a bit more of

PE

(since Hashdays)

Hack In Paris

Ange Albertini

22th June 2012

Author

- reverse engineer
  - since dos 3.21
- ashamed by a malware
- back to my studies
  - shared on my site

http://CORKAMI.com

Fact → PoC

made with love

- Hand-made, from scratch
  - ~~patched~~ ~~generated~~ ~~compiled~~
  - tedious
    - full control
- Pin-pointed
- Crystal clear
- Clean

```
code = "".join([
    GETSTATIC, struct.pack(">H", 16),
    LDC, struct.pack(">B", 18),
    INVOKEVIRTUAL, struct.pack(">H", 23)
    RETURN,
    ])

attribute_code = "".join([
struct.pack(">H", 7), # code
u4length("".join([
    struct.pack(">H
    struct.pack(">H
    u4length(code),
```

```
demo java

D>java HelloWorld
Hello World !
```

```
istruc IMAGE_DOS_HEADER
    at IMAGE_DOS_HEADER.e_magic, db 'ZM'
;   at IMAGE_DOS_HEADER.e_cblp, db LAST_BYTE    ; not re
    at IMAGE_DOS_HEADER.e_cp, dw PAGES
    at IMAGE_DOS_HEADER.e_cparhdr, dw dos_stub >> 4

; code start must be paragraph-aligned
align 10h, db 0
dos_stub:
    push    cs
    pop     ds
```

```
demoZM

D>dosZMXP.exe
 * EXE with ZM signature
```

File Edit View Window Help

Hello World!

helloworld-X - Notepad

File Edit Format View Help

```
%PDF-1.
1 0 obj<</Kids[<</Parent 1 0 R/Contents[2 0 R]>>]/Resources<<>>>>
2 0 obj<<>>
streamBT/default 99 Tf 1 0 0 1 1 715 Tm(Hello World!)Tj ET
endstream
endobj
trailer<</Root<</Pages 1 0 R>>>>
```

technical

be nice to your friends

- ~~ads~~ ~~log-in~~ ~~pay-wall~~ ~~columns~~
- *BSD*/*CC BY* licence
  - reusable commercially
- free sources, using free tools
  - reviews, comments, ***suggestions***
- free binaries
  - downloadable in one click
- free documents
  - including all the graphics

free

goals

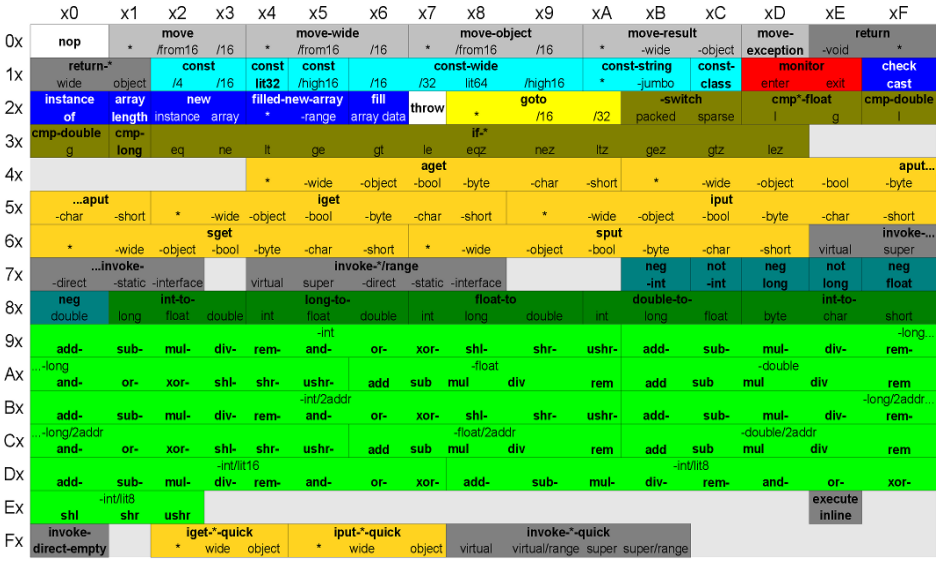
- ~~advertisement~~
  - for ***my*** own use
- a good reference
  - learn. remember. teach.
- a meaningful test set
  - failed all tools
  - clean

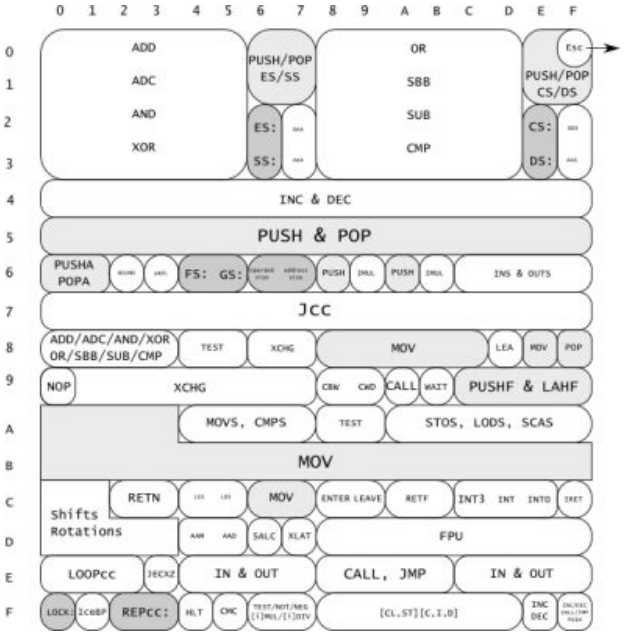
enough

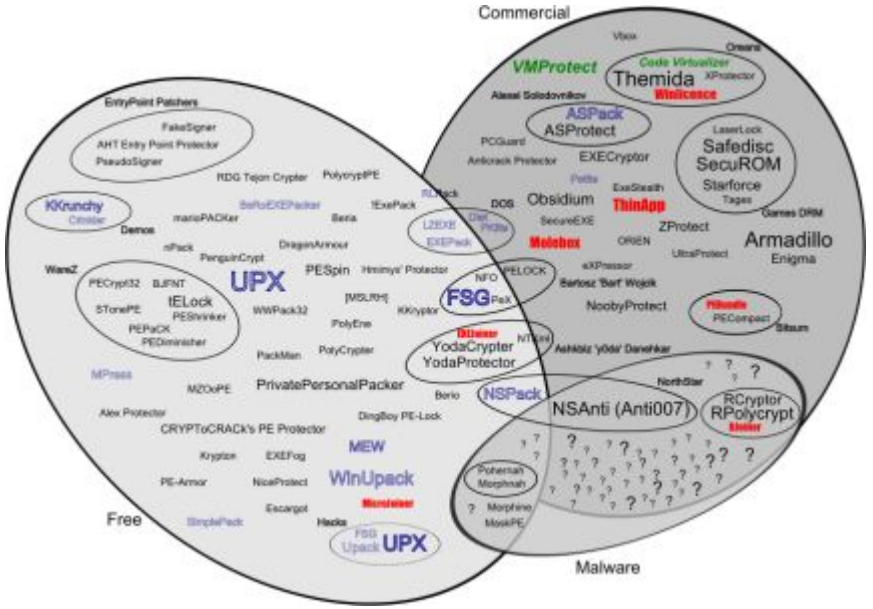
PoCs → Wiki Page

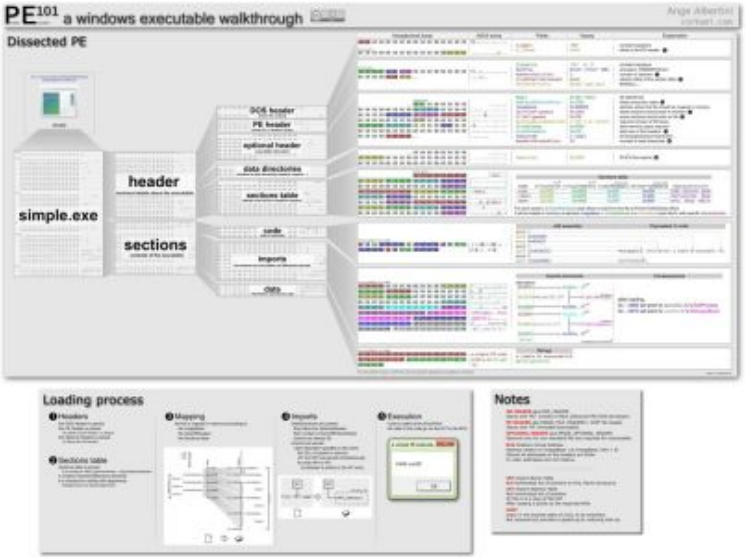
→ presentation

a graphic is worth 1000 lines of doc









useful

Ange ↔ Corkami

technical

free

useful

Agenda

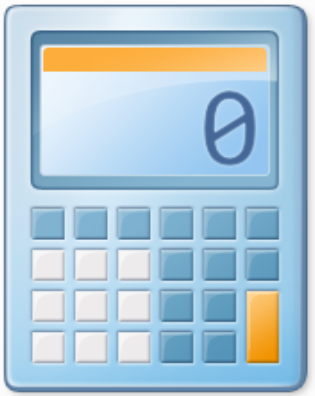
1. What's a PE?
   - yet another doc?
2. Static oddities
3. Dynamic oddities

