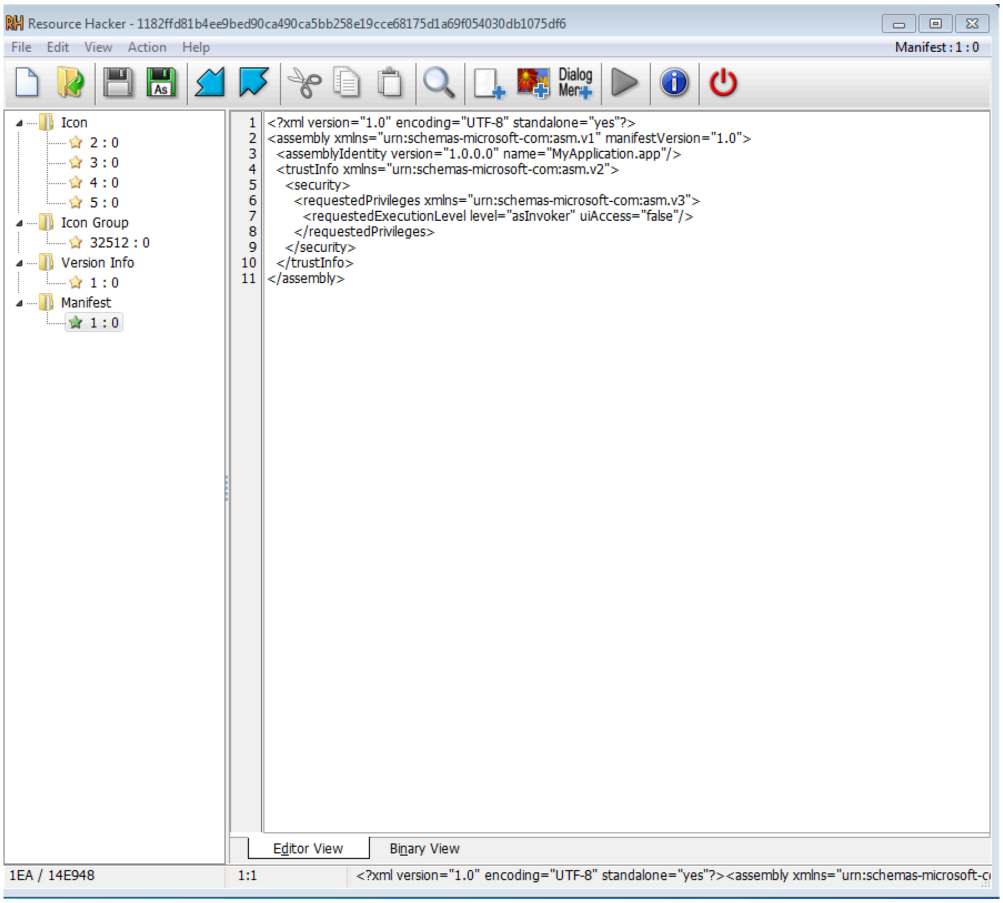
Microsoft Visual C# / Basic .NET

☑ Stay on top

No the file is not packed.

6. If GUI, then analyze its resources





```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    <security>
      <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
        <requestedExecutionLevel level="asInvoker" uiAccess="false"/>
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><assembly xmlns="urn:schemas-microsoft-c
```

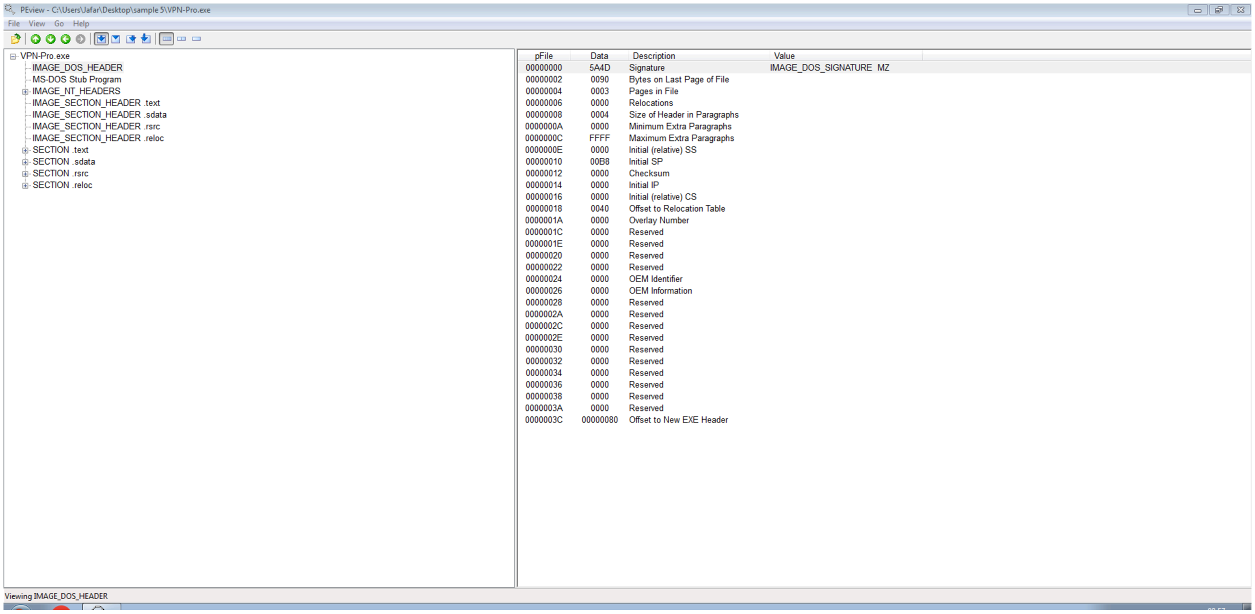
Resource hacker provides us with icons and the manifest file of the executable.

7. What is the file trying to do with suspicious functions?

The file is a potential malware that does file manipulation using functions like CreateFile and DeleteFile repeated;y along with process manipulation using mutexes. No IP address is found, so the possibility of external communication can be ruled out.

