

Dynamic Link Library (DLL) *Rebase e Bind*

- *Jeffrey Richter, Christophe Nasarre, **Windows via C/C++**, Fifth Edition, Microsoft Press, 2008 [cap. 20]*

Rebase

Rebase – secção para realojamento de código - .reloc

```
C:\WINDOWS\system32\cmd.exe
D:\SOi\Debug>dumpbin -headers Random.dll
Microsoft (R) COFF/PE Dumper Version 7.10.3077
Copyright (C) Microsoft Corporation. All rights reserved.

...

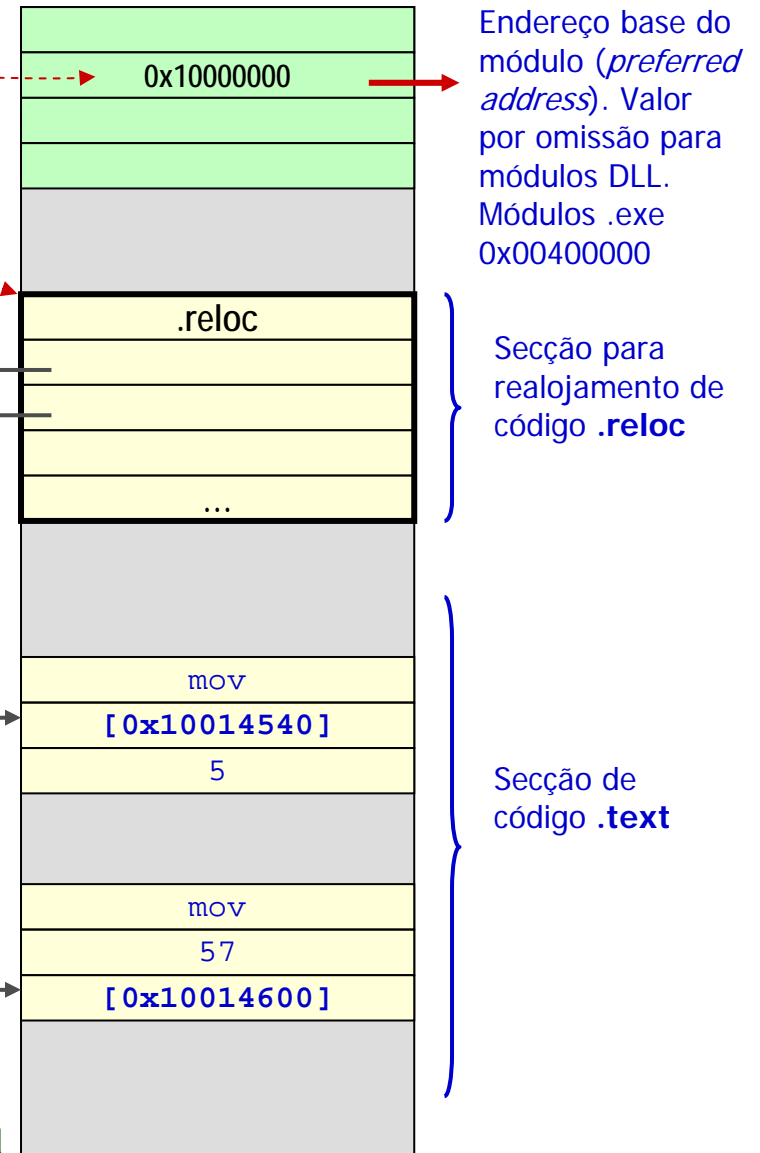
OPTIONAL HEADER VALUES
    10B magic # (PE32)
    7.10 linker version
   20000 size of code
    C000 size of initialized data
     0 size of uninitialized data
   11460 entry point (10011460)
    1000 base of code
    1000 base of data
  10000000 image base (10000000 to 1003CFFF)
    1000 section alignment
    1000 file alignment

...

SECTION HEADER #6
.reloc name
  1DC5 virtual size
  3B000 virtual address (1003B000 to 1003CDC4)
   2000 size of raw data
  29000 file pointer to raw data (00029000 to 0002AFFF)
    0 file pointer to relocation table
    0 file pointer to line numbers
    0 number of relocations
    0 number of line numbers
42000040 flags
  Initialized Data
  Discardable
  Read Only

Summary
   4000 .data
   1000 .idata
   5000 .rdata
   2000 .reloc
  20000 .text
```

Ficheiro
Random.dll



Rebase – Rebase da DLL Random.dll

O utilitário **rebase** vai proceder ao realojamento de todos os módulos indicados começando por atribuir como endereço base o indicado na opção **-b 0x<????>**