Introduction

Portable Executable

Common Object File Format

AcroRd32



calc

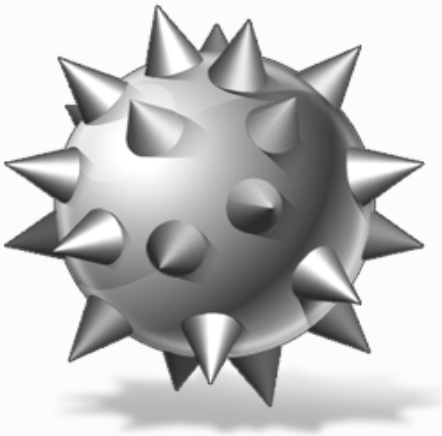
chrome

cmd

explorer

firefox

iexplore

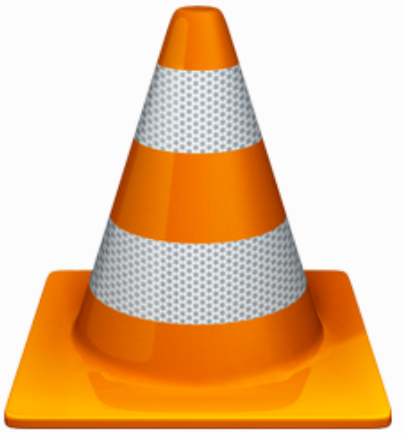


MineSweeper

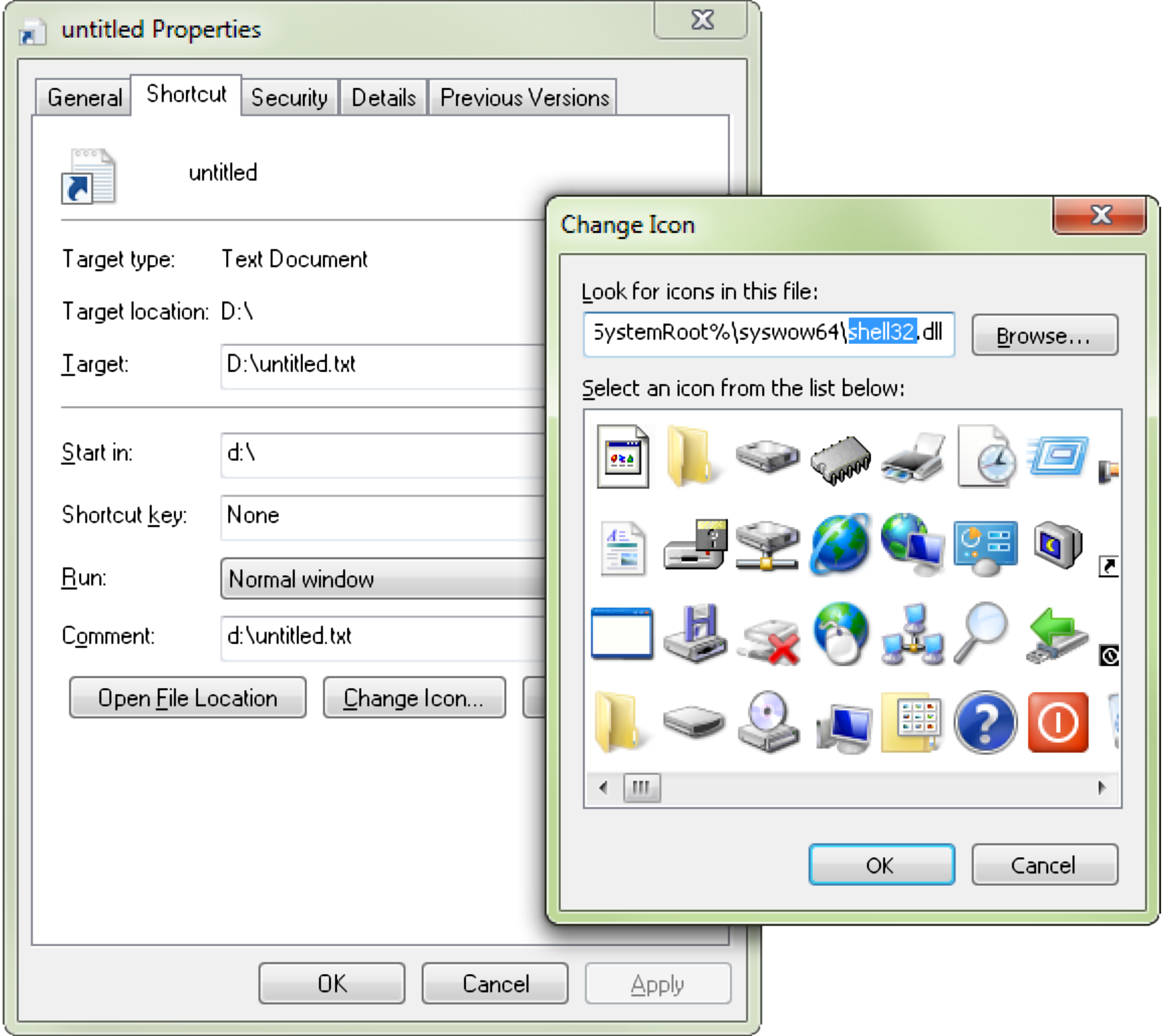
mspaint

notepad

Solitaire



vlc


untitled Properties
General
Shortcut
Security
Details
Previous Versions
untitled
Target type: Text Document
Target location: D:\
Target: D:\untitled.txt
Start in: d:\
Shortcut key: None
Run: Normal window
Comment: d:\untitled.txt
Open File Location
Change Icon...
OK
Cancel
Apply
Change Icon
Look for icons in this file:
%SystemRoot%\syswow64\shell32.dll
Browse...
Select an icon from the list below:
OK
Cancel