SAMPLE 05 - SYRIAN MALWARE

1. PE Header Information.

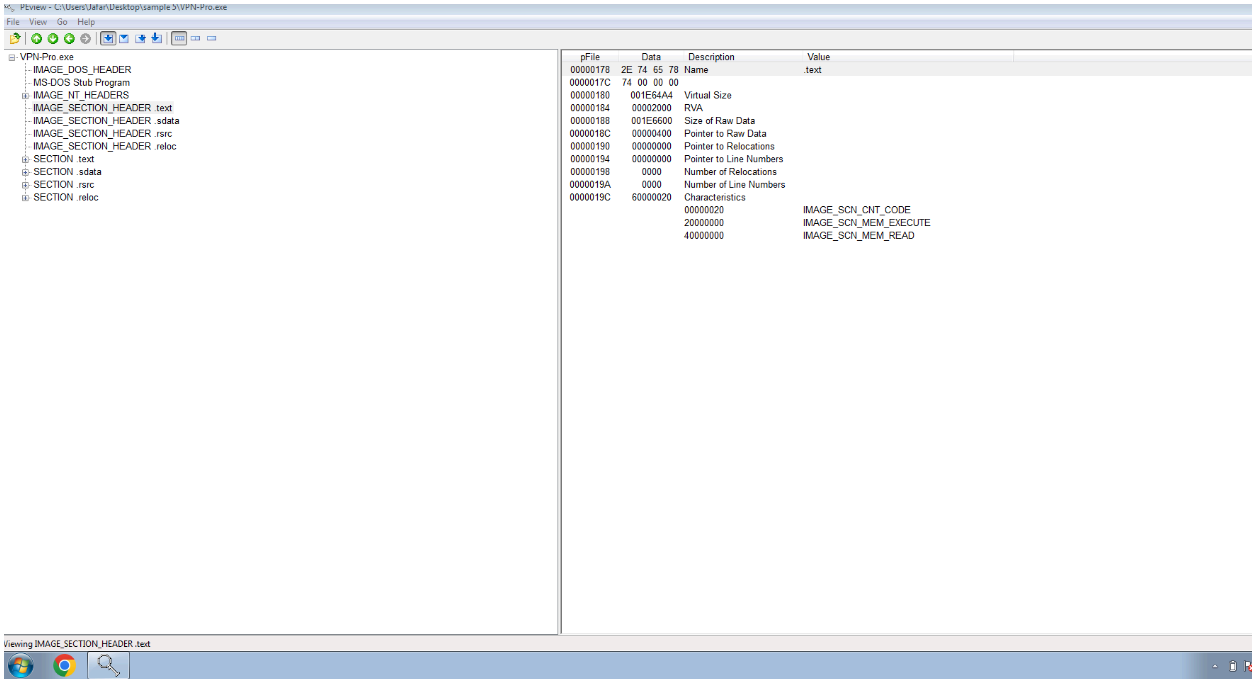

PEview - C:\Users\Jafar\Desktop\sample 5\VPN-Pro.exe
File View Go Help
VPN-Pro.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .sdata
IMAGE_SECTION_HEADER .rsrc
IMAGE_SECTION_HEADER .reloc
SECTION .text
SECTION .sdata
SECTION .rsrc
SECTION .reloc

pFile	Data	Description	Value
00000000	5A4D	Signature	IMAGE_DOS_SIGNATURE MZ
00000002	0090	Bytes on Last Page of File	
00000004	0003	Pages in File	
00000006	0000	Relocations	
00000008	0004	Size of Header in Paragraphs	
0000000A	0000	Minimum Extra Paragraphs	
0000000C	FFFF	Maximum Extra Paragraphs	
0000000E	0000	Initial (relative) SS	
00000010	00B8	Initial SP	
00000012	0000	Checksum	
00000014	0000	Initial IP	
00000016	0000	Initial (relative) CS	
00000018	0040	Offset to Relocation Table	
0000001A	0000	Overlay Number	
0000001C	0000	Reserved	
0000001E	0000	Reserved	
00000020	0000	Reserved	
00000022	0000	Reserved	
00000024	0000	OEM Identifier	
00000026	0000	OEM Information	
00000028	0000	Reserved	
0000002A	0000	Reserved	
0000002C	0000	Reserved	
0000002E	0000	Reserved	
00000030	0000	Reserved	
00000032	0000	Reserved	
00000034	0000	Reserved	
00000036	0000	Reserved	
00000038	0000	Reserved	
0000003A	0000	Reserved	
0000003C	00000080	Offset to New EXE Header	

Viewing IMAGE_DOS_HEADER

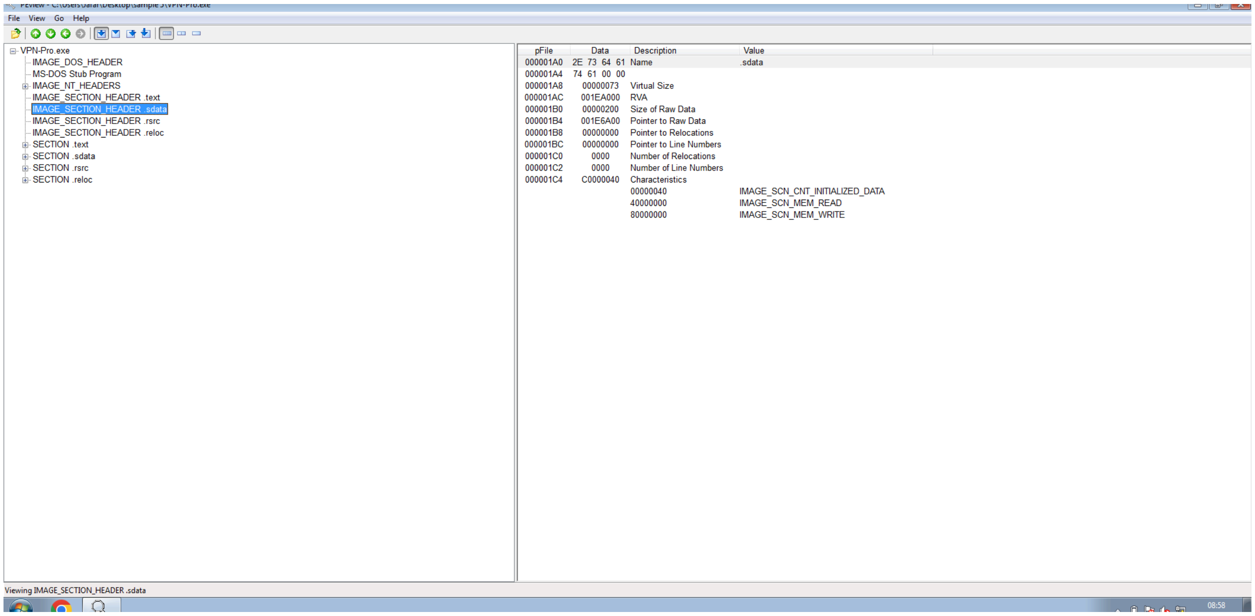
The MS DOS header, now discontinued, provides the aforementioned information. However, significant details can be found from the NT headers and section headers.

