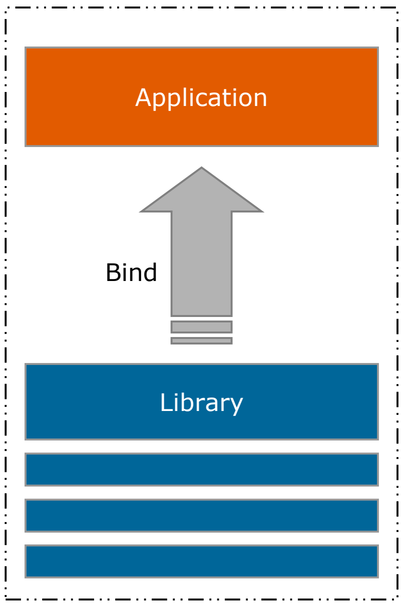
Windows Dynamic-Link Libraries

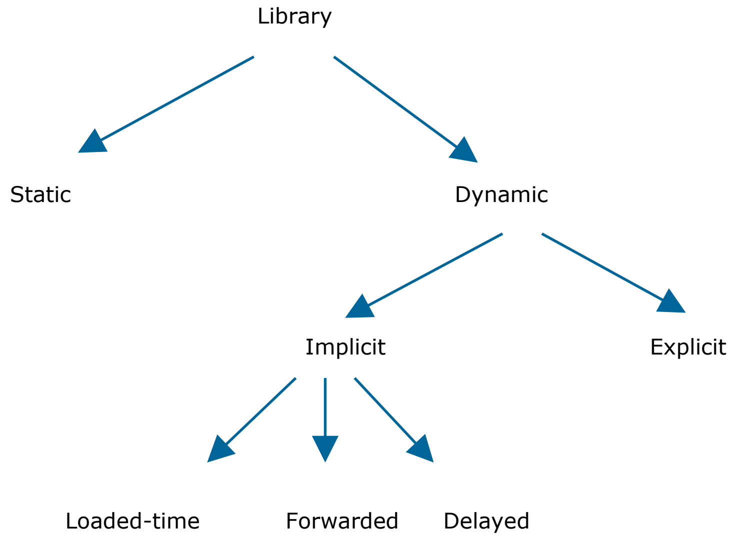
Introduction

- Cornerstone of Windows
- Reuse components
- Enable plugging mechanism
- Simplify project development
- Reduce system consumption
- Support localization
- Resolve platform differences
- Save testing/validation time