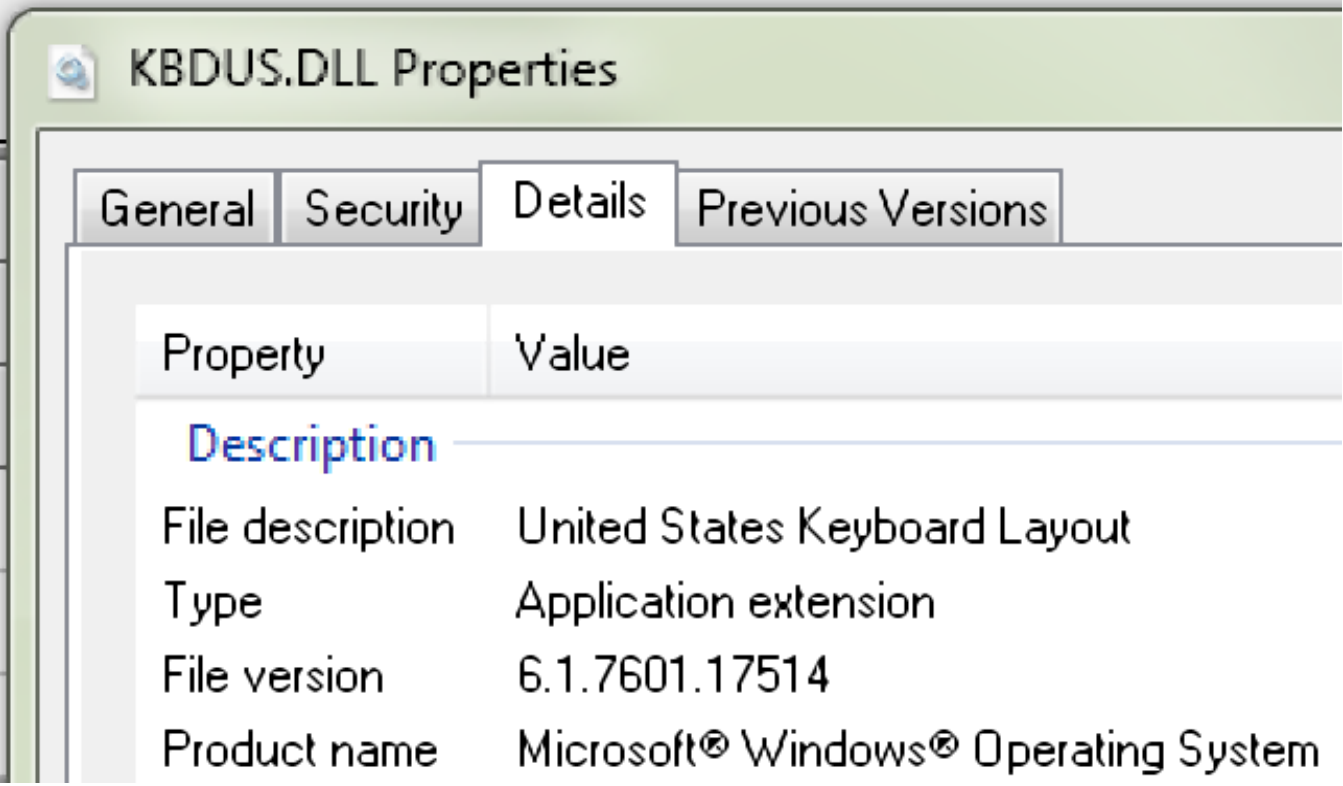
Sections

name	va	vsize	raw size	flags
.rsrc	0x1000	0x6000	0x5400	R-- IDATA

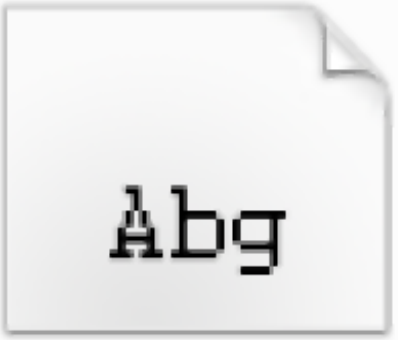
id	lang	string
300	1033	Access letters, reports, notes, and other kinds of documents.
301	1033	Displays recently opened documents and folders.
302	1033	Play music and other audio files.
303	1033	View and organize digital pictures.
304	1033	See the disk drives and other hardware connected to your computer.
305	1033	Access libraries and folders shared by other people in your homegroup.
307	1033	Change settings and customize the functionality of your computer.
312	1033	Play and manage games on your computer.
316	1033	Choose default programs for web browsing, e-mail, playing music, and other activities.
317	1033	Open your personal folder.
318	1033	See the available wireless networks, dial-up, and VPN connections that you can connect to.
319	1033	See installed printers and add new ones.
320	1033	Pinned
321	1033	Frequently used programs
322	1033	Use tab to move between sections, including the first and second panes and the power buttons.
323	1033	Pin %s
324	1033	Unpin %s
325	1033	Launch Windows Security Options to Change Password, Switch User, or Start Task Manager.
326	1033	Pinned
327	1033	Recent
328	1033	Frequent
329	1033	Tasks
330	1033	&Unpin from this list
331	1033	P&in to this list
332	1033	Unpin from Start menu
333	1033	Pin to Start menu
334	1033	Show recent or related items for %s
335	1033	Show recent or related items.
336	1033	Hide recent or related items for %s
337	1033	Hide recent or related items.
338	1033	Pin this program to taskbar
339	1033	Unpin this program from taskbar
340	1033	Location: %s (%s)
341	1033	Open

KBDUS.DLL

Name	Virtual Size
Byte[8]	Dword
.data	00000EC0
.rsrc	00000408
.reloc	000000BE



8514oem



coure

Dina

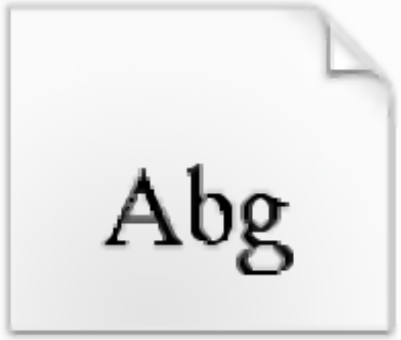
dosapp

modern

PalmOS-CP1252

roman

script



serife

smalle

vgafix

vgasys

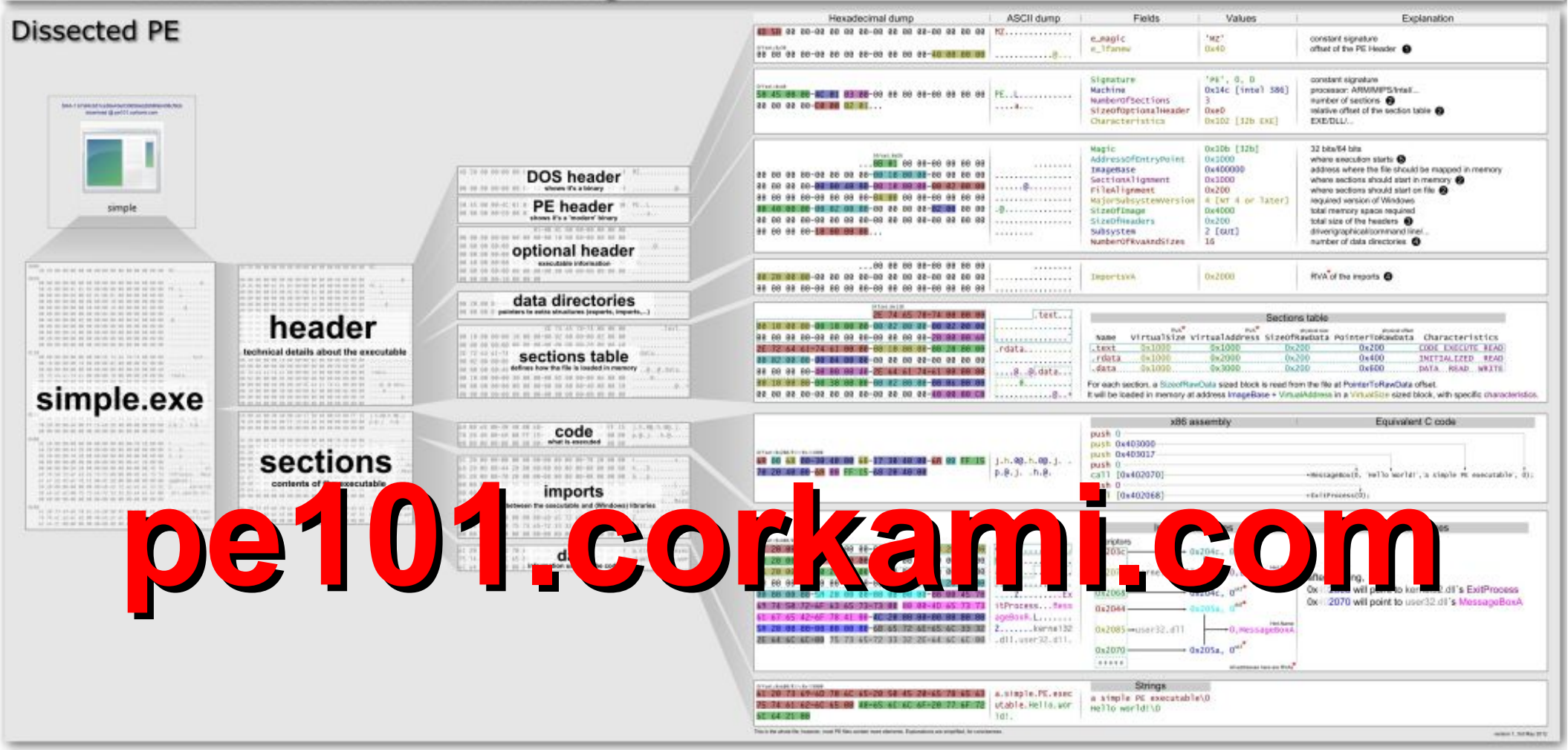
PE

universal windows binary

PE101 a windows executable walkthrough

Ange Albertini
corkami.com

Dissected PE



Loading process

❶ Headers

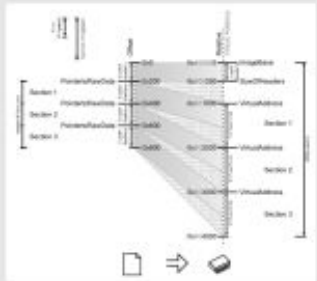
the *DOS Header* is parsed
the PE Header is parsed
(its offset is DOS Header's e_lfanew)
the Optional Header is parsed
(it follows the PE Header)

❷ Sections table

Sections table is parsed
(it is located at offset (*OptionalHeader*) + *SizeOfOptionalHeader*)
it contains *NumberOfSections* elements
it is checked for validity with alignments
FileAlignments and *SectionAlignments*

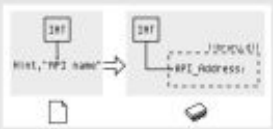
❸ Mapping

the file is mapped in memory according to:
the *ImageBase*
the *SizeOfHeaders*
the Sections table



❹ Imports

DataDirectories are parsed
they follow the OptionalHeader
their number is *NumOfRVAAndSizes*
imports are always #2
imports are parsed
each descriptor specifies a *DLLname*
this DLL is loaded in memory
IAT and *INT* are parsed simultaneously
for each API in *INT*
its address is written in the IAT entry



❺ Execution

Code is called at the *EntryPoint*
the calls of the code go via the IAT to the APIs

Notes

MZ HEADER aka DOS_HEADER
Starts with 'MZ' (initials of *Mark Zbikowski* MS-DOS developer)

PE HEADER aka IMAGE_FILE_HEADERS / COFF file header
Starts with 'PE' (Portable Executable)

OPTIONAL HEADER aka IMAGE_OPTIONAL_HEADER
Optional only for non-standard PEs but required for executables

RVA Relative Virtual Address
Address relative to ImageBase (at ImageBase, RVA = 0)
Almost all addresses of the headers are RVAs
In code, addresses are *not* relative.