2. PE Section Headers Information


PEview - C:\Users\Jafar\Desktop\sample 5\VPN-Pro.exe
File View Go Help
VPN-Pro.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .sdata
IMAGE_SECTION_HEADER .rsrc
IMAGE_SECTION_HEADER .reloc
SECTION .text
SECTION .sdata
SECTION .rsrc
SECTION .reloc

pFile	Data	Description	Value
00000178	2E 74 65 78	Name	.text
0000017C	74 00 00 00		
00000180	001E64A4	Virtual Size	
00000184	00002000	RVA	
00000188	001E6600	Size of Raw Data	
0000018C	00000400	Pointer to Raw Data	
00000190	00000000	Pointer to Relocations	
00000194	00000000	Pointer to Line Numbers	
00000198	0000	Number of Relocations	
0000019A	0000	Number of Line Numbers	
0000019C	60000020	Characteristics	
		00000020	IMAGE_SCN_CNT_CODE
		20000000	IMAGE_SCN_MEM_EXECUTE
		40000000	IMAGE_SCN_MEM_READ

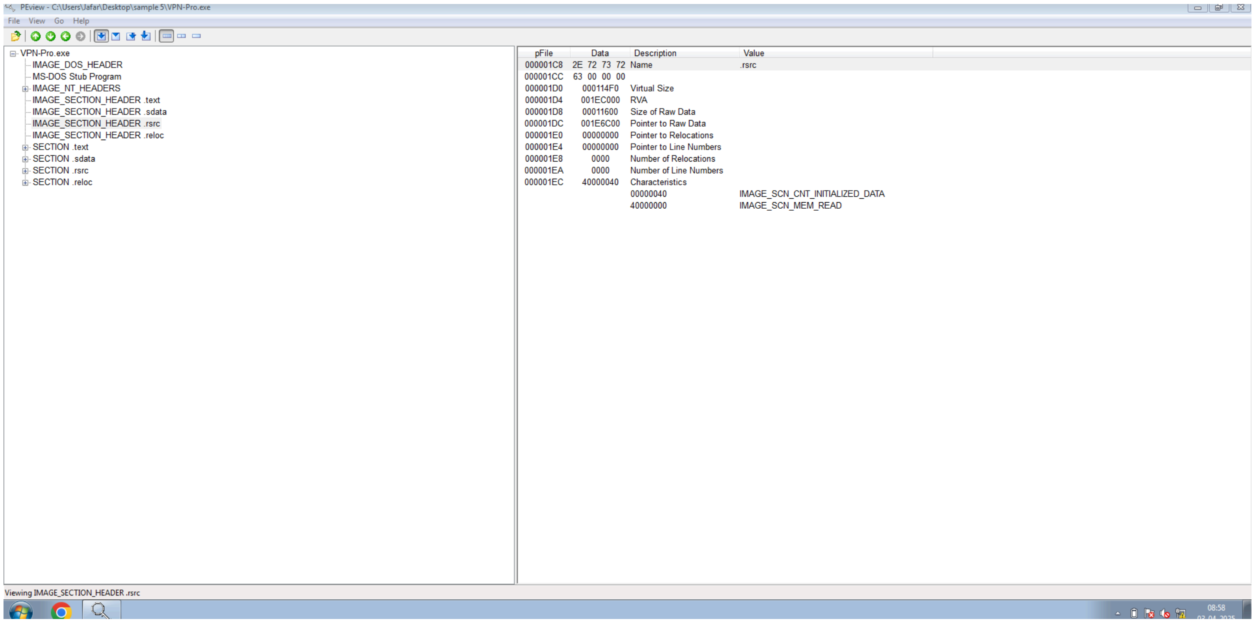
Viewing IMAGE_SECTION_HEADER .text



```
VPN-Pro.exe
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
  ⊞ IMAGE_NT_HEADERS
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .sdata
    IMAGE_SECTION_HEADER .rsrc
    IMAGE_SECTION_HEADER .reloc
  ⊞ SECTION .text
  ⊞ SECTION .sdata
  ⊞ SECTION .rsrc
  ⊞ SECTION .reloc
```

```
  pFile        Data       Description               Value
000001A0   2E 73 64 61   Name                      .sdata
000001A4   74 61 00 00
000001A8    00000073     Virtual Size
000001AC    001EA000     RVA
000001B0    00000200     Size of Raw Data
000001B4    001E6A00     Pointer to Raw Data
000001B8    00000000     Pointer to Relocations
000001BC    00000000     Pointer to Line Numbers
000001C0      0000       Number of Relocations
000001C2      0000       Number of Line Numbers
000001C4    C0000040     Characteristics
                         00000040                  IMAGE_SCN_CNT_INITIALIZED_DATA
                         40000000                  IMAGE_SCN_MEM_READ
                         80000000                  IMAGE_SCN_MEM_WRITE
```

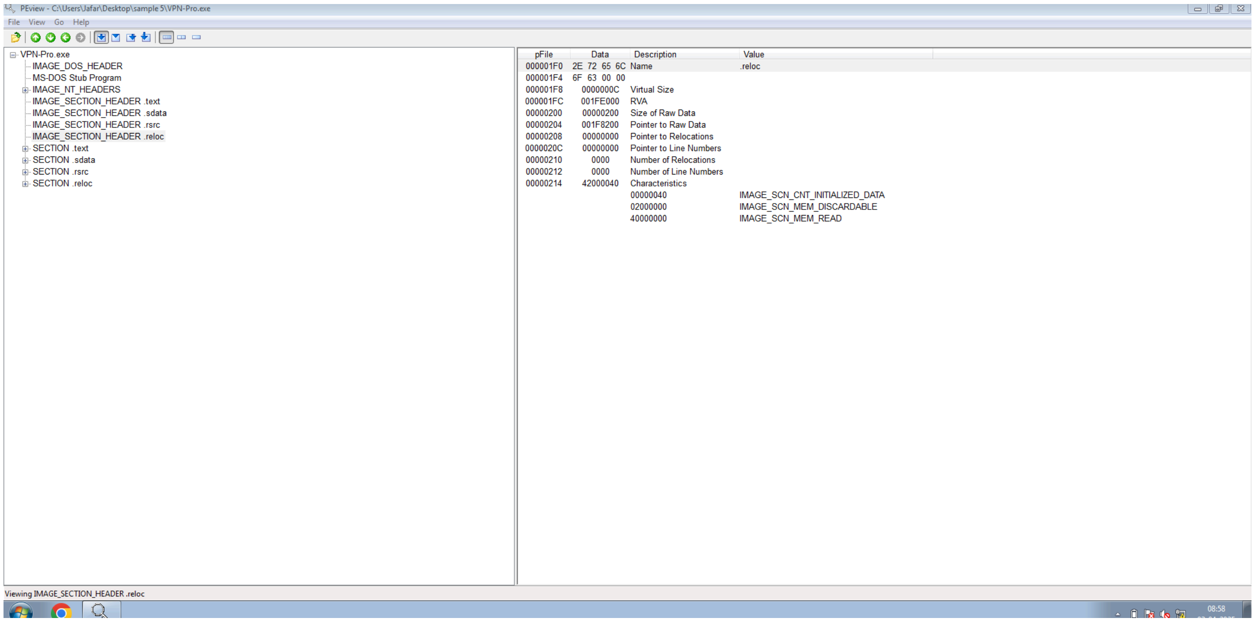
Viewing IMAGE_SECTION_HEADER .sdata



```
VPN-Pro.exe
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
  ⊞ IMAGE_NT_HEADERS
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .sdata
    IMAGE_SECTION_HEADER .rsrc
    IMAGE_SECTION_HEADER .reloc
  ⊞ SECTION .text
  ⊞ SECTION .sdata
  ⊞ SECTION .rsrc
  ⊞ SECTION .reloc
```

```
  pFile        Data       Description               Value
000001C8   2E 72 73 72   Name                      .rsrc
000001CC   63 00 00 00
000001D0    000114F0     Virtual Size
000001D4    001EC000     RVA
000001D8    00011600     Size of Raw Data
000001DC    001E6C00     Pointer to Raw Data
000001E0    00000000     Pointer to Relocations
000001E4    00000000     Pointer to Line Numbers
000001E8      0000       Number of Relocations
000001EA      0000       Number of Line Numbers
000001EC    40000040     Characteristics
                         00000040                  IMAGE_SCN_CNT_INITIALIZED_DATA
                         40000000                  IMAGE_SCN_MEM_READ
```

