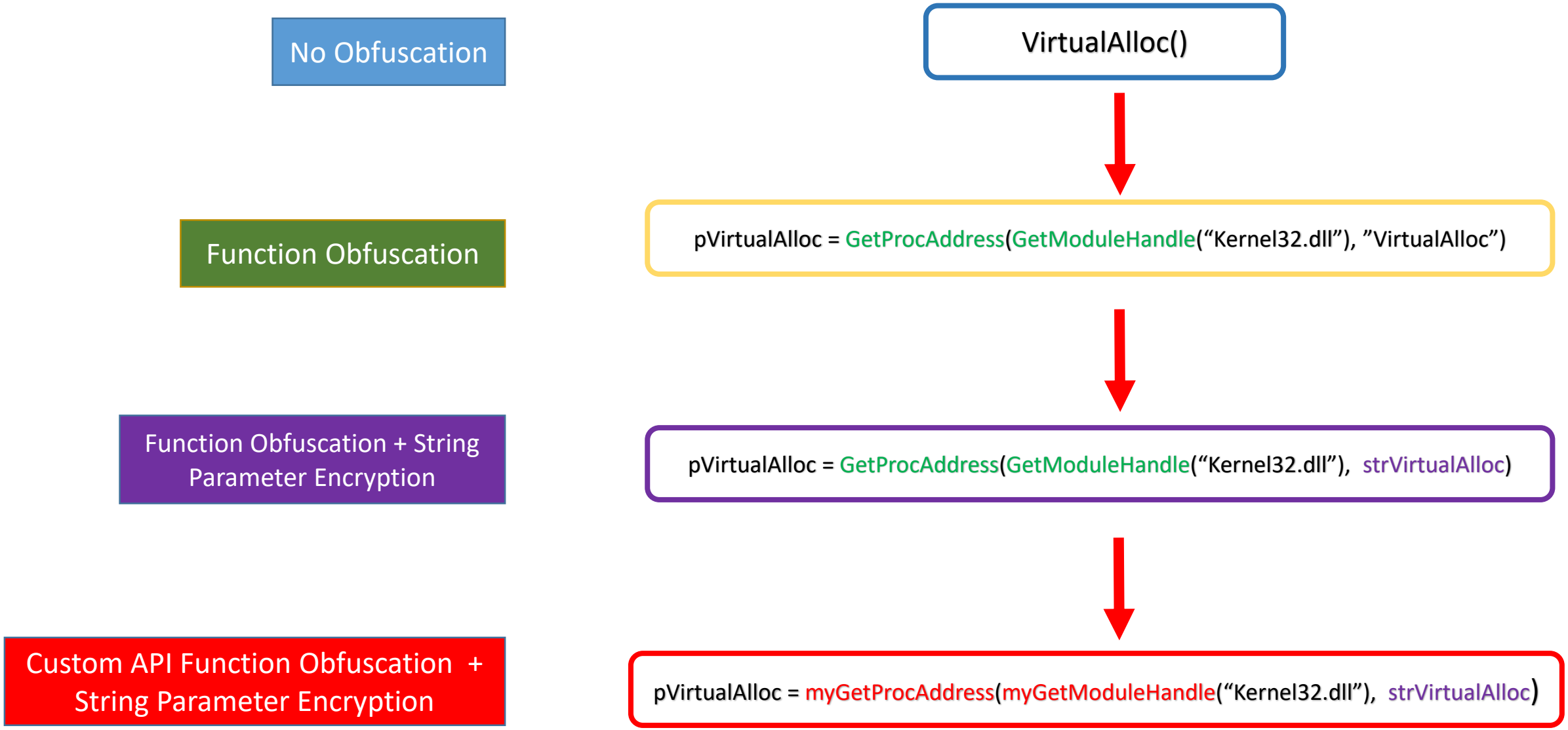
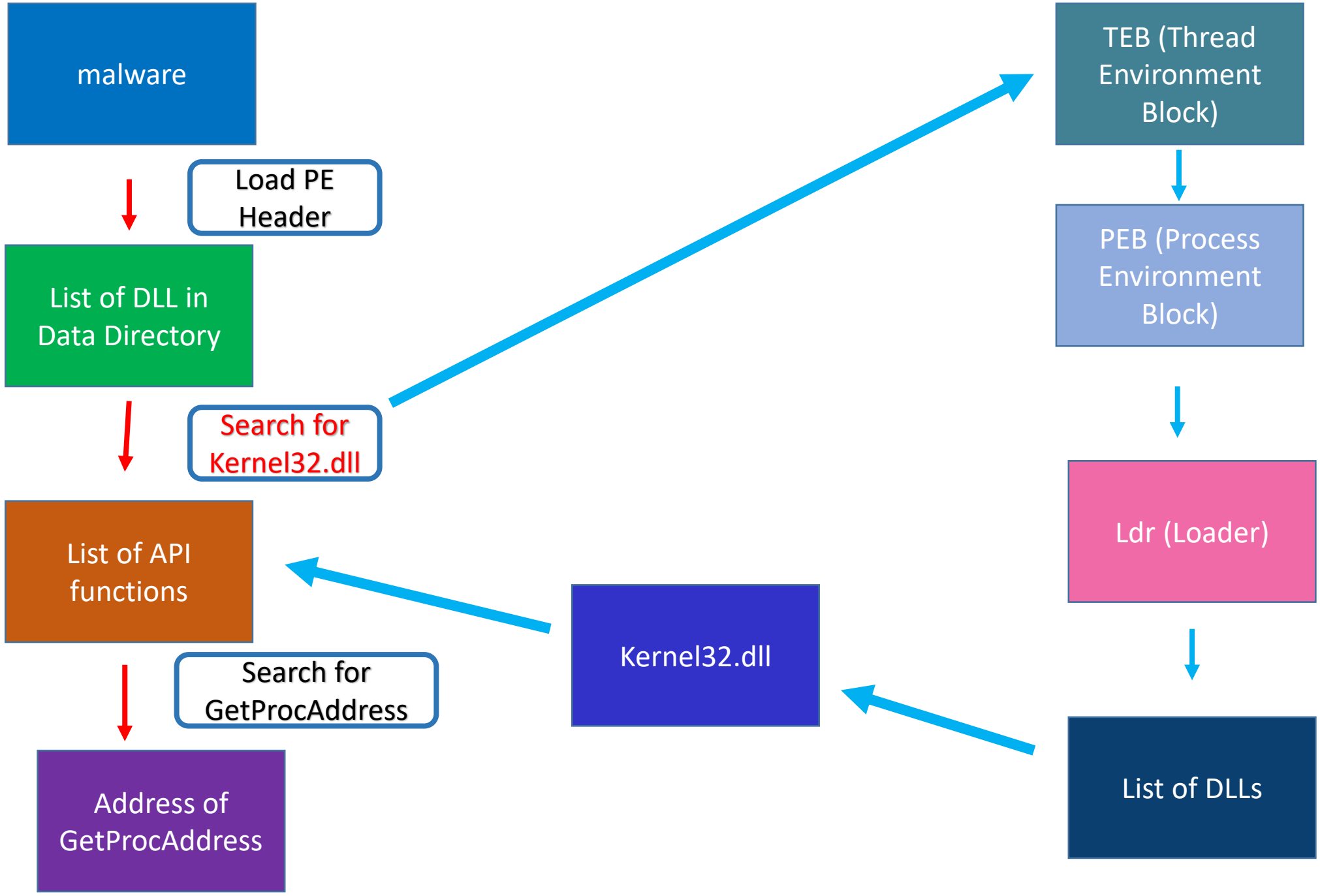
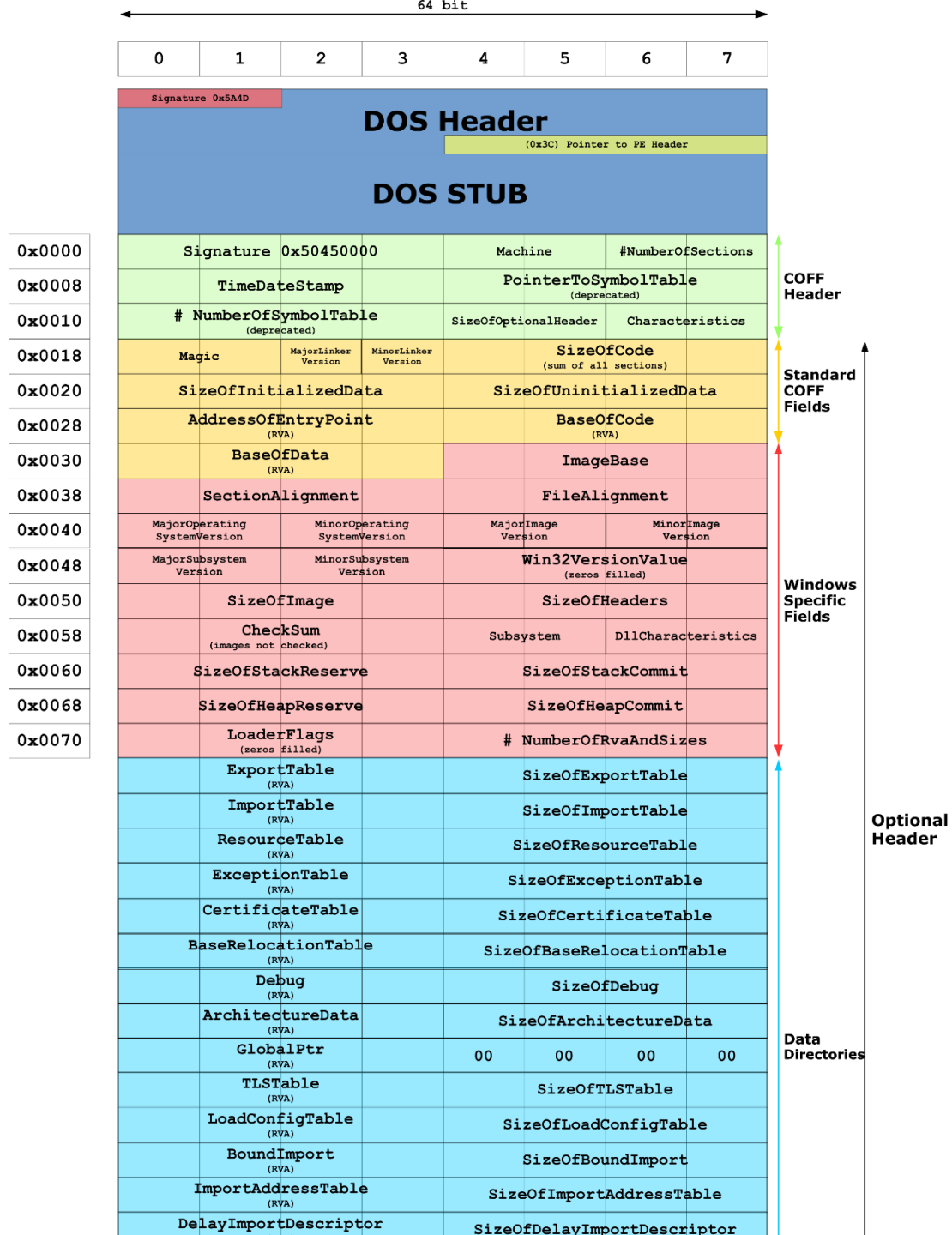
Advanced Function Obfuscation

Implementing Your Own Custom win32 API functions

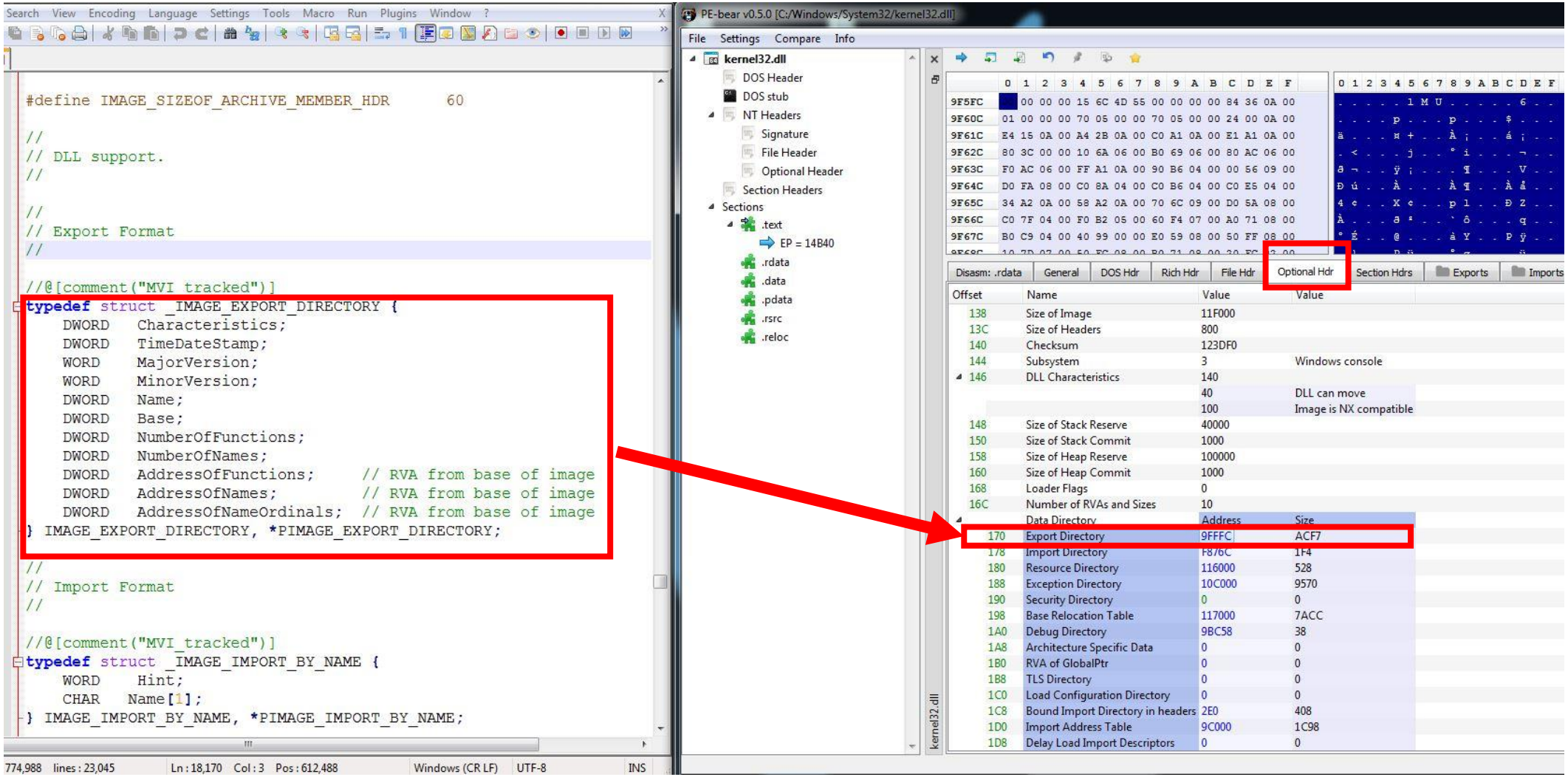

No Obfuscation
VirtualAlloc()
Function Obfuscation
pVirtualAlloc = GetProcAddress(GetModuleHandle("Kernel32.dll"), "VirtualAlloc")
Function Obfuscation + String Parameter Encryption
pVirtualAlloc = GetProcAddress(GetModuleHandle("Kernel32.dll"), strVirtualAlloc)
Custom API Function Obfuscation + String Parameter Encryption