INT Import Name Table
Null-terminated list of pointers to Hint, Name structures

IAT Import Address Table
Null-terminated list of pointers
On file it is a copy of the INT
After loading it points to the imported APIs

HINT
Index in the exports table of a DLL to be imported
Not required but provides a speed-up by reducing look-up

questions?


FASTEN YOUR
SEATBELTS

PointerToSymbolTable/NumberOfSymbols

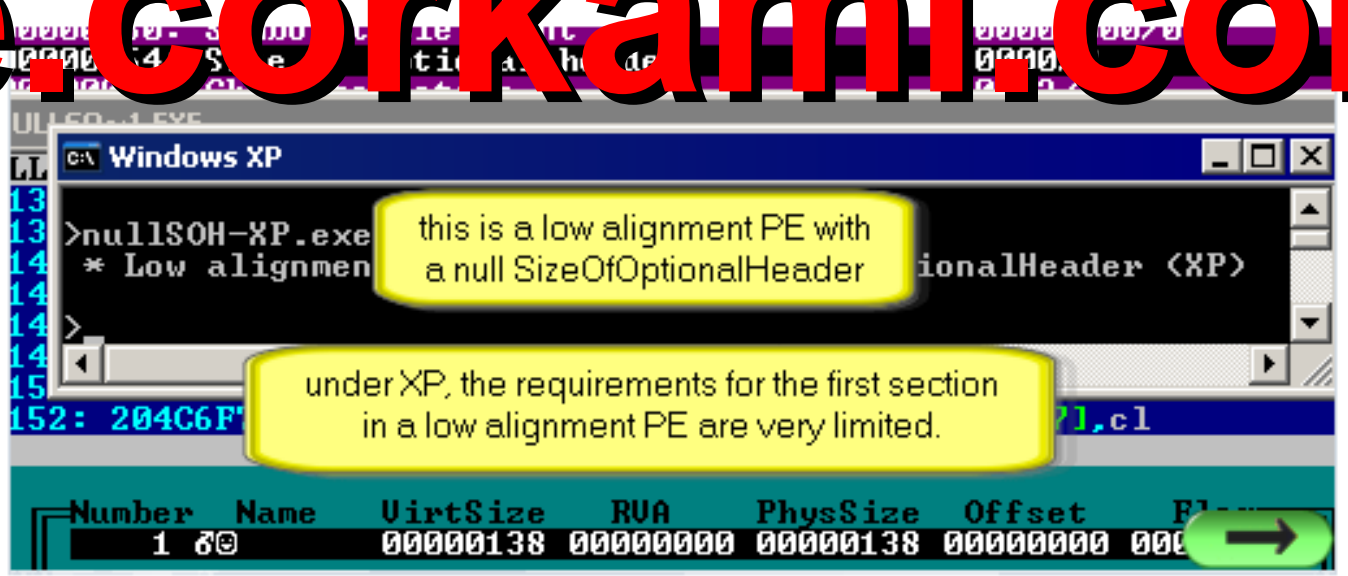
no importance whatsoever for the loader

SizeOfOptionalHeader

- is not the size of the optional header, but the delta between the top of the Optional header and the sta

  Thus, it can be null (the section table will overlap the Optional Header, or can be null when no sectior negative.

  - nullSOH-XP is a PE with a n SizeOfHeaders. the section table is thus overlapping the optio




```
...
SECTIONALIGN equ 4
FILEALIGN equ 4
...
OptionalHeader:
```

incomplete

specs

vs.