Libraries - Types

- Different types of libraries exist with different characteristics

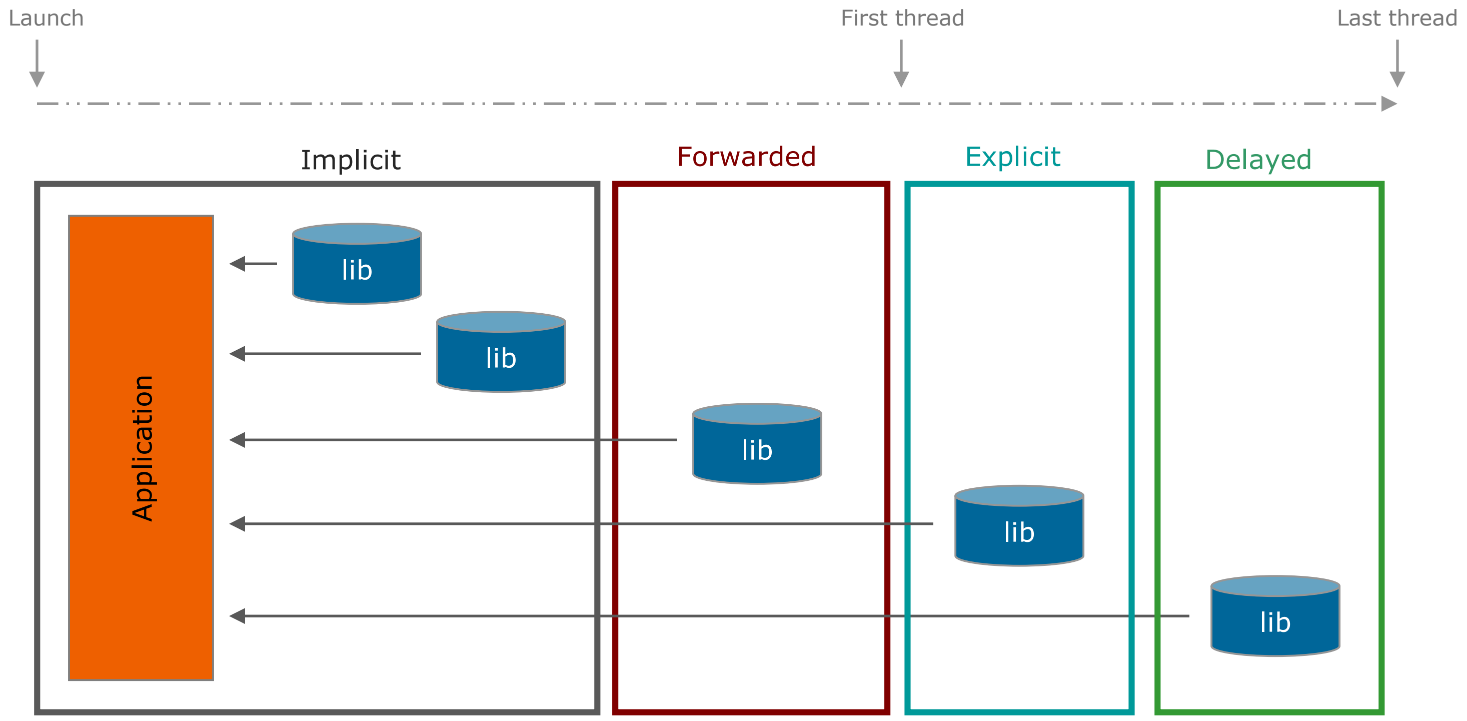




Windows Dynamic-Link Libraries

Binding Types

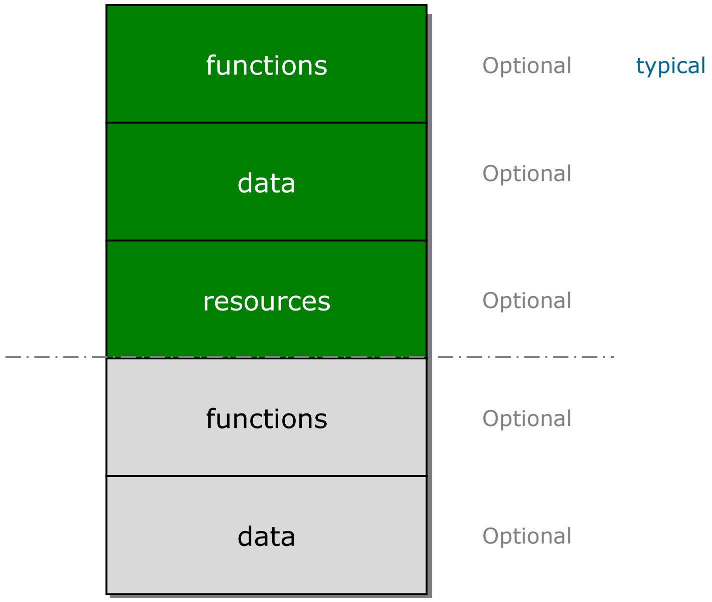
- Different binding types during a process's life-time