pVirtualAlloc = myGetProcAddress(myGetModuleHandle("Kernel32.dll"), strVirtualAlloc)


malware
Load PE Header
List of DLL in Data Directory
Search for Kernel32.dll
List of API functions
Search for GetProcAddress
Address of GetProcAddress
Kernel32.dll
List of DLLs
Ldr (Loader)
PEB (Process Environment Block)
TEB (Thread Environment Block)


64 bit
0
1
2
3
4
5
6
7
Signature 0x5A4D
DOS Header
(0x3C) Pointer to PE Header
DOS STUB
0x0000
0x0008
0x0010
0x0018
0x0020
0x0028
0x0030
0x0038
0x0040
0x0048
0x0050
0x0058
0x0060
0x0068
0x0070
Signature 0x50450000
Machine
#NumberOfSections
TimeDateStamp
PointerToSymbolTable
(deprecated)
NumberOfSymbolTable
(deprecated)
SizeOfOptionalHeader
Characteristics
Magic
MajorLinker Version
MinorLinker Version
SizeOfCode
(sum of all sections)
SizeOfInitializedData
SizeOfUninitializedData
AddressOfEntryPoint
(RVA)
BaseOfCode
(RVA)
BaseOfData
(RVA)
ImageBase
SectionAlignment
FileAlignment
MajorOperating SystemVersion
MinorOperating SystemVersion
MajorImage Version
MinorImage Version
MajorSubsystem Version
MinorSubsystem Version
Win32VersionValue
(zeros filled)
SizeOfImage
SizeOfHeaders
CheckSum
(images not checked)
Subsystem