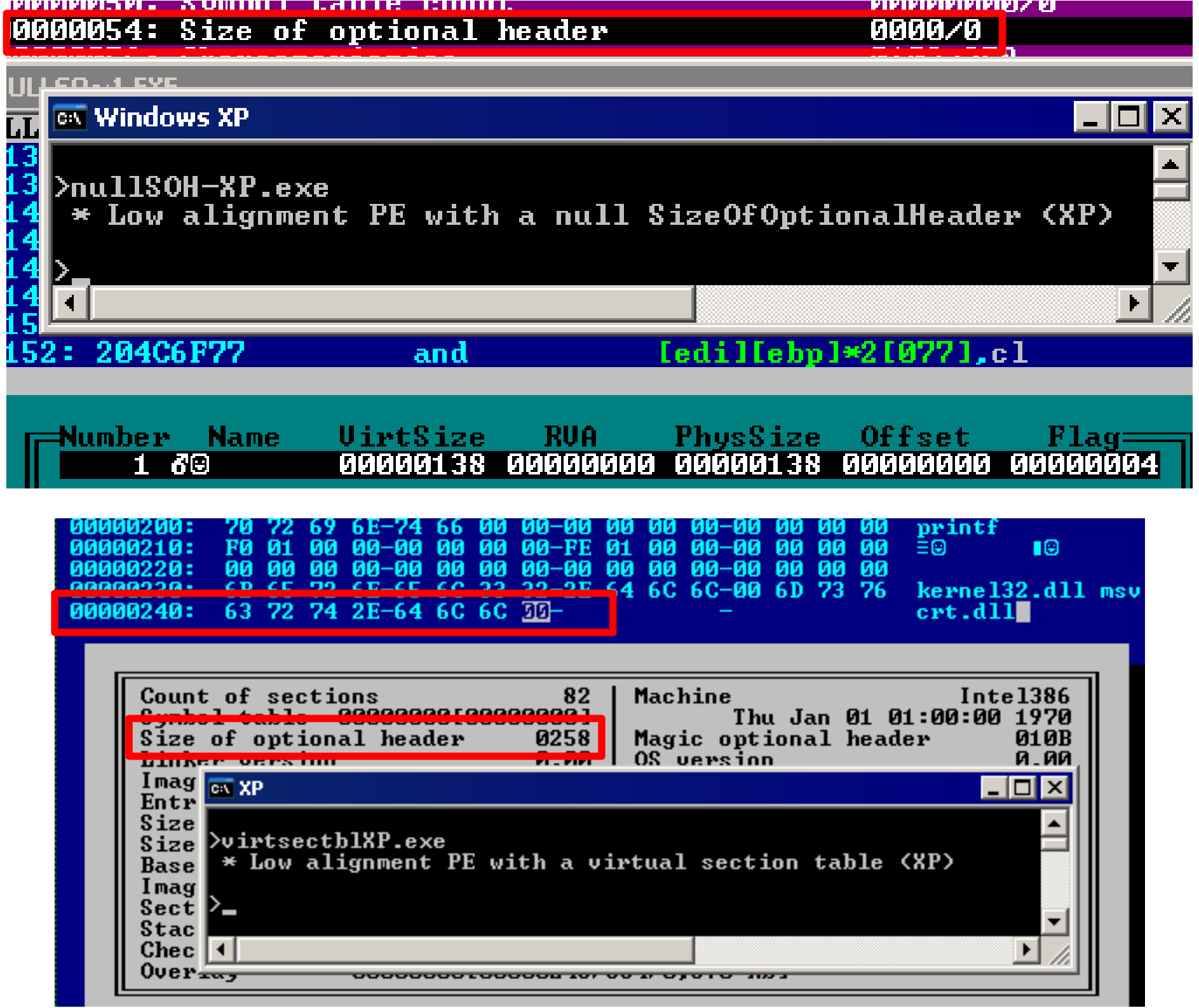
reality of the

OS

Microsoft Portable Executable and Common Object File Format Specification

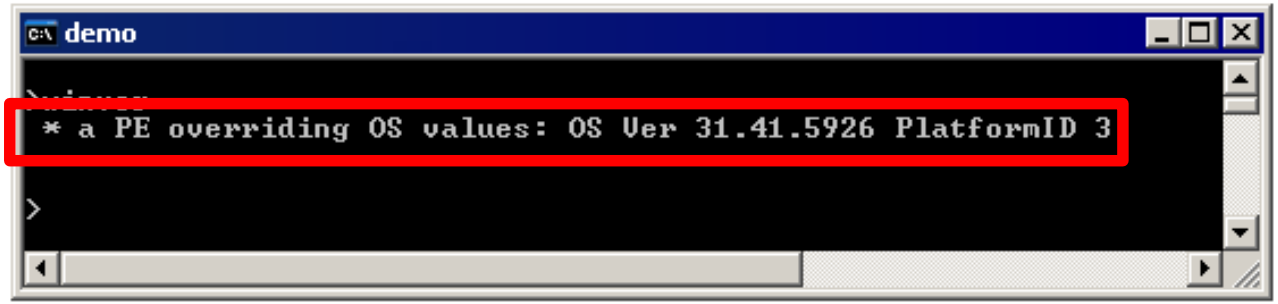
Revision 8.2 – September 21, 2010

SizeOfOptionalHeader	The size of the optional header, which is required for executable files but not for object files. This value should be zero for an object file. For a description of the header format, see section 3.4, “Optional Header (Image Only).”
Win32VersionValue	Reserved, must be zero.


00000054: Size of optional header 0000/0
Windows XP
>nullSOH-XP.exe
* Low alignment PE with a null SizeOfOptionalHeader (XP)
>
152: 204C6F77 and [edi][ebp]*2[077],cl
Number Name VirtSize RVA PhysSize Offset Flag
1 .0 00000138 00000000 00000138 00000000 00000004
00000200: 70 72 69 6E-74 66 00 00-00 00 00 00-00 00 00 00 printf
00000210: F0 01 00 00-00 00 00 00-FE 01 00 00-00 00 00 00
00000220: 00 00 00 00-00 00 00 00-00 00 00 00-00 00 00 00
00000240: 63 72 74 2E-64 6C 6C 00- crt.dll
Count of sections 82
Size of optional header 0258
Machine Intel386
Thu Jan 01 01:00:00 1970
Magic optional header 010B
XP
>virtsectblXP.exe
* Low alignment PE with a virtual section table (XP)
>_

winver.asm

```
; a PE using Win32VersionValue to override OS version numbers

[...]

OSMAJOR equ 31
OSMINOR equ 41
BUILD equ 5926
ID equ 3 ; [0;3]

    at IMAGE_OPTIONAL_HEADER32.Win32VersionValue, dd OSMAJOR | (OSMINOR << 8) | ((BUILD & 03fffh) << 16) | (((ID & 3) ^ 02h) << 30)

[...]

EntryPoint:
    push OSVerEx
    call [__imp__GetVersionExA]

    push dword [OSVerEx.dwPlatformId]
    push dword [OSVerEx.dwBuildNumber]

    push dword [OSVerEx.dwMinorVersion]
    push dword [OSVerEx.dwMajorVersion]

    push Msg
    call [__imp__printf]
    add esp, 4 * 4
...

Msg db " * a PE overriding OS values: OS Ver %i.%i.%i PlatformID %i", 0ah, 0ah, 0
```



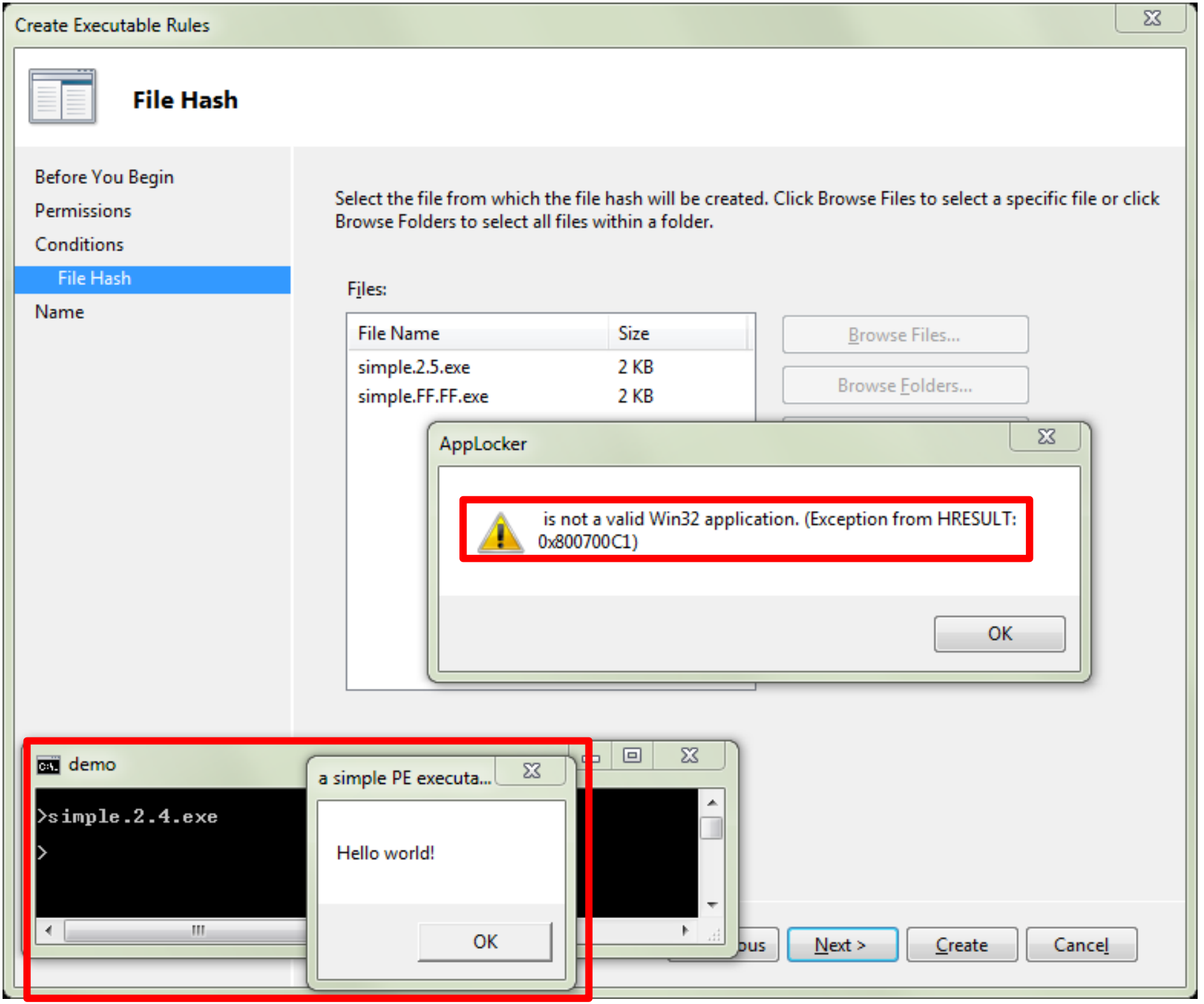
Microsoft Windows

Micro[illegible] Port[illegible]e Ex[illegible]cu[illegible]ble and Com[illegible] Ob[illegible]ct [illegible]le [illegible]or[illegible]at Spec[illegible]catio[illegible]

FAIL

Revision 8.2 – September 21, 2010

is there a *perfect* documentation?


Create Executable Rules
File Hash
Before You Begin
Permissions
Conditions
File Hash
Name
Select the file from which the file hash will be created. Click Browse Files to select a specific file or click Browse Folders to select all files within a folder.
Files:
File Name
Size
simple.2.5.exe
2 KB
simple.FF.FF.exe
2 KB
Browse Files...
Browse Folders...
AppLocker
is not a valid Win32 application. (Exception from HRESULT: 0x800700C1)
OK
demo
>simple.2.4.exe
>
a simple PE executa...
Hello world!
OK
Next >
Create
Cancel

Not at Microsoft, at least :)

Other documentations?

