```
----------DOS_HEADER----------

[IMAGE_DOS_HEADER]
0x0        0x0   e_magic:                       0x5A4D
0x2        0x2   e_cblp:                        0x90
0x4        0x4   e_cp:                          0x3
0x6        0x6   e_crlc:                        0x0
0x8        0x8   e_cparhdr:                     0x4
0xA        0xA   e_minalloc:                    0x0
0xC        0xC   e_maxalloc:                    0xFFFF
0xE        0xE   e_ss:                          0x0
0x10       0x10  e_sp:                          0xB8
0x12       0x12  e_csum:                        0x0
0x14       0x14  e_ip:                          0x0
0x16       0x16  e_cs:                          0x0
0x18       0x18  e_lfarlc:                      0x40
0x1A       0x1A  e_ovno:                        0x0
0x1C       0x1C  e_res:
0x24       0x24  e_oemid:                       0x0
0x26       0x26  e_oeminfo:                     0x0
0x28       0x28  e_res2:
0x3C       0x3C  e_lfanew:                      0x80

----------NT_HEADERS----------

[IMAGE_NT_HEADERS]
0x80       0x0   Signature:                     0x4550

----------FILE_HEADER----------

[IMAGE_FILE_HEADER]
0x84       0x0   Machine:                       0x14C
```

```
0x86       0x2   NumberOfSections:             0xF
0x88       0x4   TimeDateStamp:                0x54384BC6 [Fri Oct 10 21:12:38 2014 UTC]
0x8C       0x8   PointerToSymbolTable:         0xB800
0x90       0xC   NumberOfSymbols:              0x29D
0x94       0x10  SizeOfOptionalHeader:         0xE0
0x96       0x12  Characteristics:              0x127
Flags: IMAGE_FILE_32BIT_MACHINE, IMAGE_FILE_EXECUTABLE_IMAGE, IMAGE_FILE_LARGE_ADDRESS_AWARE,
IMAGE_FILE_LINE_NUMS_STRIPPED, IMAGE_FILE_RELOCS_STRIPPED

----------OPTIONAL_HEADER----------

[IMAGE_OPTIONAL_HEADER]
0x98       0x0   Magic:                        0x10B
0x9A       0x2   MajorLinkerVersion:           0x2
0x9B       0x3   MinorLinkerVersion:           0x18
0x9C       0x4   SizeOfCode:                   0xA00
0xA0       0x8   SizeOfInitializedData:        0x2000
0xA4       0xC   SizeOfUninitializedData:      0x200
0xA8       0x10  AddressOfEntryPoint:          0x1000
0xAC       0x14  BaseOfCode:                   0x1000
0xB0       0x18  BaseOfData:                   0x2000
0xB4       0x1C  ImageBase:                    0x400000
0xB8       0x20  SectionAlignment:             0x1000
0xBC       0x24  FileAlignment:                0x200
0xC0       0x28  MajorOperatingSystemVersion:  0x4
0xC2       0x2A  MinorOperatingSystemVersion:  0x0
0xC4       0x2C  MajorImageVersion:            0x1
0xC6       0x2E  MinorImageVersion:            0x0
0xC8       0x30  MajorSubsystemVersion:        0x4
0xCA       0x32  MinorSubsystemVersion:        0x0
0xCC       0x34  Reserved1:                    0x0
0xD0       0x38  SizeOfImage:                  0x16000
```

```
0xD4       0x3C  SizeOfHeaders:                0x400
0xD8       0x40  CheckSum:                     0x12385
0xDC       0x44  Subsystem:                    0x3
0xDE       0x46  DllCharacteristics:           0x8000
0xE0       0x48  SizeOfStackReserve:           0x200000
0xE4       0x4C  SizeOfStackCommit:            0x1000
0xE8       0x50  SizeOfHeapReserve:            0x100000
0xEC       0x54  SizeOfHeapCommit:             0x1000
0xF0       0x58  LoaderFlags:                  0x0
0xF4       0x5C  NumberOfRvaAndSizes:          0x10
DllCharacteristics: IMAGE_DLL_CHARACTERISTICS_TERMINAL_SERVER_AWARE

----------PE Sections----------

[IMAGE_SECTION_HEADER]