Windows Dynamic-Link Libraries

Components

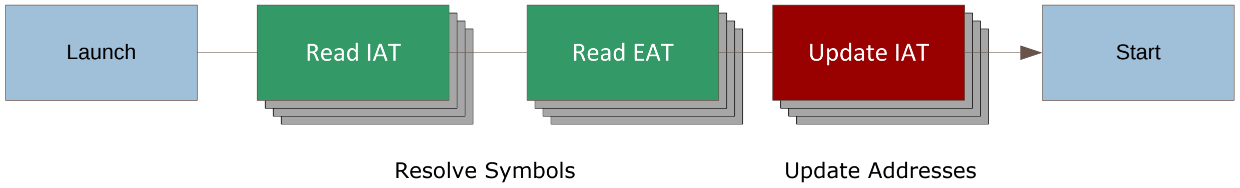
- Some components can be made public



Windows Dynamic-Link Libraries

Implicit Linking

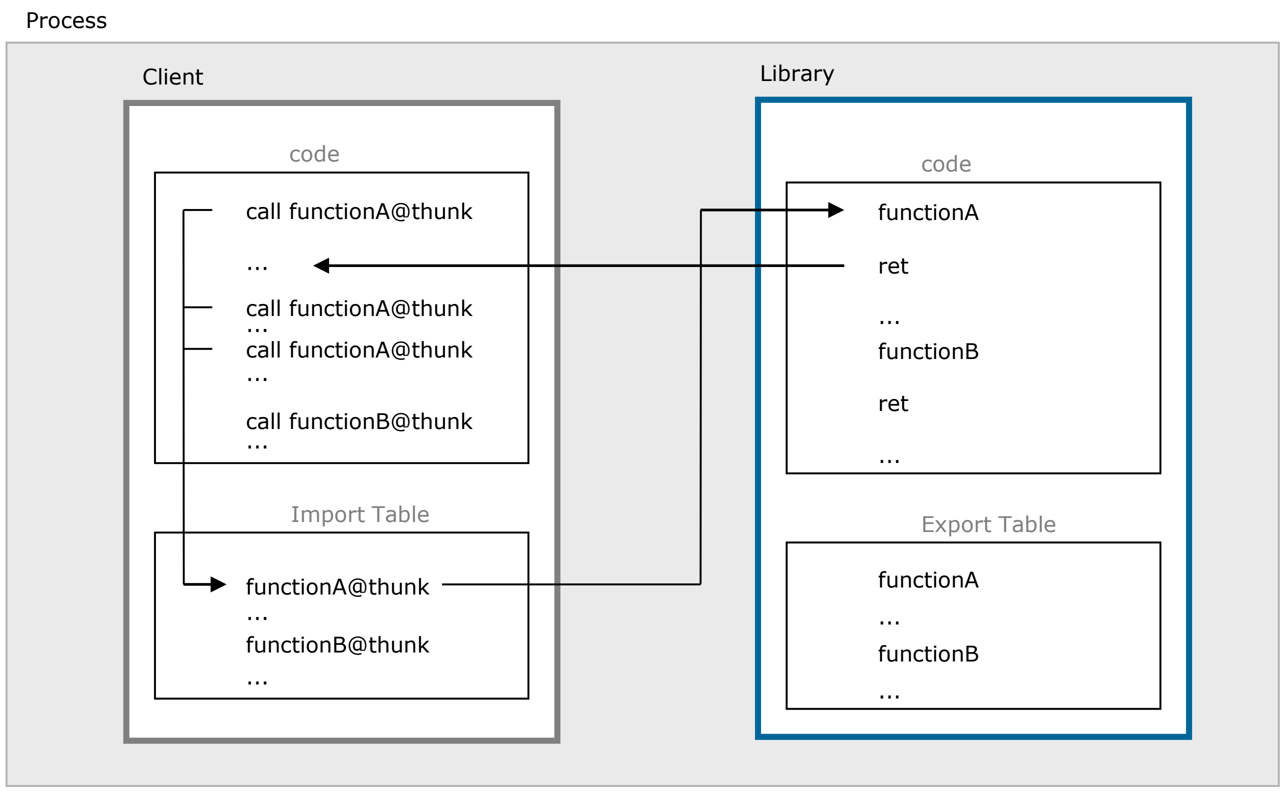
- Most common case
- Dependencies created during development
- Binding occurs when starting the client application



Windows Dynamic-Link Libraries

Implicit Linking

- Invoking methods



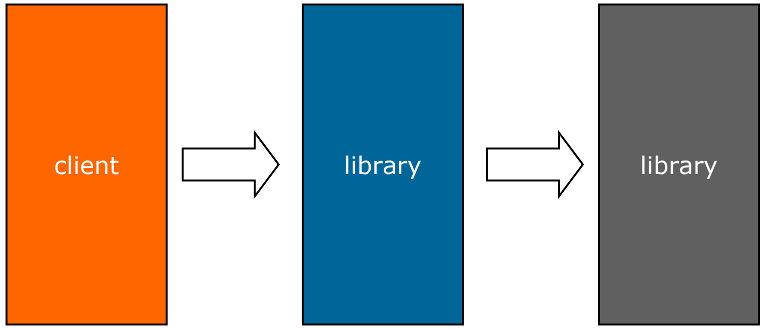
Explicit Linking

- Increase application portability
  - Library NOT found
  - Function is not found
  - Function signature is wrong
- Mechanism
  - LoadLibraryEx(...)
  - GetProcAddress(...)
  - Invoke function