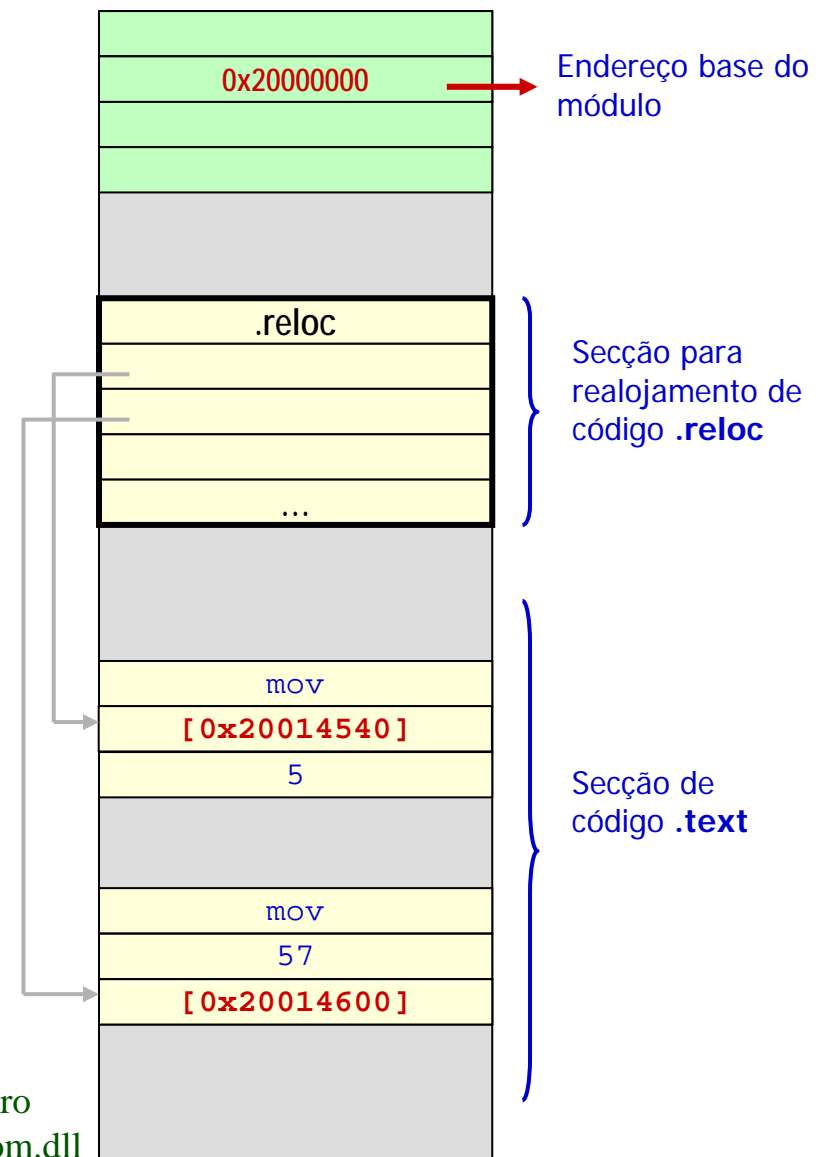
```
C:\WINDOWS\system32\cmd.exe
D:\SOi\Debug>rebase -b 0x20000000 Random.dll
REBASE: Total Size of mapping 0x0000000000040000
REBASE: Range 0x0000000020000000 -0x0000000020040000
D:\SOi\Debug>
```

Neste exemplo vai apenas alterar o módulo **Random.dll** de forma a que o seu endereço base se altere para **0x20000000**. Assim executa os seguintes passos:

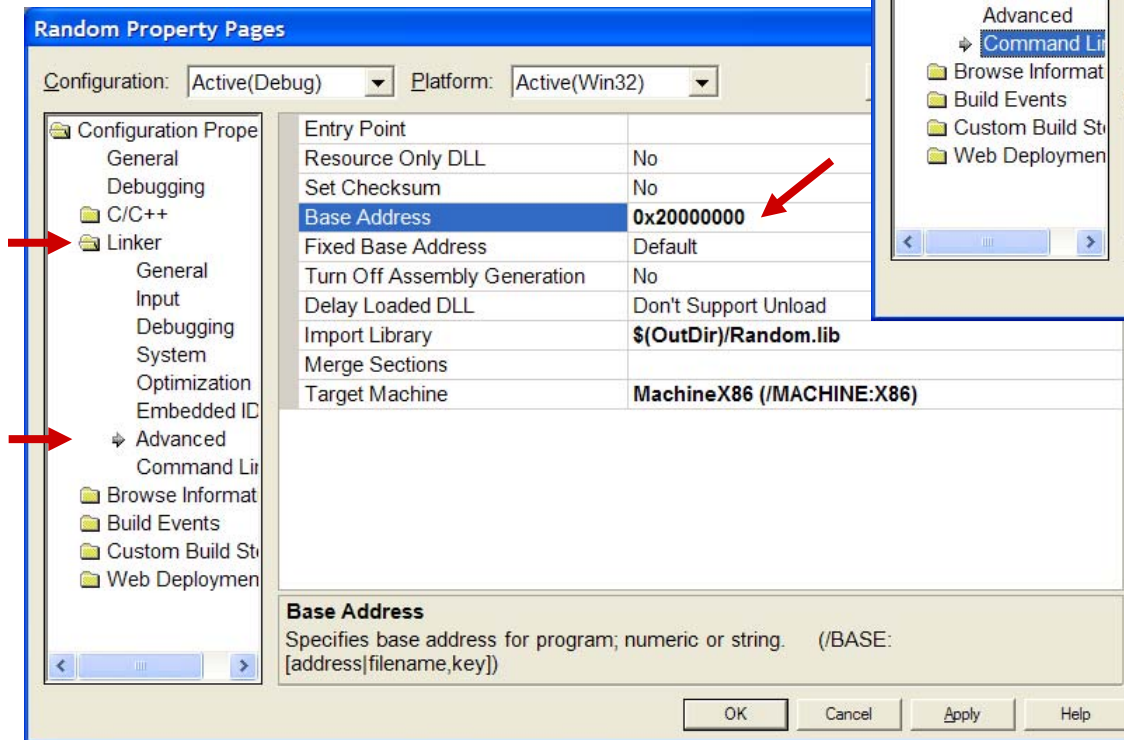
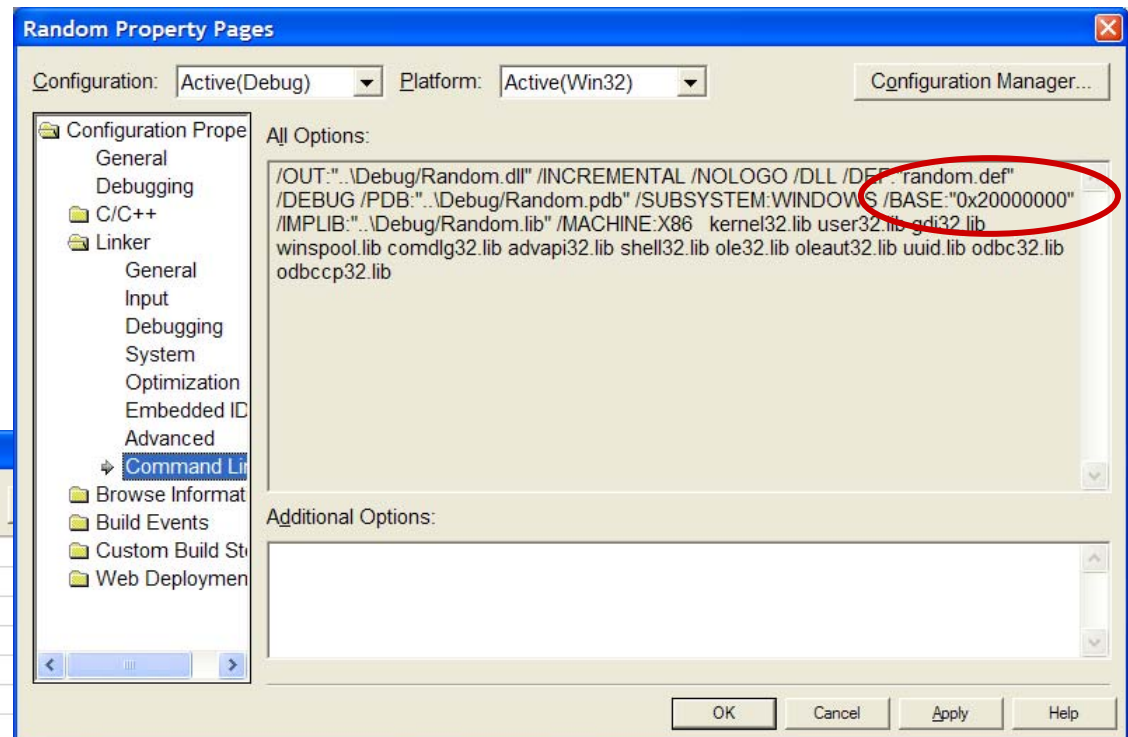
- Determina o endereço base existente no módulo e determina a diferença para o novo
- Altera endereço base do módulo
- Itera sobre a tabela de endereços da secção .reloc e adiciona essa diferença ao endereço guardado