0x178      0x0   Name:                         .text
0x180      0x8   Misc:                         0x804
0x180      0x8   Misc_PhysicalAddress:         0x804
0x180      0x8   Misc_VirtualSize:            0x804
0x184      0xC   VirtualAddress:               0x1000
0x188      0x10  SizeOfRawData:                0xA00
0x18C      0x14  PointerToRawData:             0x400
0x190      0x18  PointerToRelocations:         0x0
0x194      0x1C  PointerToLinenumbers:         0x0
0x198      0x20  NumberOfRelocations:          0x0
0x19A      0x22  NumberOfLinenumbers:          0x0
0x19C      0x24  Characteristics:              0x60500060
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_8BYTES,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_CNT_CODE,
IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_MEM_EXECUTE,
IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2048BYTES,
IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
```

```
Entropy: 4.672394 (Min=0.0, Max=8.0)
MD5     hash: 1330e21b4846de52cdb52e13af206e20
SHA-1   hash: ec97f8b6d750204e4b3b77e56c267438dfa420f2
SHA-256 hash: 55d1e90579de16bedef3c36ea47db6fa7335d9adf43458008672e4515a798091
SHA-512 hash:
51ae0764c77c19b3fdaa952934ecaa3f910aa8e281d62d8eee082d32180dabf64bc826281ccf5e5ddea46b89617c93d1cd2241
6f99744eb30a564b49062df217

[IMAGE_SECTION_HEADER]
0x1A0      0x0   Name:                          .data
0x1A8      0x8   Misc:                          0x44
0x1A8      0x8   Misc_PhysicalAddress:          0x44
0x1A8      0x8   Misc_VirtualSize:             0x44
0x1AC      0xC   VirtualAddress:                0x2000
0x1B0      0x10  SizeOfRawData:                 0x200
0x1B4      0x14  PointerToRawData:              0xE00
0x1B8      0x18  PointerToRelocations:          0x0
0x1BC      0x1C  PointerToLinenumbers:          0x0
0x1C0      0x20  NumberOfRelocations:           0x0
0x1C2      0x22  NumberOfLinenumbers:           0x0
0x1C4      0x24  Characteristics:               0xC0600040
Flags: IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_8BYTES,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_16BYTES,
IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA,
IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1024BYTES,
IMAGE_SCN_MEM_READ
Entropy: 0.000000 (Min=0.0, Max=8.0)
MD5     hash: bf619eac0cdf3f68d496ea9344137e8b
SHA-1   hash: 5c3eb80066420002bc3dcc7ca4ab6efad7ed4ae5
SHA-256 hash: 076a27c79e5ace2a3d47f9dd2e83e4ff6ea8872b3c2218f66c92b89b55f36560
SHA-512 hash:
df40d4a774e0b453a5b87c00d6f0ef5d753143454e88ee5f7b607134598294c7905ccbcf94bbc46e474db6eb44e56a6dbb6d9a
```

1be9d4fb5d1b5f2d0c6ed34bfe

[IMAGE_SECTION_HEADER]
0x1C8 0x0 Name: .rdata
0x1D0 0x8 Misc: 0x370
0x1D0 0x8 Misc_PhysicalAddress: 0x370
0x1D0 0x8 Misc_VirtualSize: 0x370
0x1D4 0xC VirtualAddress: 0x3000
0x1D8 0x10 SizeOfRawData: 0x400
0x1DC 0x14 PointerToRawData: 0x1000
0x1E0 0x18 PointerToRelocations: 0x0
0x1E4 0x1C PointerToLinenumbers: 0x0
0x1E8 0x20 NumberOfRelocations: 0x0
0x1EA 0x22 NumberOfLinenumbers: 0x0
0x1EC 0x24 Characteristics: 0x40300040
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_512BYTES,
IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA,
IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
Entropy: 4.709421 (Min=0.0, Max=8.0)
MD5 hash: 38eb86a6e835c002f39dbdb53d2172fc
SHA-1 hash: df245a9199511fd579ebc150ab504323e4bb3126
SHA-256 hash: af0e156dc658b85153b355fb10ebfbdf3d221363817233abf835ed562fa08bef
SHA-512 hash:
41c8121d098145c64f1da484eea2f74f81ff43a7884649756f10524b465a1c748a52674b7307cc64a3e5ffdb9d0cd3b170bc0c