- mostly based on existing files
- no PoCs anyway
  - messy/limited/private

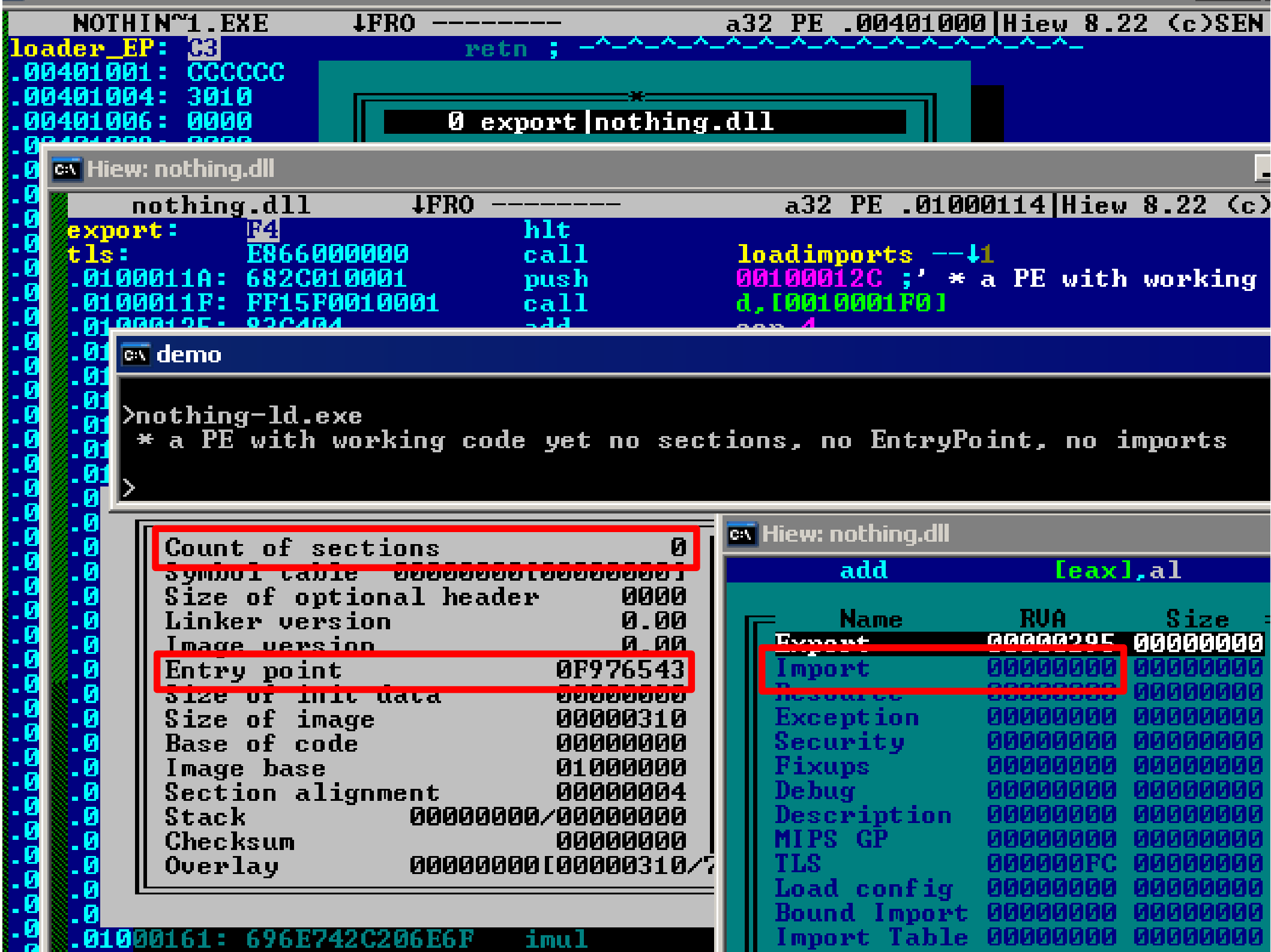
Corkami's is perfect?

- ***no!***
  - just a hobby
- ~~explain everything~~
  - highlight oddities

just to make sure

standard PE:

- Sections
- EntryPoint
- Imports


NOTHIN~1.EXE ↓FRO -------- a32 PE .00401000|Hiew 8.22 (c)SEN
loader_EP: C3 retn ; -^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-^-
.00401001: CCCCCC
.00401004: 3010
.00401006: 0000
0 export|nothing.dll
Hiew: nothing.dll
nothing.dll ↓FRO -------- a32 PE .01000114|Hiew 8.22 (c)
export: F4 hlt
tls: E866000000 call loadimports --↓1
.0100011A: 682C010001 push 01000012C ;' * a PE with working
.0100011F: FF15F0010001 call d,[010001F0]
demo
>nothing-ld.exe
* a PE with working code yet no sections, no EntryPoint, no imports
>
Count of sections 0
Symbol table 00000000[00000000]
Size of optional header 0000
Linker version 0.00
Image version 0.00
Entry point 0F976543
Size of init data 00000000
Size of image 00000310
Base of code 00000000
Image base 01000000
Section alignment 00000004
Stack 00000000/00000000
Checksum 00000000
Overlay 00000000[00000310/7
.01000161: 696E742C206E6F imul
Hiew: nothing.dll
add [eax],al
Name RVA Size
Export 00000295 00000000
Import 00000000 00000000
Exception 00000000 00000000
Security 00000000 00000000
Fixups 00000000 00000000
Debug 00000000 00000000
Description 00000000 00000000
MIPS GP 00000000 00000000
TLS 000000FC 00000000
Load config 00000000 00000000
Bound Import 00000000 00000000
Import Table 00000000 00000000

Static oddities

most basic PE

- 'DataFile PE'
  - *LoadlibraryEx* with *LOAD_LIBRARY_AS_DATAFILE*
- must be a PE
- ***just*** a PE
  - 'MZ' / e_lfanew / 'PE'. that's ***it***
  - ~~machine~~ ~~magic~~ ~~imagebase~~ ~~alignments~~ ~~subsystem~~
  - code!
  - non-null!
  - break parsers
    - Corrupt values/truncated headers

d_resource.dll

info | MZ | PE | resources | hexdump | log (4)

PE Header

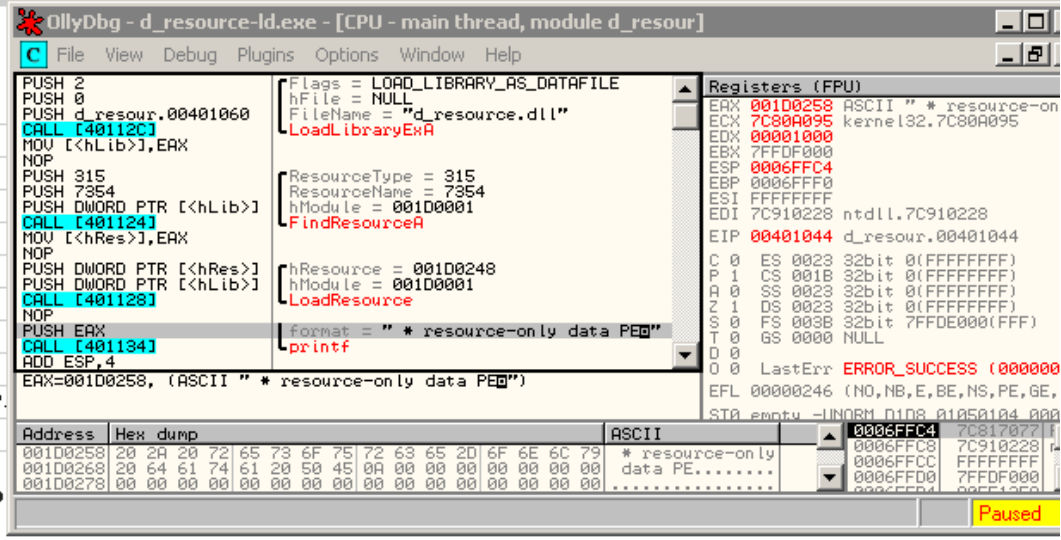
Signature	PE
Machine	0x[illegible]
NumberOfSections	0xffff
TimeDateStamp	0xffffffff
PointerToSymbolTable	0xffffffff
NumberOfSymbols	0xffffffff
SizeOfOptionalHeader	0xe0
Characteristics	0x[illegible]
Magic	0x10b
LinkerVersion	255.255
SizeOfCode	0xffffffff
SizeOfInitializedData	0xffffffff
SizeOfUninitializedData	0xffffffff
AddressOfEntryPoint	0xffffffff
BaseOfCode	0xffffffff
BaseOfData	0xffffffff
ImageBase	0xffffffff
SectionAlignment	0xffffffff
FileAlignment	0xffffffff
OperatingSystemVersion	65535.65535
ImageVersion	65535.65535
SubsystemVersion	65535.65535
Reserved1	0xffffffff
SizeOfImage	0xffffffff
SizeOfHeaders	0x1000
CheckSum	0xffffffff
Subsystem	0xffff
DllCharacteristics	0xffff
SizeOfStackReserve	0xffffffff
SizeOfStackCommit	0xffffffff
SizeOfHeapReserve	0xffffffff
SizeOfHeapCommit	0xffffffff
LoaderFlags	0xffffffff

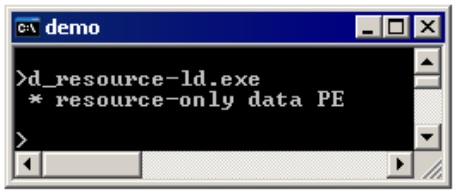
Sections

name	
Ts[illegible]	
	0x7.