Viewing IMAGE_SECTION_HEADER .rsrc



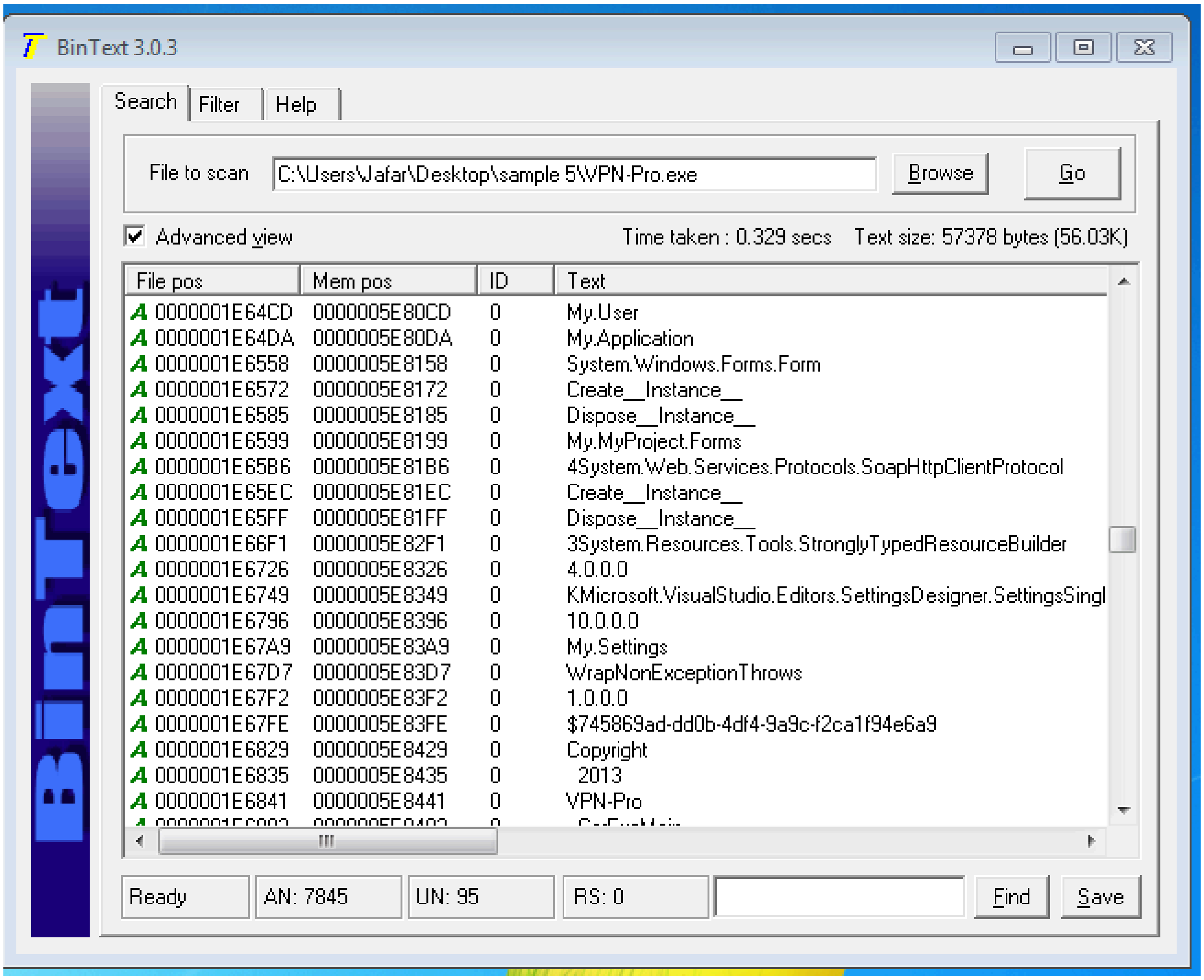
```
VPN-Pro.exe
    IMAGE_DOS_HEADER
    MS-DOS Stub Program
    IMAGE_NT_HEADERS
    IMAGE_SECTION_HEADER .text
    IMAGE_SECTION_HEADER .sdata
    IMAGE_SECTION_HEADER .rsrc
    IMAGE_SECTION_HEADER .reloc
    SECTION .text
    SECTION .sdata
    SECTION .rsrc
    SECTION .reloc
```

```
pFile     Data         Description              Value
000001F0  2E 72 65 6C  Name                     .reloc
000001F4  6F 63 00 00
000001F8   0000000C    Virtual Size
000001FC   001FE000    RVA
00000200   00000200    Size of Raw Data
00000204   001F8200    Pointer to Raw Data
00000208   00000000    Pointer to Relocations
0000020C   00000000    Pointer to Line Numbers
00000210     0000      Number of Relocations
00000212     0000      Number of Line Numbers
00000214   42000040    Characteristics
                       00000040                 IMAGE_SCN_CNT_INITIALIZED_DATA
                       02000000                 IMAGE_SCN_MEM_DISCARDABLE
                       40000000                 IMAGE_SCN_MEM_READ
```

Viewing IMAGE_SECTION_HEADER .reloc

The section headers provide useful information about the 4 sections of the PE file and their associated details like Virtual Size and Size of Raw Data.