c5823ec7fceb422a7f2b9bb66b

[IMAGE_SECTION_HEADER]
0x1F0 0x0 Name: /4
0x1F8 0x8 Misc: 0x35
0x1F8 0x8 Misc_PhysicalAddress: 0x35
0x1F8 0x8 Misc_VirtualSize: 0x35

```
0x1FC      0xC   VirtualAddress:                0x4000
0x200      0x10  SizeOfRawData:                 0x200
0x204      0x14  PointerToRawData:              0x1400
0x208      0x18  PointerToRelocations:          0x0
0x20C      0x1C  PointerToLinenumbers:          0x0
0x210      0x20  NumberOfRelocations:           0x0
0x212      0x22  NumberOfLinenumbers:           0x0
0x214      0x24  Characteristics:               0x40300040
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_512BYTES,
IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA,
IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
Entropy: 0.540834 (Min=0.0, Max=8.0)
MD5     hash: a3d4813fe3203c95cdffd1a65807e1d5
SHA-1   hash: 6d4bd400725cbb0b886c801c2a9ecdbe3412d29d
SHA-256 hash: e442d444cc264f79e6d122b07f57789cf0046800a2c112eeaec5854e6f7ed9e5
SHA-512 hash:
c1aa9aee301c86646e39849c5265587f2332ee93c1533643edfd5e3a1dbbb5a1f06e45fa08b7709ba832c95f6e0eb71e8ced57
f9a476fa5a4f5bfa05f7bb9882

[IMAGE_SECTION_HEADER]
0x218      0x0   Name:                          /14
0x220      0x8   Misc:                          0x388
0x220      0x8   Misc_PhysicalAddress:          0x388
0x220      0x8   Misc_VirtualSize:              0x388
0x224      0xC   VirtualAddress:                0x5000
0x228      0x10  SizeOfRawData:                 0x400
0x22C      0x14  PointerToRawData:              0x1600
0x230      0x18  PointerToRelocations:          0x0
0x234      0x1C  PointerToLinenumbers:          0x0
0x238      0x20  NumberOfRelocations:           0x0
0x23A      0x22  NumberOfLinenumbers:           0x0
```

```
0x23C      0x24  Characteristics:               0x40300040
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_512BYTES,
IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA,
IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
Entropy: 3.692414 (Min=0.0, Max=8.0)
MD5     hash: d6c9c1745ffba20f244bb22b82026e2f
SHA-1   hash: c013330209334fe6f0f3c1831a6855b7bdf14fe2
SHA-256 hash: 4f8c8804a1845a84844a3e800bc2e47b8ab9c9d81fe557129b0a81bde44149ed
SHA-512 hash:
d9c941d270dff750882a1be57b54fcb86ad152b419347ed9e95f5b04a99ac2609153d99dec9217873237d7d45760f30c499cc7
0a61e39eaa4ad3732a4f701d4c

[IMAGE_SECTION_HEADER]
0x240      0x0   Name:                          .bss
0x248      0x8   Misc:                          0x114
0x248      0x8   Misc_PhysicalAddress:          0x114
0x248      0x8   Misc_VirtualSize:             0x114
0x24C      0xC   VirtualAddress:                0x6000
0x250      0x10  SizeOfRawData:                 0x0
0x254      0x14  PointerToRawData:              0x0
0x258      0x18  PointerToRelocations:          0x0
0x25C      0x1C  PointerToLinenumbers:          0x0
0x260      0x20  NumberOfRelocations:           0x0
0x262      0x22  NumberOfLinenumbers:           0x0
0x264      0x24  Characteristics:               0xC0600080
Flags: IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_8BYTES,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_16BYTES,
IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_CNT_UNINITIALIZED_DATA,
IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1024BYTES,
IMAGE_SCN_MEM_READ
Entropy: 0.000000 (Min=0.0, Max=8.0)
```

```
MD5     hash: d41d8cd98f00b204e9800998ecf8427e
SHA-1   hash: da39a3ee5e6b4b0d3255bfef95601890afd80709
SHA-256 hash: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA-512 hash:
cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931
bd47417a81a538327af927da3e

[IMAGE_SECTION_HEADER]
0x268      0x0   Name:                          .idata
0x270      0x8   Misc:                          0x274
0x270      0x8   Misc_PhysicalAddress:          0x274
0x270      0x8   Misc_VirtualSize:             0x274
0x274      0xC   VirtualAddress:                0x7000
0x278      0x10  SizeOfRawData:                 0x400
0x27C      0x14  PointerToRawData:              0x1A00
0x280      0x18  PointerToRelocations:          0x0
0x284      0x1C  PointerToLinenumbers:          0x0
0x288      0x20  NumberOfRelocations:           0x0
0x28A      0x22  NumberOfLinenumbers:           0x0
0x28C      0x24  Characteristics:               0xC0300040
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_16BYTES,
IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_256BYTES,
IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES,
IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
Entropy: 2.856460 (Min=0.0, Max=8.0)
MD5     hash: f4b39be28ee292ce9f4fcc955341ef41
SHA-1   hash: bac589fc425bb53f32f0032b9b3e5bf0dc15dc92
SHA-256 hash: e61ec06ea021bf6024ebf828b21b570c71aa6abca8c51a876114adea5578bf9c
SHA-512 hash:
8be03f8a2f2b0dd989ceb8212b1767158513637e1e4f2197c5672ccdd8a078b03fca62b9ef6615bc051677db944f7f5b22887e
80028e2b7b392f811564fc37d2
```

```
[IMAGE_SECTION_HEADER]
0x290      0x0   Name:                          .rsrc
0x298      0x8   Misc:                          0x460
0x298      0x8   Misc_PhysicalAddress:          0x460
0x298      0x8   Misc_VirtualSize:             0x460
0x29C      0xC   VirtualAddress:                0x8000
0x2A0      0x10  SizeOfRawData:                 0x600
0x2A4      0x14  PointerToRawData:              0x1E00
0x2A8      0x18  PointerToRelocations:          0x0
0x2AC      0x1C  PointerToLinenumbers:          0x0
0x2B0      0x20  NumberOfRelocations:           0x0
0x2B2      0x22  NumberOfLinenumbers:           0x0
0x2B4      0x24  Characteristics:               0xC0300040
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_16BYTES,
IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_256BYTES,
IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES,
IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
Entropy: 4.443020 (Min=0.0, Max=8.0)
MD5     hash: b40b90e62b4676beb27eeab365141cc5
SHA-1   hash: 21c8e346f2415ebf47d68b2f0dfa475550792247
SHA-256 hash: 2a61767a9dfaf978c5bde5eea187aa0036e6fb3a4462dadff5cae3ba4c73eb4b
SHA-512 hash:
322dec8713b554eceef717c676e0858d7a7cff1e18310a7d4f5e7fc9a8738adc2f002ed0a8e22054de8aee501791954090a265
86dc5e7b05fbb3c1df92bad194

[IMAGE_SECTION_HEADER]
0x2B8      0x0   Name:                          /24
0x2C0      0x8   Misc:                          0x178
0x2C0      0x8   Misc_PhysicalAddress:          0x178
0x2C0      0x8   Misc_VirtualSize:             0x178
```

```
0x2C4      0xC   VirtualAddress:                0x9000
0x2C8      0x10  SizeOfRawData:                 0x200
0x2CC      0x14  PointerToRawData:              0x2400
0x2D0      0x18  PointerToRelocations:          0x0
0x2D4      0x1C  PointerToLinenumbers:          0x0
0x2D8      0x20  NumberOfRelocations:           0x0
0x2DA      0x22  NumberOfLinenumbers:           0x0
0x2DC      0x24  Characteristics:               0x42100040
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_256BYTES,
IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_64BYTES,
IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
Entropy: 1.607206 (Min=0.0, Max=8.0)