Data Directo

type	va	size
EXPORT	0xffffffff	0xffffffff
IMPORT	0xffffffff	0xffffffff
RESOURCE	0x1000	0xffffffff
EXCEPTION	0xffffffff	0xffffffff
SECURITY	0xffffffff	0xffffffff
BASERELOC	0xffffffff	0xffffffff
DEBUG	0xffffffff	0xffffffff
ARCHITECTURE	0xffffffff	0xffffffff
GLOBALPTR	0xffffffff	0xffffffff
TLS	0xffffffff	0xffffffff
LOAD_CONFIG	0xffffffff	0xffffffff
Bound_IAT	0xffffffff	0xffffffff
IAT	0xffffffff	0xffffffff
Delay_IAT	0xffffffff	0xffffffff
CLR_Header	0xffffffff	0xffffffff
	0xffffffff	0xffffffff

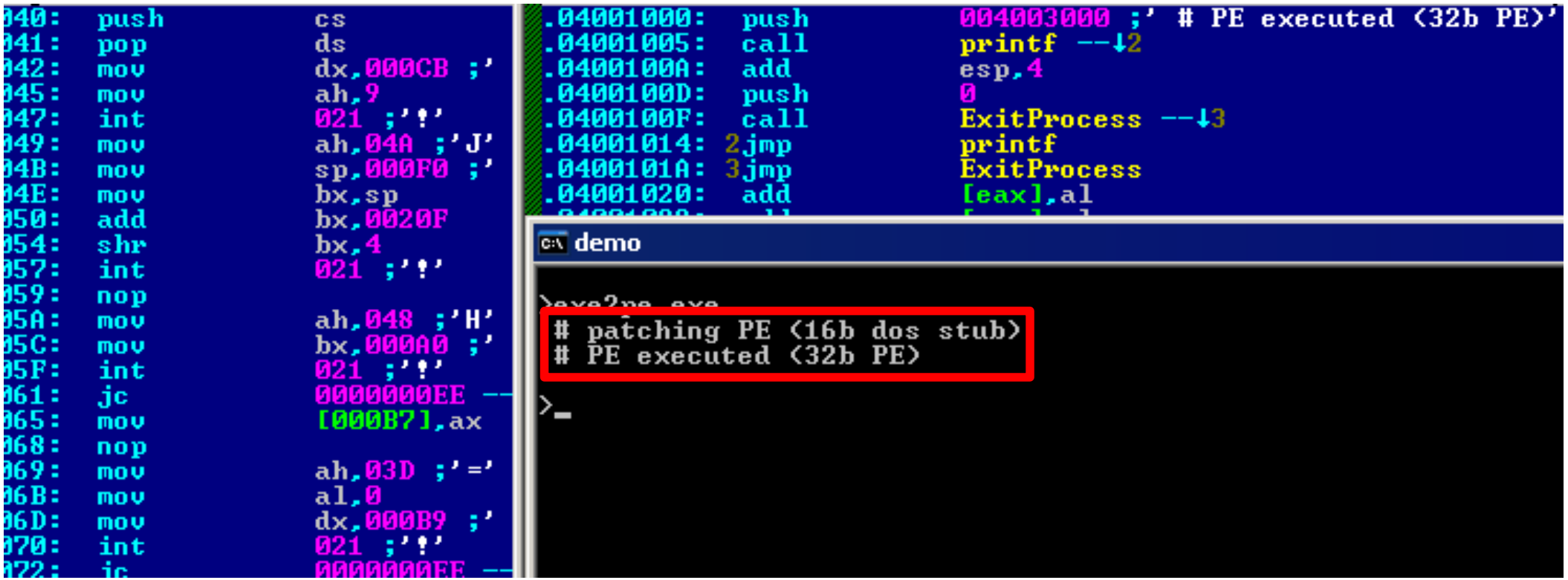




back to 'classic' PEs

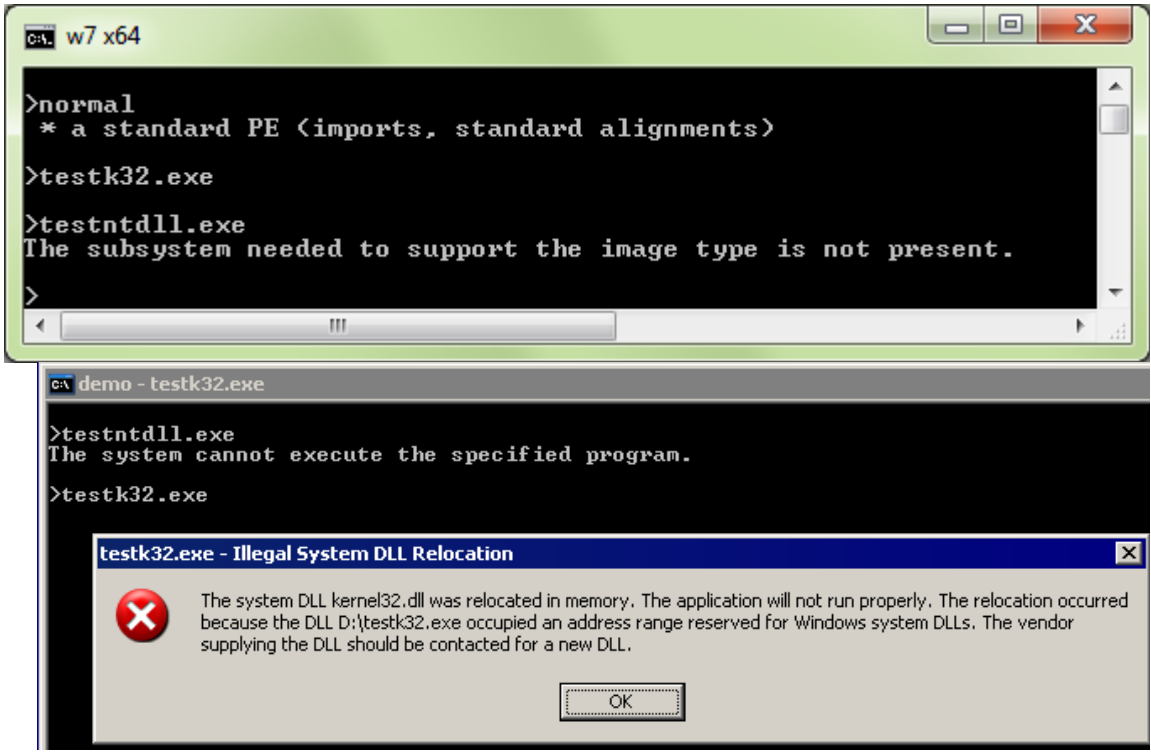
DOS header

- Good old 16b stub
  - still in Windows 7 64b !
- “This program cannot be run in DOS mode.” ?