3. String Analysis

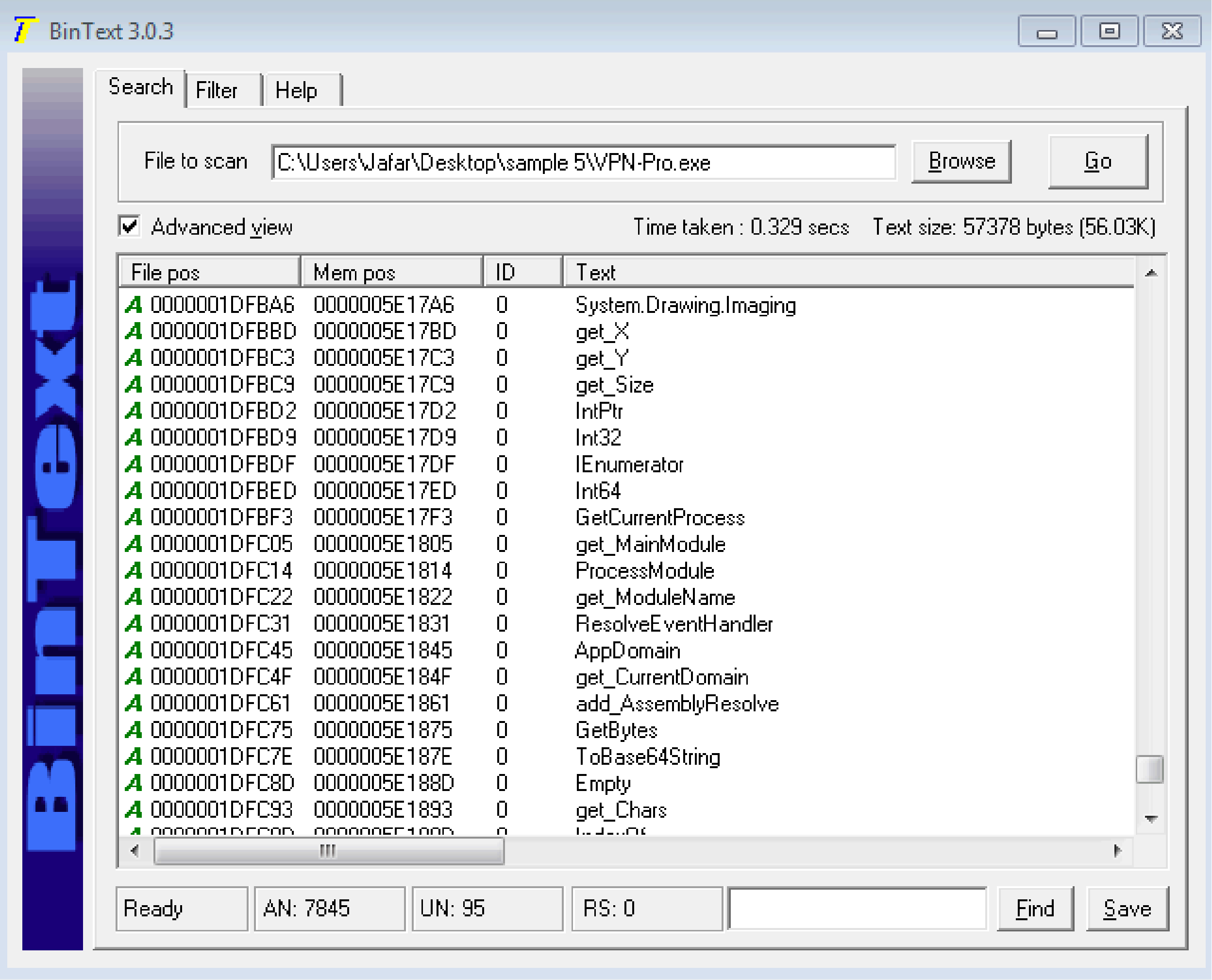


File to scan: C:\Users\Jafar\Desktop\sample 5\VPN-Pro.exe

☑ Advanced view   Time taken : 0.329 secs   Text size: 57378 bytes (56.03K)

```
File pos          Mem pos           ID   Text
A 0000001E64CD    0000005E80CD      0    My.User
A 0000001E64DA    0000005E80DA      0    My.Application
A 0000001E6558    0000005E8158      0    System.Windows.Forms.Form
A 0000001E6572    0000005E8172      0    Create__Instance__
A 0000001E6585    0000005E8185      0    Dispose__Instance__
A 0000001E6599    0000005E8199      0    My.MyProject.Forms
A 0000001E65B6    0000005E81B6      0    4System.Web.Services.Protocols.SoapHttpClientProtocol
A 0000001E65EC    0000005E81EC      0    Create__Instance__
A 0000001E65FF    0000005E81FF      0    Dispose__Instance__
A 0000001E66F1    0000005E82F1      0    3System.Resources.Tools.StronglyTypedResourceBuilder
A 0000001E6726    0000005E8326      0    4.0.0.0
A 0000001E6749    0000005E8349      0    KMicrosoft.VisualStudio.Editors.SettingsDesigner.SettingsSingl
A 0000001E6796    0000005E8396      0    10.0.0.0
A 0000001E67A9    0000005E83A9      0    My.Settings
A 0000001E67D7    0000005E83D7      0    WrapNonExceptionThrows
A 0000001E67F2    0000005E83F2      0    1.0.0.0
A 0000001E67FE    0000005E83FE      0    $745869ad-dd0b-4df4-9a9c-f2ca1f94e6a9
A 0000001E6829    0000005E8429      0    Copyright
A 0000001E6835    0000005E8435      0     2013
A 0000001E6841    0000005E8441      0    VPN-Pro
```

Ready | AN: 7845 | UN: 95 | RS: 0



File to scan: C:\Users\Jafar\Desktop\sample 5\VPN-Pro.exe

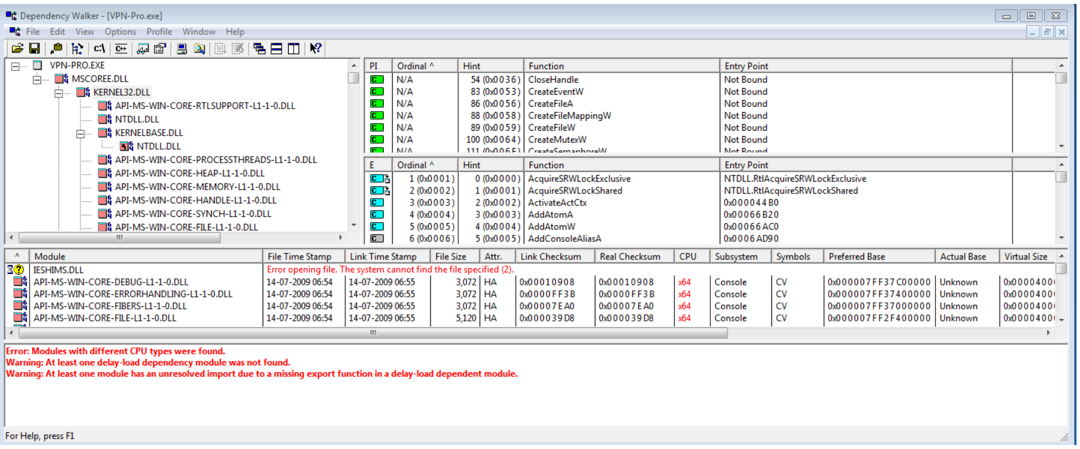
☑ Advanced view — Time taken : 0.329 secs — Text size: 57378 bytes (56.03K)