MD5     hash: 3678e1e85982f749cd74ffb088f3c695
SHA-1   hash: 204125cf2b4f4702c7fe15245f5a7f95e1f640ce
SHA-256 hash: 6cdb87a038b434c32a306d381f8b4a3d375b010cd3e44ceed5337968fd1fd974
SHA-512 hash:
b25bc1cee5bea04eeba9fc786ca07da9965938c0ded2b95794f6a62881433971b3d68843bb63a6592d4a6edf3a8e373daea65e
bb0eccd91ebb5b7f20b4b3dba4

[IMAGE_SECTION_HEADER]
0x2E0      0x0   Name:                          /39
0x2E8      0x8   Misc:                          0x6EDC
0x2E8      0x8   Misc_PhysicalAddress:          0x6EDC
0x2E8      0x8   Misc_VirtualSize:              0x6EDC
0x2EC      0xC   VirtualAddress:                0xA000
0x2F0      0x10  SizeOfRawData:                 0x7000
0x2F4      0x14  PointerToRawData:              0x2600
0x2F8      0x18  PointerToRelocations:          0x0
0x2FC      0x1C  PointerToLinenumbers:          0x0
0x300      0x20  NumberOfRelocations:           0x0
0x302      0x22  NumberOfLinenumbers:           0x0
```

```
0x304      0x24  Characteristics:               0x42100040
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_256BYTES,
IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_64BYTES,
IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
Entropy: 6.028770 (Min=0.0, Max=8.0)
MD5     hash: 958e45ef6d76ec0a39b774095a8e4214
SHA-1   hash: 3ac9a9d29c4ad2941ad1641d9a6904e7e693baf1
SHA-256 hash: c466fb5d88ed0a15ed0815ebfdb9e049e0853a0197179d7e109ce5799b695198
SHA-512 hash:
12867b621da11ca3314c008bd5beffebdd47d794637e14401e13d85d5ddf980df62e04dda1864214af85e84d89e7ad03d7ecc4
3b05dc50f0f5552ee6bc6dc013

[IMAGE_SECTION_HEADER]
0x308      0x0   Name:                          /51
0x310      0x8   Misc:                          0xCB1
0x310      0x8   Misc_PhysicalAddress:          0xCB1
0x310      0x8   Misc_VirtualSize:             0xCB1
0x314      0xC   VirtualAddress:                0x11000
0x318      0x10  SizeOfRawData:                 0xE00
0x31C      0x14  PointerToRawData:              0x9600
0x320      0x18  PointerToRelocations:          0x0
0x324      0x1C  PointerToLinenumbers:          0x0
0x328      0x20  NumberOfRelocations:           0x0
0x32A      0x22  NumberOfLinenumbers:           0x0
0x32C      0x24  Characteristics:               0x42100040
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_256BYTES,
IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_64BYTES,
IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
Entropy: 4.347152 (Min=0.0, Max=8.0)
MD5     hash: 93f06f191608277fae1e61671b0ed95d
```

```
SHA-1   hash: af31bfb059a02226c8155a8e9371748f24356a1d
SHA-256 hash: 49e5e440f705a75b96f2e0b0a719d070ce373503fcbd975cd6d0cc2e1e439ae5
SHA-512 hash:
7f13dc690406a8ba225cdc6bb7e8ccea08f3dcc6c584f8d739a5de72336cc3e80086d5ad5e59702a7b6c68c5a07d661faba0ff
1c09dbfb4d460b0a4f8f8487a1

[IMAGE_SECTION_HEADER]
0x330      0x0   Name:                          /65
0x338      0x8   Misc:                          0xDB8
0x338      0x8   Misc_PhysicalAddress:          0xDB8
0x338      0x8   Misc_VirtualSize:             0xDB8
0x33C      0xC   VirtualAddress:                0x12000
0x340      0x10  SizeOfRawData:                 0xE00
0x344      0x14  PointerToRawData:              0xA400
0x348      0x18  PointerToRelocations:          0x0
0x34C      0x1C  PointerToLinenumbers:          0x0
0x350      0x20  NumberOfRelocations:           0x0
0x352      0x22  NumberOfLinenumbers:           0x0
0x354      0x24  Characteristics:               0x42100040
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_256BYTES,
IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_64BYTES,
IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
Entropy: 5.047972 (Min=0.0, Max=8.0)
MD5     hash: 542138829307908bc79f1f882f04d757
SHA-1   hash: c2b7ca937dbf0fbc63959770bc935fa984a71319
SHA-256 hash: e5b96de3e67f577f295c215bcc049c624f0e88530aa863767ddb383575ac0d51
SHA-512 hash:
f28de40f926f7d9749aa213b8f3b937f3201cd11554ca5ced49713927c3895970784f1da5eae386e425db4b949423e819b6022
aa08da53d38809d20df0111c23

[IMAGE_SECTION_HEADER]
```

```
0x358      0x0   Name:                         /77
0x360      0x8   Misc:                         0x43
0x360      0x8   Misc_PhysicalAddress:         0x43
0x360      0x8   Misc_VirtualSize:             0x43
0x364      0xC   VirtualAddress:               0x13000
0x368      0x10  SizeOfRawData:                0x200
0x36C      0x14  PointerToRawData:             0xB200
0x370      0x18  PointerToRelocations:         0x0
0x374      0x1C  PointerToLinenumbers:         0x0
0x378      0x20  NumberOfRelocations:          0x0
0x37A      0x22  NumberOfLinenumbers:          0x0
0x37C      0x24  Characteristics:              0x42100040
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_256BYTES,
IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_64BYTES,
IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
Entropy: 0.999676 (Min=0.0, Max=8.0)
MD5     hash: 15e98a141785ec1e9058317df179468f
SHA-1   hash: 71a4560ed071af52f0bf7922e847759f95e87015
SHA-256 hash: 3a7932dccf3a9e26a691b87cde3988f61f67fb43d199631623855fa69a0c83f2
SHA-512 hash:
d523e8b72cc262e20e18cf6c747b509cb90e14a3ba9bb36299de6d577ba6c0cf0a8393c8943e5e986bd65197afdc9798ba3d1b
3cc7eb9b5511dc7b0b0cf5f622

[IMAGE_SECTION_HEADER]
0x380      0x0   Name:                         /88
0x388      0x8   Misc:                         0x150
0x388      0x8   Misc_PhysicalAddress:         0x150
0x388      0x8   Misc_VirtualSize:             0x150
0x38C      0xC   VirtualAddress:               0x14000
0x390      0x10  SizeOfRawData:                0x200
0x394      0x14  PointerToRawData:             0xB400
```

```
0x398      0x18  PointerToRelocations:          0x0
0x39C      0x1C  PointerToLinenumbers:          0x0
0x3A0      0x20  NumberOfRelocations:           0x0
0x3A2      0x22  NumberOfLinenumbers:           0x0
0x3A4      0x24  Characteristics:               0x42100040
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_256BYTES,
IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_64BYTES,
IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
Entropy: 1.810615 (Min=0.0, Max=8.0)
MD5     hash: 37660a3663b847c72f9c164c6906bb19
SHA-1   hash: 2fe07b27e11e69fc029d7d701a50c4536533e961
SHA-256 hash: 0c04e7559e9f9a68a56dae2cae4efaa5907ae99589ea1e74ef1d855f40da4263
SHA-512 hash:
e94df108514a931f2bfb56f1ae70947305644887074b9c7a5c95640710d194022341e76a93063a94de722b7c0a0c77fde4098c
f29b1c163d28ffba981a37ce37

[IMAGE_SECTION_HEADER]
0x3A8      0x0   Name:                          /99
0x3B0      0x8   Misc:                          0x18
0x3B0      0x8   Misc_PhysicalAddress:          0x18
0x3B0      0x8   Misc_VirtualSize:              0x18
0x3B4      0xC   VirtualAddress:                0x15000
0x3B8      0x10  SizeOfRawData:                 0x200
0x3BC      0x14  PointerToRawData:              0xB600
0x3C0      0x18  PointerToRelocations:          0x0
0x3C4      0x1C  PointerToLinenumbers:          0x0
0x3C8      0x20  NumberOfRelocations:           0x0
0x3CA      0x22  NumberOfLinenumbers:           0x0
0x3CC      0x24  Characteristics:               0x42100040