Windows Dynamic-Link Libraries

Forwarded Library

- Delegate a call to another function of another library
- Mechanism



Windows Dynamic-Link Libraries

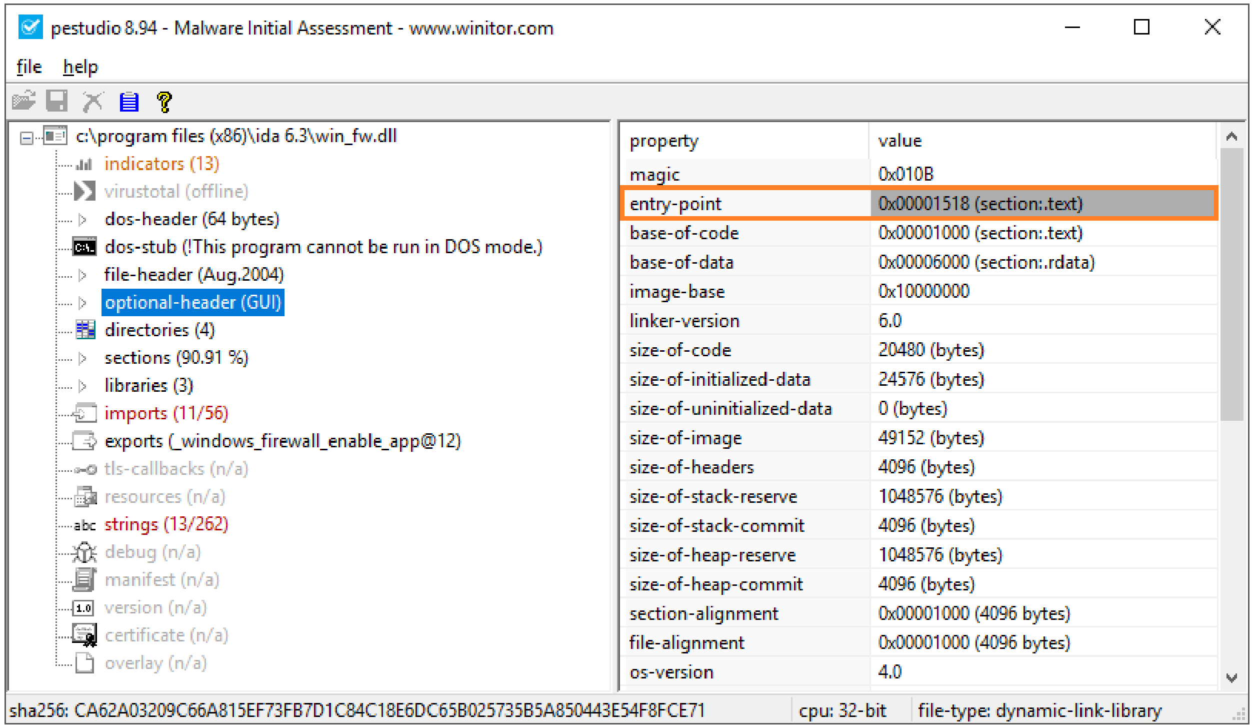
Delay Loaded Library

- Hybrid between implicit and explicit linking
- Reduce application loading time
- Avoid loading rarely used DLLs
- Declared during development

Windows Dynamic-Link Libraries

Entry Point

- Function implemented as a callback
  - Is optional...but often implemented
  - Is case sensitive
  - Is informational
  - Global initialization
  - TLS initialization



pestudio 8.94 - Malware Initial Assessment - www.winitor.com

file help

c:\program files (x86)\ida 6.3\win_fw.dll
- indicators (13)
- virustotal (offline)
- dos-header (64 bytes)
- dos-stub (!This program cannot be run in DOS mode.)
- file-header (Aug.2004)
- optional-header (GUI)
- directories (4)
- sections (90.91 %)
- libraries (3)
- imports (11/56)
- exports (_windows_firewall_enable_app@12)
- tls-callbacks (n/a)
- resources (n/a)
- strings (13/262)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