DllCharacteristics
SizeOfStackReserve
SizeOfStackCommit
SizeOfHeapReserve
SizeOfHeapCommit
LoaderFlags
(zeros filled)
NumberOfRvaAndSizes
ExportTable
(RVA)
SizeOfExportTable
ImportTable
(RVA)
SizeOfImportTable
ResourceTable
(RVA)
SizeOfResourceTable
ExceptionTable
(RVA)
SizeOfExceptionTable
CertificateTable
(RVA)
SizeOfCertificateTable
BaseRelocationTable
(RVA)
SizeOfBaseRelocationTable
Debug
(RVA)
SizeOfDebug
ArchitectureData
(RVA)
SizeOfArchitectureData
GlobalPtr
(RVA)
00
00
00
00
TLSTable
(RVA)
SizeOfTLSTable
LoadConfigTable
(RVA)
SizeOfLoadConfigTable
BoundImport
(RVA)
SizeOfBoundImport
ImportAddressTable
(RVA)
SizeOfImportAddressTable
DelayImportDescriptor
SizeOfDelayImportDescriptor
COFF Header
Standard COFF Fields
Windows Specific Fields
Data Directories
Optional Header

winnt.h

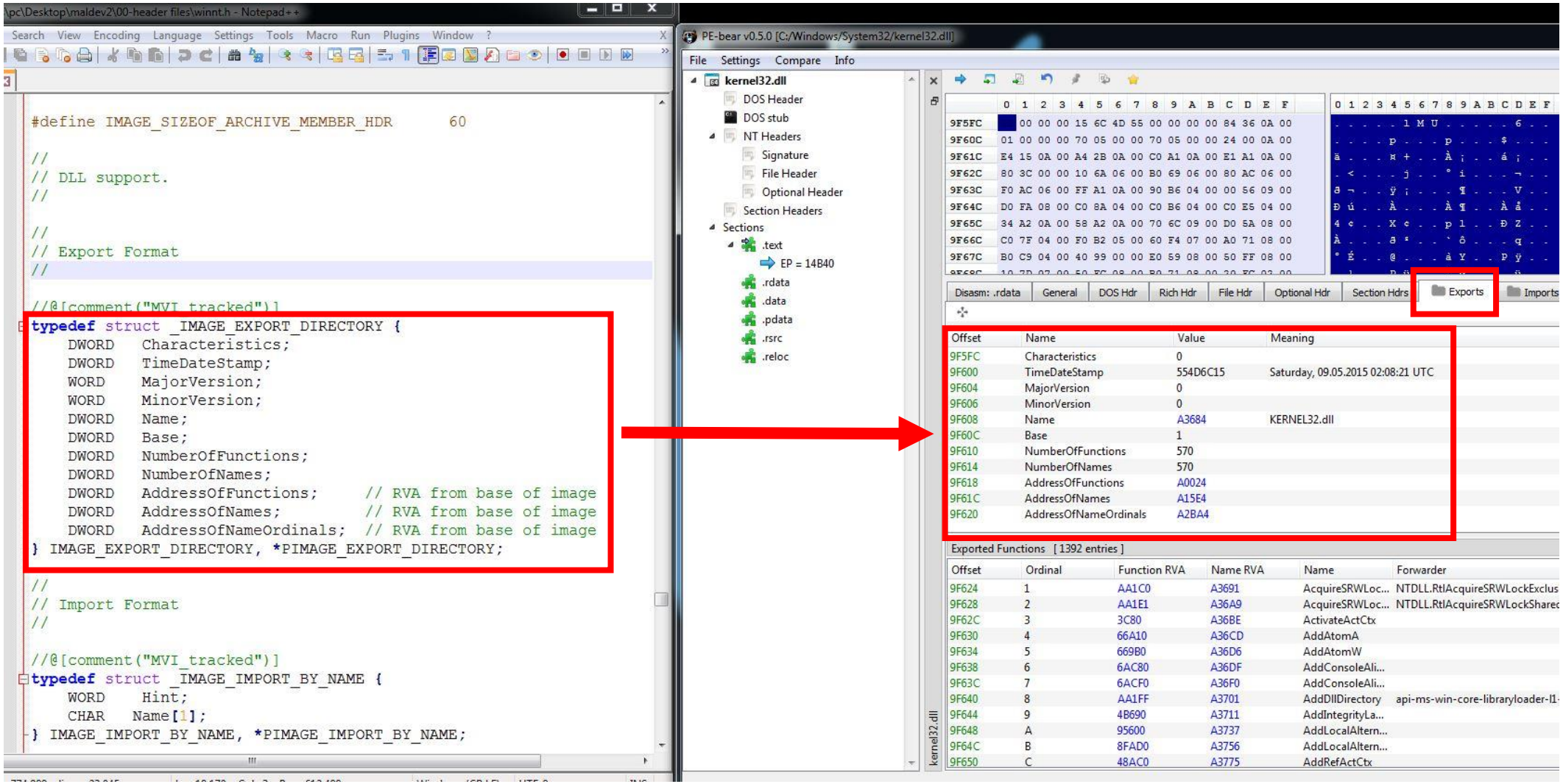
PE Header of Kernel32.dll (Optional Header Tab)



```
#define IMAGE_SIZEOF_ARCHIVE_MEMBER_HDR      60

//
// DLL support.
//

//
// Export Format
//

//@[comment("MVI_tracked")]
typedef struct _IMAGE_EXPORT_DIRECTORY {
    DWORD   Characteristics;
    DWORD   TimeDateStamp;
    WORD    MajorVersion;
    WORD    MinorVersion;
    DWORD   Name;
    DWORD   Base;
    DWORD   NumberOfFunctions;
    DWORD   NumberOfNames;
    DWORD   AddressOfFunctions;     // RVA from base of image
    DWORD   AddressOfNames;         // RVA from base of image
    DWORD   AddressOfNameOrdinals;  // RVA from base of image
} IMAGE_EXPORT_DIRECTORY, *PIMAGE_EXPORT_DIRECTORY;

//
// Import Format
//

//@[comment("MVI_tracked")]
typedef struct _IMAGE_IMPORT_BY_NAME {
    WORD    Hint;
    CHAR    Name[1];
} IMAGE_IMPORT_BY_NAME, *PIMAGE_IMPORT_BY_NAME;
```

winnt.h

PE Header of Kernel32.dll (Exports Tab)



Thank you