diferença
0x10000000

Ficheiro
Random.dll



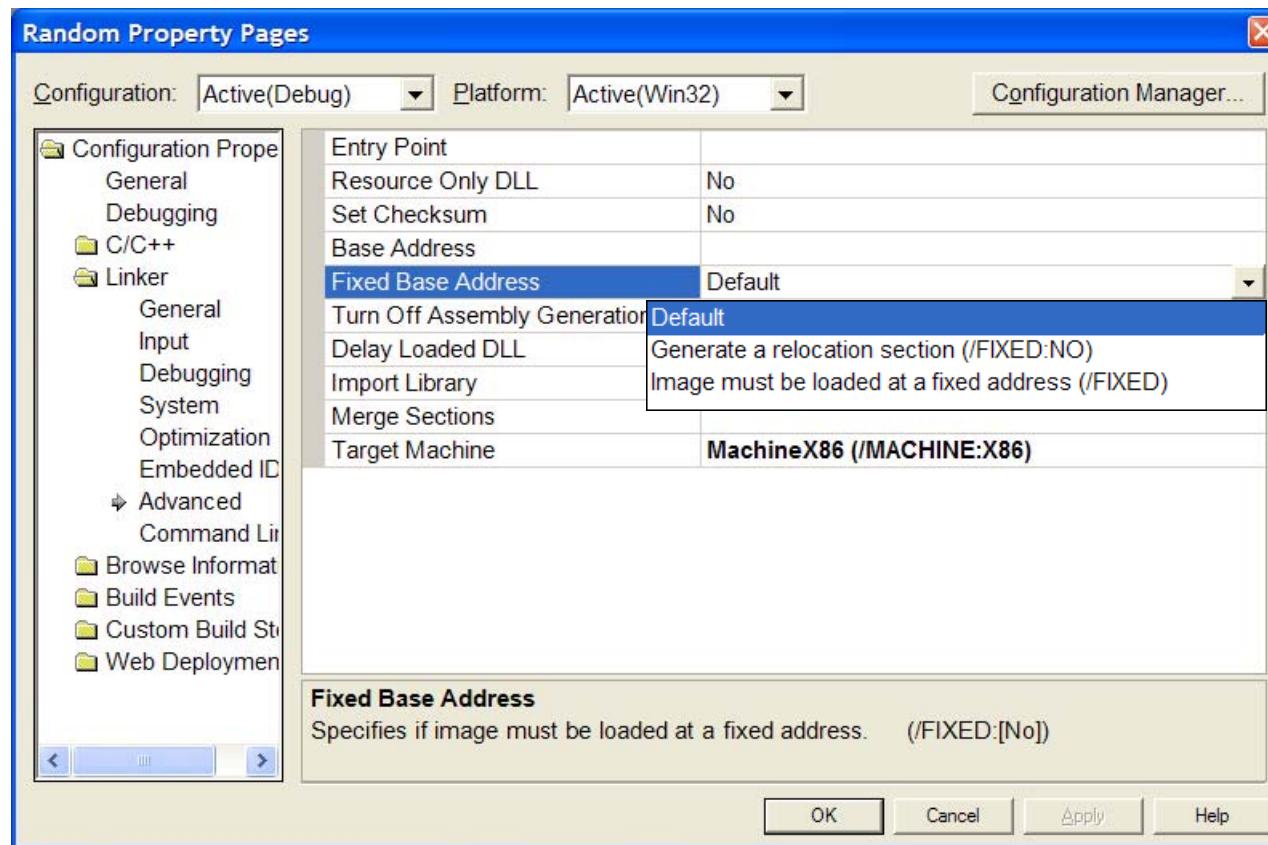
Rebase – Definição do endereço base no Visual Studio



Rebase – Excluir a secção de realojamento de código da DLL

Existe a possibilidade de excluir a secção de realojamento de código da DLL através do **switch /FIXED** do linker. Neste caso o módulo só pode ser carregado no seu endereço base.

A imagem apresenta como pode ser definido este *switch* no Visual Studio.



Rebase – Rebase das DLL's Random.dll e Quadrado.dll

```
C:\WINDOWS\system32\cmd.exe

D:\SOi\Debug>rebase -b 0x16000000 Random.dll Quadrado.dll

REBASE: Total Size of mapping 0x0000000000070000
REBASE: Range 0x0000000016000000 -0x0000000016070000

D:\SOi\Debug>
```

```
C:\WINDOWS\system32\cmd.exe

D:\SOi\Debug>dumpbin -headers Random.dll
Microsoft (R) COFF/PE Dumper Version 7.10.3077
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file Random.dll

PE signature found

File Type: DLL
```