property	value
magic	0x010B
entry-point	0x00001518 (section:.text)
base-of-code	0x00001000 (section:.text)
base-of-data	0x00006000 (section:.rdata)
image-base	0x10000000
linker-version	6.0
size-of-code	20480 (bytes)
size-of-initialized-data	24576 (bytes)
size-of-uninitialized-data	0 (bytes)
size-of-image	49152 (bytes)
size-of-headers	4096 (bytes)
size-of-stack-reserve	1048576 (bytes)
size-of-stack-commit	4096 (bytes)
size-of-heap-reserve	1048576 (bytes)
size-of-heap-commit	4096 (bytes)
section-alignment	0x00001000 (4096 bytes)
file-alignment	0x00001000 (4096 bytes)
os-version	4.0

sha256: CA62A03209C66A815EF73FB7D1C84C18E6DC65B025735B5A850443E54F8FCE71 | cpu: 32-bit | file-type: dynamic-link-library

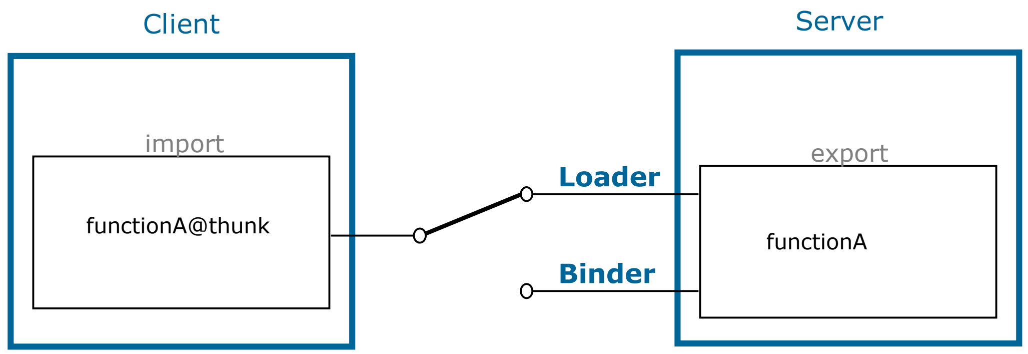
pestudio – www.winitor.com

Performance - Rebasing

- Every module has a preferred base address
- Addresses conflict when loading several components
- Used at the end of the build cycle

Performance - Binding

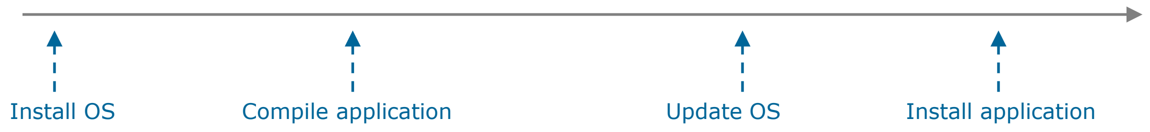
- Loader resolves the addresses of the imported symbols
- Bind the application during the installation process
- Application must have been previously rebased



Windows Dynamic-Link Libraries

Issues

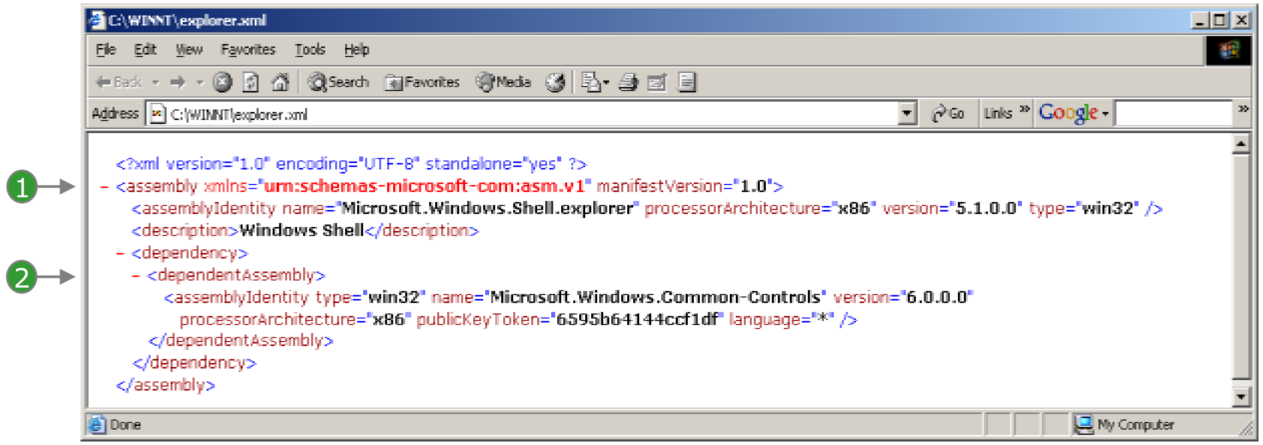
- Simple name-based dependencies
- Installing a product which overwrites a DLL file
- Solutions
  - WFP
  - Redirection
  - Known Directories
  - Known Libraries
  - WinSxS