	File pos	Mem pos	ID	Text
A	0000001DFBA6	0000005E17A6	0	System.Drawing.Imaging
A	0000001DFBBD	0000005E17BD	0	get_X
A	0000001DFBC3	0000005E17C3	0	get_Y
A	0000001DFBC9	0000005E17C9	0	get_Size
A	0000001DFBD2	0000005E17D2	0	IntPtr
A	0000001DFBD9	0000005E17D9	0	Int32
A	0000001DFBDF	0000005E17DF	0	IEnumerator
A	0000001DFBED	0000005E17ED	0	Int64
A	0000001DFBF3	0000005E17F3	0	GetCurrentProcess
A	0000001DFC05	0000005E1805	0	get_MainModule
A	0000001DFC14	0000005E1814	0	ProcessModule
A	0000001DFC22	0000005E1822	0	get_ModuleName
A	0000001DFC31	0000005E1831	0	ResolveEventHandler
A	0000001DFC45	0000005E1845	0	AppDomain
A	0000001DFC4F	0000005E184F	0	get_CurrentDomain
A	0000001DFC61	0000005E1861	0	add_AssemblyResolve
A	0000001DFC75	0000005E1875	0	GetBytes
A	0000001DFC7E	0000005E187E	0	ToBase64String
A	0000001DFC8D	0000005E188D	0	Empty
A	0000001DFC93	0000005E1893	0	get_Chars

Ready | AN: 7845 | UN: 95 | RS: 0

Strings contain encryption to base64 as well as an IP address.

4. Imports/Exports Analysis



```
VPN-PRO.EXE
  MSCOREE.DLL
    KERNEL32.DLL
      API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
      NTDLL.DLL
      KERNELBASE.DLL
        NTDLL.DLL
      API-MS-WIN-CORE-PROCESSTHREADS-L1-1-0.DLL
      API-MS-WIN-CORE-HEAP-L1-1-0.DLL
      API-MS-WIN-CORE-MEMORY-L1-1-0.DLL
      API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
      API-MS-WIN-CORE-SYNCH-L1-1-0.DLL
      API-MS-WIN-CORE-FILE-L1-1-0.DLL
```

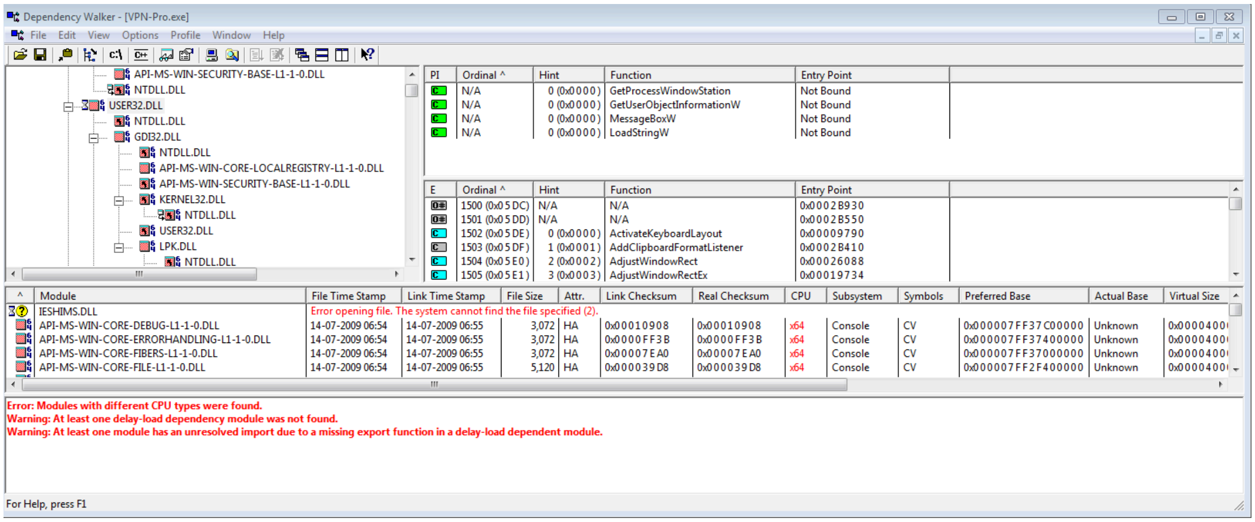
PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	54 (0x0036)	CloseHandle	Not Bound
C	N/A	83 (0x0053)	CreateEventW	Not Bound
C	N/A	86 (0x0056)	CreateFileA	Not Bound
C	N/A	88 (0x0058)	CreateFileMappingW	Not Bound
C	N/A	89 (0x0059)	CreateFileW	Not Bound
C	N/A	100 (0x0064)	CreateMutexW	Not Bound
C	N/A	111 (0x006F)	CreateSemaphoreW	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
C	2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
C	3 (0x0003)	2 (0x0002)	ActivateActCtx	0x000044B0
C	4 (0x0004)	3 (0x0003)	AddAtomA	0x00066B20
C	5 (0x0005)	4 (0x0004)	AddAtomW	0x00066AC0
C	6 (0x0006)	5 (0x0005)	AddConsoleAliasA	0x0006AD90

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
?	IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).											
	API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00010908	0x00010908	x64	Console	CV	0x000007FF37C00000	Unknown	0x0000400
	API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000FF3B	0x0000FF3B	x64	Console	CV	0x000007FF37400000	Unknown	0x0000400
	API-MS-WIN-CORE-FIBERS-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00007EA0	0x00007EA0	x64	Console	CV	0x000007FF37000000	Unknown	0x0000400
	API-MS-WIN-CORE-FILE-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	5,120	HA	0x000039D8	0x000039D8	x64	Console	CV	0x000007FF2F400000	Unknown	0x0000400

Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

For Help, press F1



Dependency Walker - [VPN-Pro.exe]

```
        API-MS-WIN-SECURITY-BASE-L1-1-0.DLL
        NTDLL.DLL
    USER32.DLL
        NTDLL.DLL
        GDI32.DLL
            NTDLL.DLL
            API-MS-WIN-CORE-LOCALREGISTRY-L1-1-0.DLL
            API-MS-WIN-SECURITY-BASE-L1-1-0.DLL
            KERNEL32.DLL
                NTDLL.DLL
            USER32.DLL
            LPK.DLL
                NTDLL.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	0 (0x0000)	GetProcessWindowStation	Not Bound
C	N/A	0 (0x0000)	GetUserObjectInformationW	Not Bound
C	N/A	0 (0x0000)	MessageBoxW	Not Bound
C	N/A	0 (0x0000)	LoadStringW	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
O#	1500 (0x05DC)	N/A	N/A	0x0002B930
O#	1501 (0x05DD)	N/A	N/A	0x0002B550
C	1502 (0x05DE)	0 (0x0000)	ActivateKeyboardLayout	0x00009790
C	1503 (0x05DF)	1 (0x0001)	AddClipboardFormatListener	0x0002B410
C	1504 (0x05E0)	2 (0x0002)	AdjustWindowRect	0x00026088
C	1505 (0x05E1)	3 (0x0003)	AdjustWindowRectEx	0x00019734

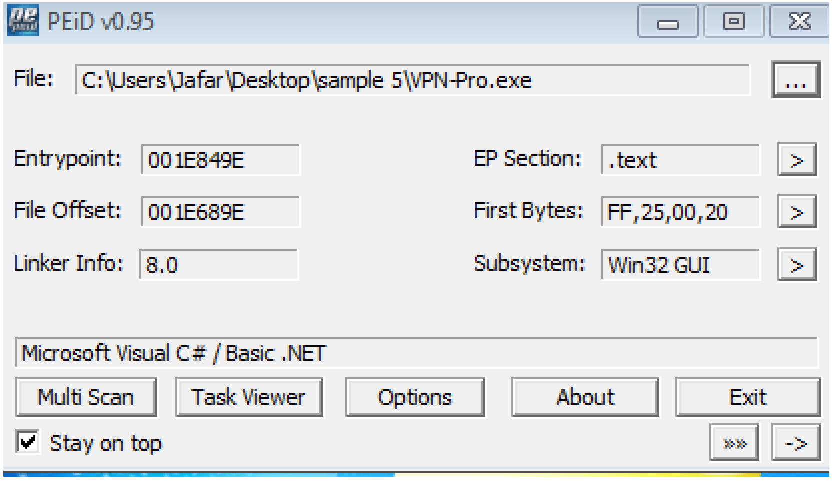
^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size
?	IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).											
	API-MS-WIN-CORE-DEBUG-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00010908	0x00010908	x64	Console	CV	0x000007FF37C00000	Unknown	0x0004000
	API-MS-WIN-CORE-ERRORHANDLING-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x0000FF3B	0x0000FF3B	x64	Console	CV	0x000007FF37400000	Unknown	0x0004000
	API-MS-WIN-CORE-FIBERS-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	3,072	HA	0x00007EA0	0x00007EA0	x64	Console	CV	0x000007FF37000000	Unknown	0x0004000
	API-MS-WIN-CORE-FILE-L1-1-0.DLL	14-07-2009 06:54	14-07-2009 06:55	5,120	HA	0x000039D8	0x000039D8	x64	Console	CV	0x000007FF2F400000	Unknown	0x0004000

```
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```

For Help, press F1

NTDLL is being called by other dlls and file manipulation as well as mutex functions are being called.