OPTIONAL HEADER VALUES

10B	magic # (PE32)
7.10	linker version
20000	size of code
C000	size of initialized data
0	size of uninitialized data
11460	entry point (16011460)
1000	base of code
1000	base of data
16000000	image base (16000000 to 1603CFFF)
1000	section alignment
1000	file alignment
4.00	operating system version
0.00	image version
4.00	subsystem version
0	Win32 version
30000	size of image

```
C:\WINDOWS\system32\cmd.exe

D:\SOi\Debug>dumpbin -headers Quadrado.dll
Microsoft (R) COFF/PE Dumper Version 7.10.3077
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file Quadrado.dll

PE signature found

File Type: DLL
```

OPTIONAL HEADER VALUES

10B	magic # (PE32)
7.10	linker version
13000	size of code
A000	size of initialized data
0	size of uninitialized data
112F3	entry point (160512F3)
1000	base of code
1000	base of data
16040000	image base (16040000 to 1606DFFF)
1000	section alignment
1000	file alignment
4.00	operating system version
0.00	image version
4.00	subsystem version
0	Win32 version
2F000	size of image

Rebase – Função da API

```
BOOL ReBaseImage(  
    __in    PCSTR CurrentImageName,  
    __in    PCSTR SymbolPath,  
    __in    BOOL fReBase,  
    __in    BOOL fRebaseSysfileOk,  
    __in    BOOL fGoingDown,  
    __in    ULONG CheckImageSize,  
    __out   ULONG* OldImageSize,  
    __out   ULONG_PTR* OldImageBase,  
    __out   ULONG* NewImageSize,  
    __in_out ULONG_PTR* NewImageBase,  
    __in    ULONG TimeStamp  
);
```


Bind

Bind – Estrutura da secção de *import* de um módulo

```
C:\WINDOWS\system32\cmd.exe
D:\SOi\Debug>dumpbin -imports AppRandESquare.exe
Microsoft (R) COFF/PE Dumper Version 7.10.3077
Copyright (C) Microsoft Corporation. All rights reserved.

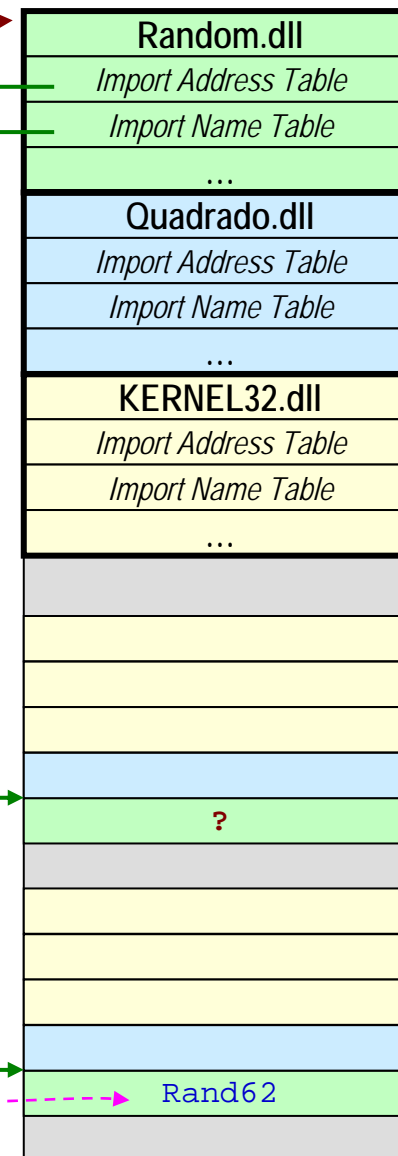
Dump of file AppRandESquare.exe
File Type: EXECUTABLE IMAGE

Section contains the following imports:

  Random.dll
    42C390 Import Address Table
    42C1D8 Import Name Table
    0 time date stamp
    0 Index of first forwarder reference
    0 Rand62

  Quadrado.dll
    42C360 Import Address Table
    42C1A8 Import Name Table
    0 time date stamp
    0 Index of first forwarder reference
    0 quadrado

  KERNEL32.dll
    42C208 Import Address Table
    42C050 Import Name Table
    0 time date stamp
    0 Index of first forwarder reference
    20A HeapDestroy
    16C GetLocaleInfoA
```



Secção
Import de um
Módulo
binário (por
exemplo um
.EXE)