Flags: IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_MASK,
IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_256BYTES,
```

```
IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_64BYTES,
IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_READ
Entropy: 0.138730 (Min=0.0, Max=8.0)
MD5     hash: e22fefb29d3806ea0176f79bbd80e4a1
SHA-1   hash: b7686bce64655a93a77978d01e60d47fd013f6e2
SHA-256 hash: 2035926e8093354a0d3222f1f7fe1a212ed5b21689c13e6b5a100c9ba2a986ee
SHA-512 hash:
ab19147a1e445866f74d5bfe8f43a11f01c71b088d34b7b0f13ff1749afbf2301449ea2c151ea46afe17c41b8a729091fd4342
fe6d098042e5362c40cf283f9b

----------Directories----------

[IMAGE_DIRECTORY_ENTRY_EXPORT]
0xF8       0x0   VirtualAddress:              0x0
0xFC       0x4   Size:                        0x0
[IMAGE_DIRECTORY_ENTRY_IMPORT]
0x100      0x0   VirtualAddress:              0x7000
0x104      0x4   Size:                        0x274
[IMAGE_DIRECTORY_ENTRY_RESOURCE]
0x108      0x0   VirtualAddress:              0x8000
0x10C      0x4   Size:                        0x460
[IMAGE_DIRECTORY_ENTRY_EXCEPTION]
0x110      0x0   VirtualAddress:              0x0
0x114      0x4   Size:                        0x0
[IMAGE_DIRECTORY_ENTRY_SECURITY]
0x118      0x0   VirtualAddress:              0x0
0x11C      0x4   Size:                        0x0
[IMAGE_DIRECTORY_ENTRY_BASERELOC]
0x120      0x0   VirtualAddress:              0x0
0x124      0x4   Size:                        0x0
[IMAGE_DIRECTORY_ENTRY_DEBUG]
0x128      0x0   VirtualAddress:              0x4000
```

```
0x12C      0x4   Size:                           0x1C
[IMAGE_DIRECTORY_ENTRY_COPYRIGHT]
0x130      0x0   VirtualAddress:                 0x0
0x134      0x4   Size:                           0x0
[IMAGE_DIRECTORY_ENTRY_GLOBALPTR]
0x138      0x0   VirtualAddress:                 0x0
0x13C      0x4   Size:                           0x0
[IMAGE_DIRECTORY_ENTRY_TLS]
0x140      0x0   VirtualAddress:                 0x0
0x144      0x4   Size:                           0x0
[IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG]
0x148      0x0   VirtualAddress:                 0x0
0x14C      0x4   Size:                           0x0
[IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT]
0x150      0x0   VirtualAddress:                 0x0
0x154      0x4   Size:                           0x0
[IMAGE_DIRECTORY_ENTRY_IAT]
0x158      0x0   VirtualAddress:                 0x7094
0x15C      0x4   Size:                           0x58
[IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT]
0x160      0x0   VirtualAddress:                 0x0
0x164      0x4   Size:                           0x0
[IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR]
0x168      0x0   VirtualAddress:                 0x0
0x16C      0x4   Size:                           0x0
[IMAGE_DIRECTORY_ENTRY_RESERVED]
0x170      0x0   VirtualAddress:                 0x0
0x174      0x4   Size:                           0x0

----------Imported symbols----------

[IMAGE_IMPORT_DESCRIPTOR]
```

```
0x1A00     0x0   OriginalFirstThunk:           0x703C
0x1A00     0x0   Characteristics:              0x703C
0x1A04     0x4   TimeDateStamp:                0x0        [Thu Jan  1 00:00:00 1970 UTC]
0x1A08     0x8   ForwarderChain:               0x0
0x1A0C     0xC   Name:                         0x7248
0x1A10     0x10  FirstThunk:                   0x7094

cygwin1.dll.__main Hint[67]
cygwin1.dll._dll_crt0@0 Hint[190]
cygwin1.dll._impure_ptr Hint[375]
cygwin1.dll.atexit Hint[724]