5. Is the file packed/obfuscated?



PEiD v0.95

File: C:\Users\Jafar\Desktop\sample 5\VPN-Pro.exe

Entrypoint: 001E849E

EP Section: .text

File Offset: 001E689E

First Bytes: FF,25,00,20

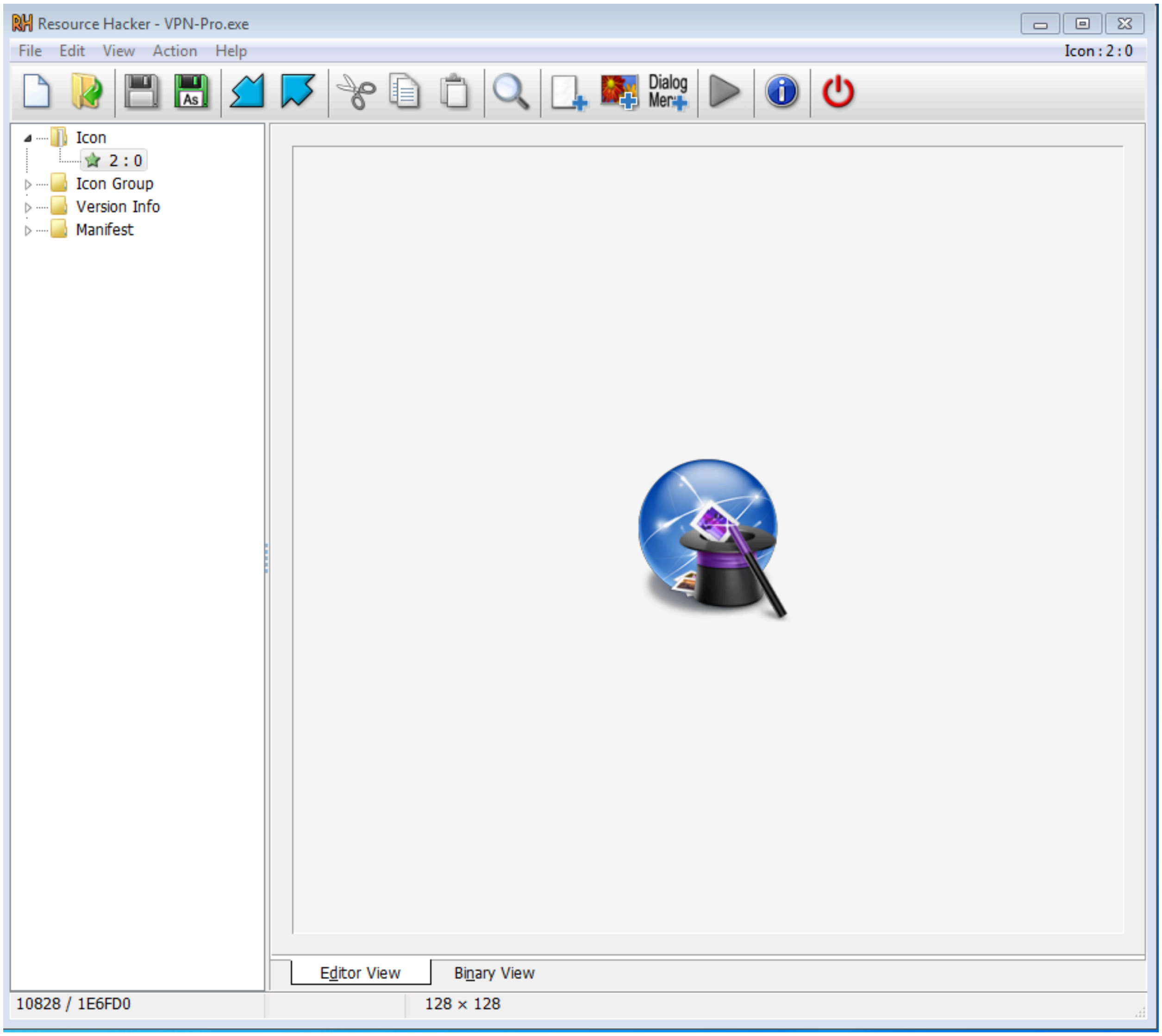
Linker Info: 8.0

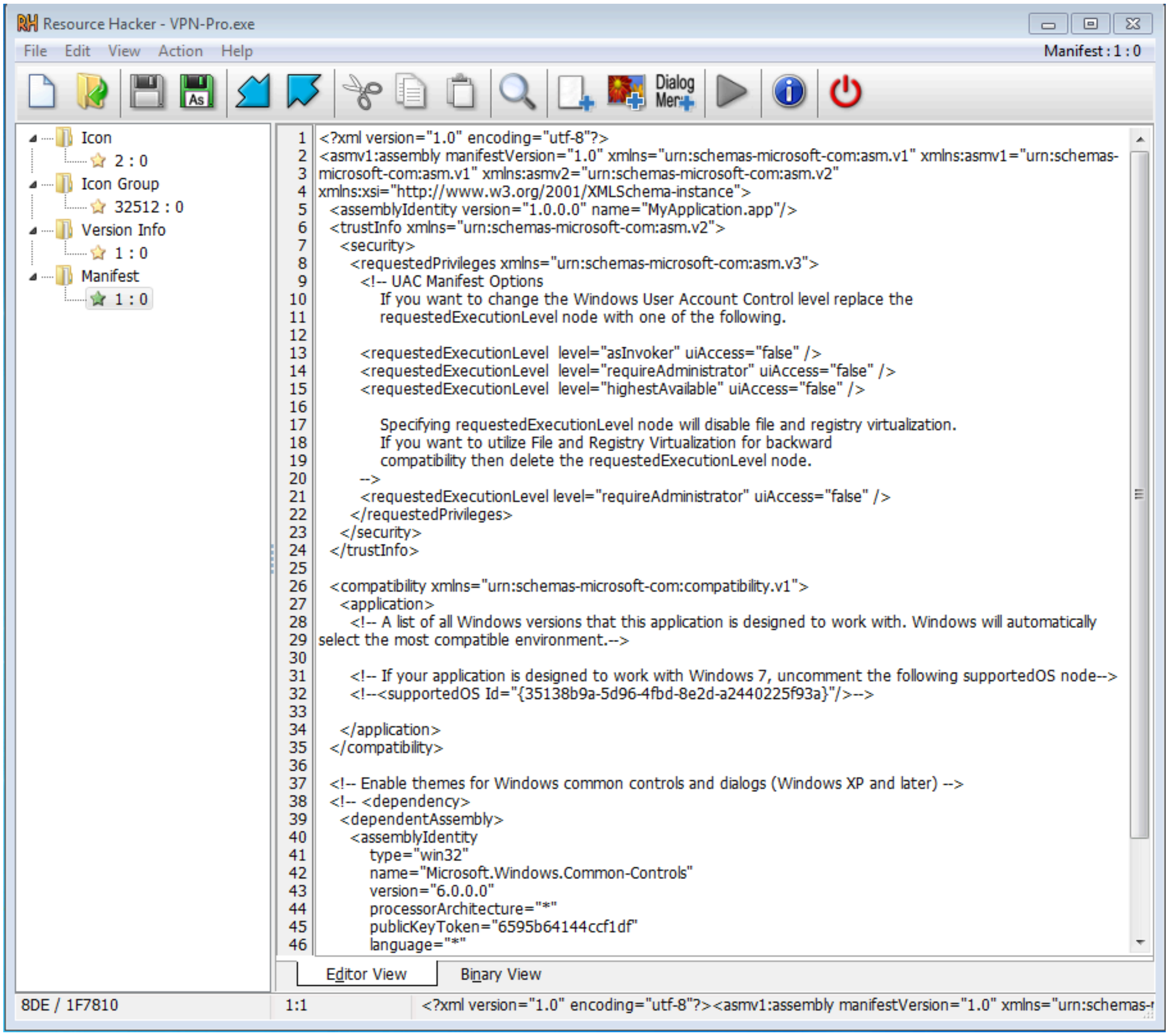
Subsystem: Win32 GUI

Microsoft Visual C# / Basic .NET

No the file is not packed.

6. If GUI, analyse its resources





```
<?xml version="1.0" encoding="utf-8"?>
<asmv1:assembly manifestVersion="1.0" xmlns="urn:schemas-microsoft-com:asm.v1" xmlns:asmv1="urn:schemas-
microsoft-com:asm.v1" xmlns:asmv2="urn:schemas-microsoft-com:asm.v2"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <assemblyIdentity version="1.0.0.0" name="MyApplication.app"/>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v2">
    <security>
      <requestedPrivileges xmlns="urn:schemas-microsoft-com:asm.v3">
        <!-- UAC Manifest Options
            If you want to change the Windows User Account Control level replace the
            requestedExecutionLevel node with one of the following.

        <requestedExecutionLevel  level="asInvoker" uiAccess="false" />
        <requestedExecutionLevel  level="requireAdministrator" uiAccess="false" />
        <requestedExecutionLevel  level="highestAvailable" uiAccess="false" />

            Specifying requestedExecutionLevel node will disable file and registry virtualization.
            If you want to utilize File and Registry Virtualization for backward
            compatibility then delete the requestedExecutionLevel node.
        -->
        <requestedExecutionLevel level="requireAdministrator" uiAccess="false" />
      </requestedPrivileges>
    </security>
  </trustInfo>

  <compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">
    <application>
      <!-- A list of all Windows versions that this application is designed to work with. Windows will automatically
select the most compatible environment.-->

      <!-- If your application is designed to work with Windows 7, uncomment the following supportedOS node-->
      <!--<supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"/>-->

    </application>
  </compatibility>

  <!-- Enable themes for Windows common controls and dialogs (Windows XP and later) -->
  <!-- <dependency>
    <dependentAssembly>
      <assemblyIdentity
          type="win32"
          name="Microsoft.Windows.Common-Controls"
          version="6.0.0.0"
          processorArchitecture="*"
          publicKeyToken="6595b64144ccf1df"
          language="*"
```

```
<?xml version="1.0" encoding="utf-8"?><asmv1:assembly manifestVersion="1.0" xmlns="urn:schemas-
```

Resource hacker provides us with icons and the manifest file of the executable.

7. What is the file trying to do with suspicious functions?

The file is a potential malware that does file manipulation using functions like CreateFile and DeleteFile repeated;y along with process manipulation using mutexes. No IP address is found, so the possibility of external communication can be ruled out.