*Import
Address
Tables*

*Import
Name
Tables*

Bind – Estrutura da secção de *import* de um módulo

```
C:\WINDOWS\system32\cmd.exe
D:\SOi\Debug>dumpbin -imports AppRandESquare.exe
Microsoft (R) COFF/PE Dumper Version 7.10.3077
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file AppRandESquare.exe
File Type: EXECUTABLE IMAGE

Section contains the following imports:

  Random.dll
    42C390 Import Address Table
    42C1D8 Import Name Table
    0 time date stamp
    0 Index of first forwarder reference

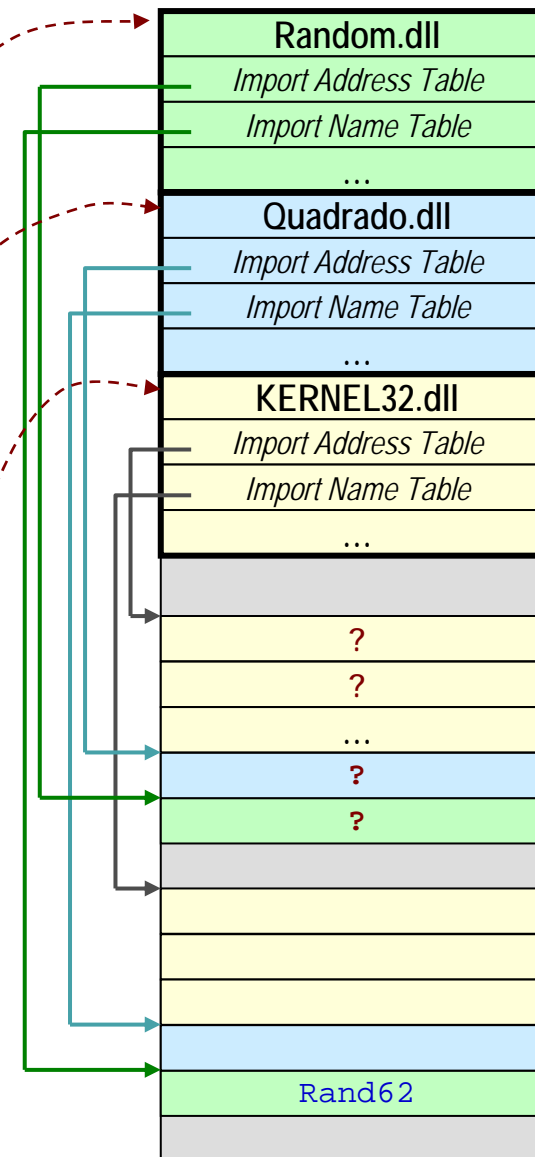
    0 Rand62

  Quadrado.dll
    42C360 Import Address Table
    42C1A8 Import Name Table
    0 time date stamp
    0 Index of first forwarder reference

    0 quadrado

  KERNEL32.dll
    42C208 Import Address Table
    42C050 Import Name Table
    0 time date stamp
    0 Index of first forwarder reference

    20A HeapDestroy
    16C GetLocaleInfoA
```