Windows Dynamic-Link Libraries

Manifest

- Allow different versions of the same DLL to exist “side-by-side”
- Typtes
  - Extern
  - Intern
- Assemblies
  - Private
  - Shared

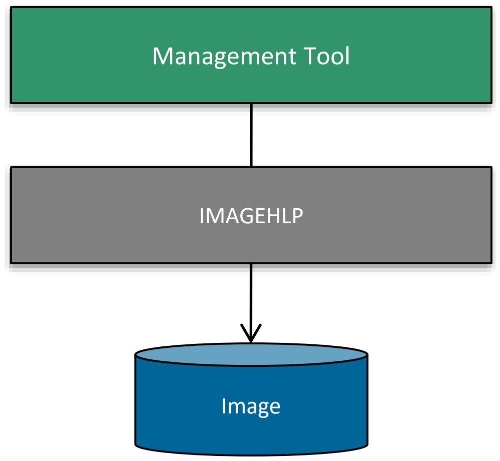

C:\WINNT\explorer.xml
File Edit View Favorites Tools Help
Back Search Favorites Media
Address C:\WINNT\explorer.xml
Go Links Google
1
2
Done
My Computer

```
  <?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
    <assemblyIdentity name="Microsoft.Windows.Shell.explorer" processorArchitecture="x86" version="5.1.0.0" type="win32" />
    <description>Windows Shell</description>
  - <dependency>
    - <dependentAssembly>
        <assemblyIdentity type="win32" name="Microsoft.Windows.Common-Controls" version="6.0.0.0"
          processorArchitecture="x86" publicKeyToken="6595b64144ccf1df" language="*" />
      </dependentAssembly>
    </dependency>
  </assembly>
```

Windows Dynamic-Link Libraries

Management

- Access the (some) parts of an image
  - Update the version
  - Manage the certificate
  - Edit the executable image