cygwin1.dll.calloc Hint[745]
cygwin1.dll.cygwin_detach_dll Hint[847]
cygwin1.dll.cygwin_internal Hint[849]
cygwin1.dll.dll_dllcrt0 Hint[870]
cygwin1.dll.free Hint[1012]
cygwin1.dll.gets Hint[1126]
cygwin1.dll.malloc Hint[1294]
cygwin1.dll.posix_memalign Hint[1392]
cygwin1.dll.printf Hint[1425]
cygwin1.dll.puts Hint[1533]
cygwin1.dll.realloc Hint[1554]
cygwin1.dll.strcmp Hint[1753]

[IMAGE_IMPORT_DESCRIPTOR]
0x1A14     0x0   OriginalFirstThunk:           0x7080
0x1A14     0x0   Characteristics:              0x7080
0x1A18     0x4   TimeDateStamp:                0x0        [Thu Jan  1 00:00:00 1970 UTC]
0x1A1C     0x8   ForwarderChain:               0x0
0x1A20     0xC   Name:                         0x7264
0x1A24     0x10  FirstThunk:                   0x70D8
```

```
KERNEL32.dll.FreeLibrary Hint[356]
KERNEL32.dll.GetModuleHandleA Hint[533]
KERNEL32.dll.GetProcAddress Hint[581]
KERNEL32.dll.LoadLibraryA Hint[809]

----------Resource directory----------

[IMAGE_RESOURCE_DIRECTORY]
0x1E00     0x0   Characteristics:              0x0
0x1E04     0x4   TimeDateStamp:                0x0        [Thu Jan  1 00:00:00 1970 UTC]
0x1E08     0x8   MajorVersion:                 0x0
0x1E0A     0xA   MinorVersion:                 0x0
0x1E0C     0xC   NumberOfNamedEntries:         0x0
0x1E0E     0xE   NumberOfIdEntries:           0x1
  Id: [0x18] (RT_MANIFEST)
  [IMAGE_RESOURCE_DIRECTORY_ENTRY]
  0x1E10     0x0   Name:                         0x18
  0x1E14     0x4   OffsetToData:                 0x80000018
    [IMAGE_RESOURCE_DIRECTORY]
    0x1E18     0x0   Characteristics:            0x0
    0x1E1C     0x4   TimeDateStamp:              0x0        [Thu Jan  1 00:00:00 1970 UTC]
    0x1E20     0x8   MajorVersion:               0x0
    0x1E22     0xA   MinorVersion:               0x0
    0x1E24     0xC   NumberOfNamedEntries:       0x0
    0x1E26     0xE   NumberOfIdEntries:         0x1
      Id: [0x1]
      [IMAGE_RESOURCE_DIRECTORY_ENTRY]
      0x1E28     0x0   Name:                       0x1
      0x1E2C     0x4   OffsetToData:               0x80000030
        [IMAGE_RESOURCE_DIRECTORY]
        0x1E30     0x0   Characteristics:          0x0
        0x1E34     0x4   TimeDateStamp:            0x0        [Thu Jan  1 00:00:00 1970 UTC]
```

```
        0x1E38     0x8   MajorVersion:                0x0
        0x1E3A     0xA   MinorVersion:                0x0
        0x1E3C     0xC   NumberOfNamedEntries:        0x0
        0x1E3E     0xE   NumberOfIdEntries:           0x1
        \--- LANG [0,0][LANG_NEUTRAL,SUBLANG_NEUTRAL]
          [IMAGE_RESOURCE_DIRECTORY_ENTRY]
          0x1E40     0x0   Name:                        0x0
          0x1E44     0x4   OffsetToData:               0x48
            [IMAGE_RESOURCE_DATA_ENTRY]
            0x1E48     0x0   OffsetToData:               0x8058
            0x1E4C     0x4   Size:                       0x405
            0x1E50     0x8   CodePage:                   0x0
            0x1E54     0xC   Reserved:                   0x0


----------Debug information----------

[IMAGE_DEBUG_DIRECTORY]
0x1400     0x0   Characteristics:            0x0
0x1404     0x4   TimeDateStamp:              0x0        [Thu Jan  1 00:00:00 1970 UTC]
0x1408     0x8   MajorVersion:               0x0
0x140A     0xA   MinorVersion:               0x0
0x140C     0xC   Type:                       0x2
0x1410     0x10  SizeOfData:                 0x19
0x1414     0x14  AddressOfRawData:           0x401C
0x1418     0x18  PointerToRawData:           0x141C
Type: IMAGE_DEBUG_TYPE_CODEVIEW
```