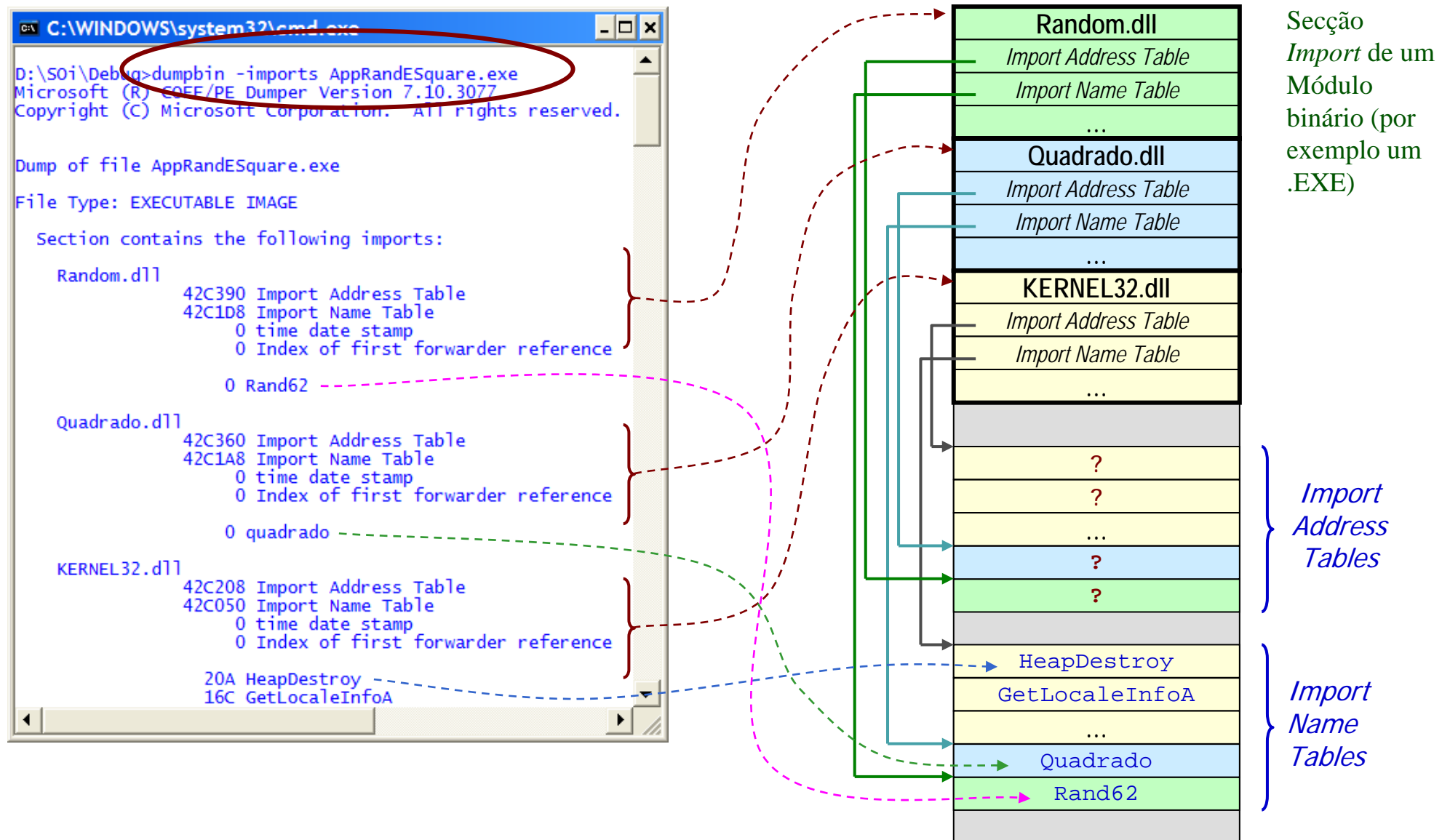


Secção
Import de um
Módulo
binário (por
exemplo um
.EXE)

*Import
Address
Tables*

*Import
Name
Tables*

Bind – Estrutura da secção de *import* de um módulo



Bind – Diferenças na secção de Imports após realizado o bind

```
C:\WINDOWS\system32\cmd.exe

D:\SOi\Debug>dumpbin -imports AppRandESquare.exe
Microsoft (R) COFF/PE Dumper Version 7.10.3077
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file AppRandESquare.exe
File Type: EXECUTABLE IMAGE

Section contains the following imports:

Random.dll
  42C390 Import Address Table
  42C1D8 Import Name Table
  0 time date stamp
  0 Index of first forwarder reference

  0 Rand62

Quadrado.dll
  42C360 Import Address Table
  42C1A8 Import Name Table
  0 time date stamp
  0 Index of first forwarder reference

  0 quadrado

KERNEL32.dll
  42C208 Import Address Table
  42C050 Import Name Table
  0 time date stamp
  0 Index of first forwarder reference

  20A HeapDestroy
  16C GetLocaleInfoA
```

**Secção de imports
antes do bind**

```
C:\WINDOWS\system32\cmd.exe

D:\SOi\Debug>bind
usage: BIND [switches] image-names...
[-?] display this message
[-c] no caching of import dlls
[-o] disable new import descriptors
[-p dll search path]
[-s Symbol directory] update any associated .DBG file
[-u] update the image
[-v] verbose output
[-x image name] exclude this image from binding
[-y] allow binding on images located above 2G

D:\SOi\Debug>bind -u AppRandESquare.exe
```

**bind do módulo
AppRandESquare.exe**

```
C:\WINDOWS\system32\cmd.exe

D:\SOi\Debug>dumpbin -imports AppRandESquare.exe
Microsoft (R) COFF/PE Dumper Version 7.10.3077
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file AppRandESquare.exe
File Type: EXECUTABLE IMAGE

Section contains the following imports:

Random.dll
  42C390 Import Address Table
  42C1D8 Import Name Table
  FFFFFFFF time date stamp
  FFFFFFFF Index of first forwarder reference

  160110E6 0 Rand62

Quadrado.dll
  42C360 Import Address Table
  42C1A8 Import Name Table
  FFFFFFFF time date stamp
  FFFFFFFF Index of first forwarder reference

  1605105F 0 quadrado

KERNEL32.dll
  42C208 Import Address Table
  42C050 Import Name Table
  FFFFFFFF time date stamp
  FFFFFFFF Index of first forwarder reference

  7C811110 20A HeapDestroy
  7C80D47E 16C GetLocaleInfoA
```