Windows Dynamic-Link Libraries

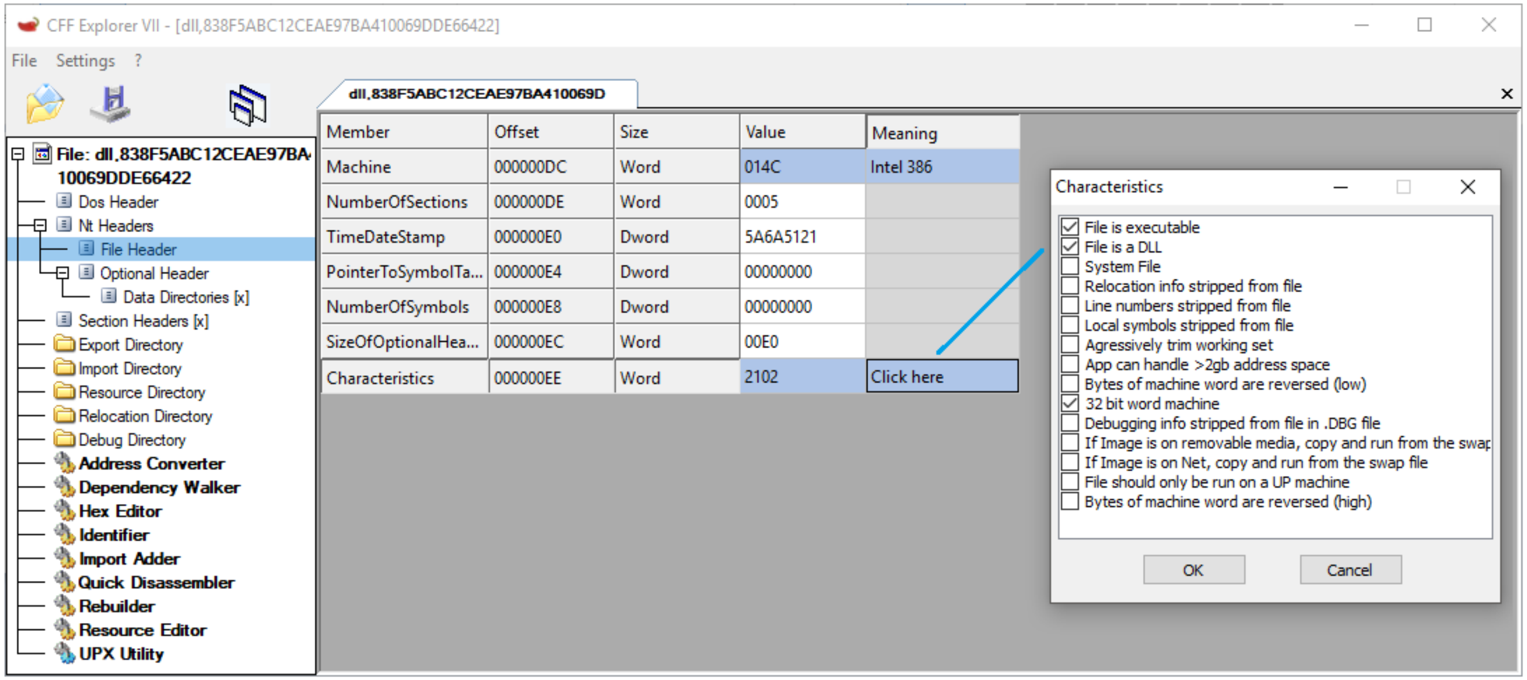
Difference between executable and DLL

- Executable vs. Dynamic-Link Library

Executable	DLL
IMAGE_FILE_EXECUTABLE (0x2)	IMAGE_FILE_DLL (0x2000)
Entry point is mandatory	Entry point is optional
Usually without exported functions	Often with exported functions
Code is mandatory	Code is optional
Can host and can be hosted	Must be hosted
Own separated address space	Shared address space
Unhandled exception crashes process	Unhandled exception crashes host

Convert a DLL into an Executable

- A DLL can be converted into an Executable (e.g. to ease debugging)
  - Modify PE Characteristic: IMAGE_FILE_EXECUTABLE > IMAGE_FILE_DLL
  - Modify the existing entry-point to an exported function



Member	Offset	Size	Value	Meaning
Machine	000000DC	Word	014C	Intel 386
NumberOfSections	000000DE	Word	0005	
TimeDateStamp	000000E0	Dword	5A6A5121	
PointerToSymbolTa...	000000E4	Dword	00000000	
NumberOfSymbols	000000E8	Dword	00000000	
SizeOfOptionalHea...	000000EC	Word	00E0	
Characteristics	000000EE	Word	2102	Click here

- [x] File is executable
- [x] File is a DLL
- [ ] System File
- [ ] Relocation info stripped from file
- [ ] Line numbers stripped from file
- [ ] Local symbols stripped from file
- [ ] Agressively trim working set
- [ ] App can handle >2gb address space
- [ ] Bytes of machine word are reversed (low)
- [x] 32 bit word machine
- [ ] Debugging info stripped from file in .DBG file
- [ ] If Image is on removable media, copy and run from the swap
- [ ] If Image is on Net, copy and run from the swap file
- [ ] File should only be run on a UP machine
- [ ] Bytes of machine word are reversed (high)

CFF Explorer – https://ntcore.com

Windows Dynamic-Link Libraries

References

- Dynamic-Link Library Entry-Point Function
  - https://docs.microsoft.com/en-us/windows/desktop/Dlls/dynamic-link-library-entry-point-function
- DllMain entry point
  - https://docs.microsoft.com/en-us/windows/desktop/Dlls/dllmain

Windows Dynamic-Link Libraries

Thank you

- Questions?