**Secção de imports
depois do bind**

Bind – Como se obtém o novo valor associado a cada função

Da secção de *exports* do módulo Random.dll podemos encontrar o **RVA** (*Relative Virtual Address*) da função Rand62 que indica o offset da função no módulo DLL

```
C:\WINDOWS\system32\cmd.exe
Microsoft (R) COFF/PE Dumper Version 7.10.3077
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file Random.dll
File Type: DLL

Section contains the following exports for Random.dll

00000000 characteristics
441872BD time date stamp Wed Mar 15 20:02:05 2006
0.00 version
1 ordinal base
1 number of functions
1 number of names

ordinal hint RVA      name
1      0 000110E6 Rand62
```

> **dumpbin –headers Random.dll** podemos verificar o endereço base do módulo

```
OPTIONAL HEADER VALUES
10B magic # (PE32)
7.10 linker version
20000 size of code
C000 size of initialized data
0 size of uninitialized data
11460 entry point (16011460)
1000 base of code
1000 base of data
16000000 image base (16000000 to 1603CFFF)
1000 section alignment
1000 file alignment
```

```
C:\WINDOWS\system32\cmd.exe
D:\SOI\Debug>dumpbin -imports AppRandESquare.exe
Microsoft (R) COFF/PE Dumper Version 7.10.3077
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file AppRandESquare.exe
File Type: EXECUTABLE IMAGE

Section contains the following imports:

Random.dll
42C390 Import Address Table
42C1D8 Import Name Table
FFFFFFFF time date stamp
FFFFFFFF Index of first forwarder reference

160110E6 0 Rand62

Quadrado.dll
42C360 Import Address Table
42C1A8 Import Name Table
FFFFFFFF time date stamp
FFFFFFFF Index of first forwarder reference

1605105F 0 quadrado

KERNEL32.dll
42C208 Import Address Table
42C050 Import Name Table
FFFFFFFF time date stamp
FFFFFFFF Index of first forwarder reference

7C811110 20A HeapDestroy
7C80D47E 16C GetLocaleInfoA
```



Bind – Cada módulo contém nos seus *headers* informação sobre os *binds*

C:\WINDOWS\system32\cmd.exe

```
D:\SOi\Debug>dumpbin -headers Random.dll
Microsoft (R) COFF/PE Dumper Version 7.10.3077
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file Random.dll

PE signature found

File Type: DLL

FILE HEADER VALUES
 14C machine (x86)
 6 number of sections
 441872BD time date stamp Wed Mar 15 20:02:05 2006
 0 file pointer to symbol table
 0 number of symbols
 E0 size of optional header
 210E characteristics
    Executable
    Line numbers stripped
```

C:\WINDOWS\system32\cmd.exe

```
Header contains the following bound import information:
Bound to Random.dll [44186E3B] Wed Mar 15 19:42:51 2006
Bound to Quadrado.dll [44186E3B] Wed Mar 15 19:42:51 2006
Bound to KERNEL32.dll [411096B4] Wed Aug 04 08:56:36 2004
    Contained forwarders bound to NTDLL.DLL [411096B4] Wed Aug 04 08:56:36 2004

Summary
 4000 .data
 1000 .idata
 3000 .rdata
14000 .text
10000 .textbss
```

No final do dumpbin -imports
AppRandESquare.exe aparece a
informação sobre as DLL's que se
encontram bind

C:\WINDOWS\system32\cmd.exe

```
D:\SOi\Debug>dumpbin -headers Quadrado.dll
Microsoft (R) COFF/PE Dumper Version 7.10.3077
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file Quadrado.dll

PE signature found

File Type: DLL

FILE HEADER VALUES
 14C machine (x86)
 6 number of sections
 441872BB time date stamp Wed Mar 15 20:02:03 2006
 0 file pointer to symbol table
 0 number of symbols
 E0 size of optional header
 210E characteristics
    Executable
    Line numbers stripped
```

C:\WINDOWS\system32\cmd.exe

```
C:\WINDOWS\system32>dumpbin -headers kernel32.dll
Microsoft (R) COFF/PE Dumper Version 7.10.3077
Copyright (C) Microsoft Corporation. All rights reserved.

Dump of file kernel32.dll

PE signature found

File Type: DLL

FILE HEADER VALUES
 14C machine (x86)
 4 number of sections
 411096B4 time date stamp Wed Aug 04 08:56:36 2004
 0 file pointer to symbol table
 0 number of symbols
 E0 size of optional header
 210E characteristics
    Executable
    Line numbers stripped
```

Bind – Função da API

```
BOOL BindImageEx(  
    __in    DWORD Flags,  
    __in    PSTR ImageName,  
    __in    PSTR DllPath,  
    __in    PSTR SymbolPath,  
    __in    PIMAGEHLP_STATUS_ROUTINE StatusRoutine  
);
```