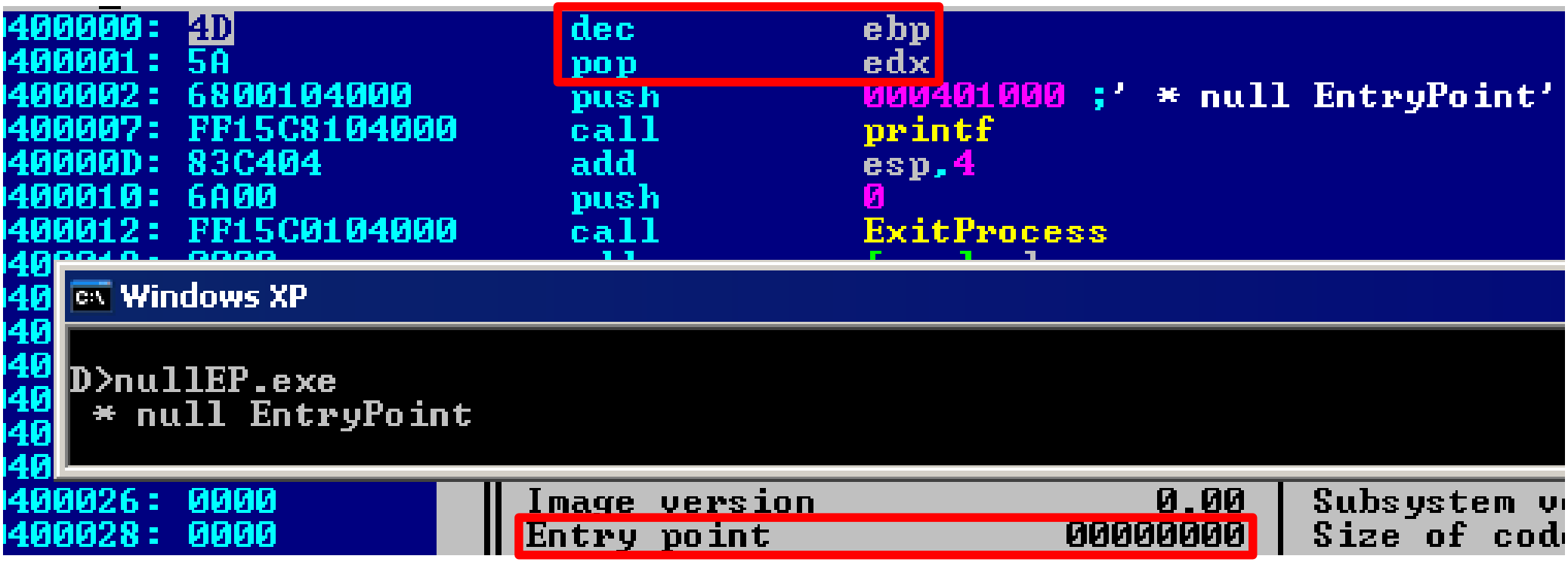
ImageBase

- multiple of 0x10000
- user-mode
  - any address except system DLLs
  - 00000000 under XP
- kernel-mode
  - via relocation
  - relocated to 10000
  - CVE-2012-2273



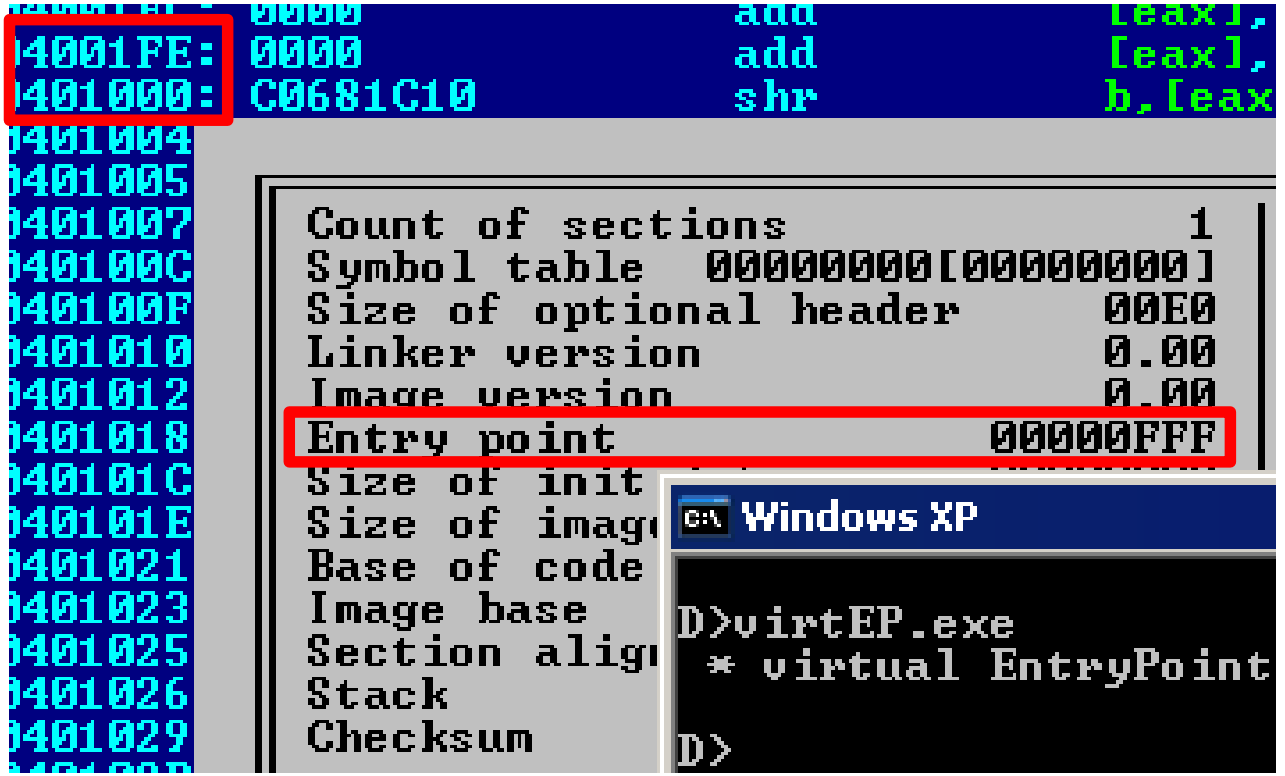
EntryPoint

- null
  - MZ => dec ebp/pop edx



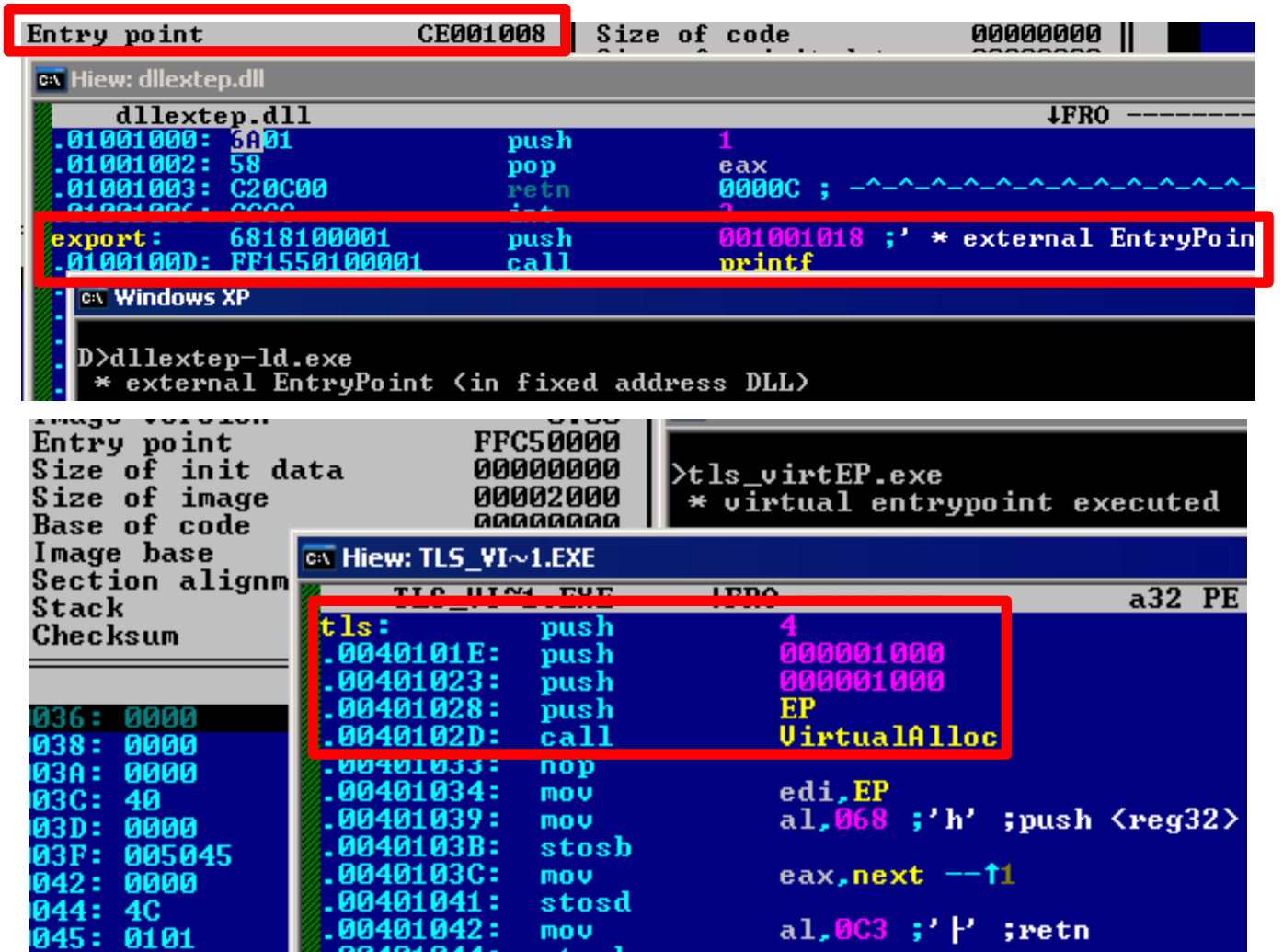
EntryPoint

- virtual
  - 00 C0 => add al, al



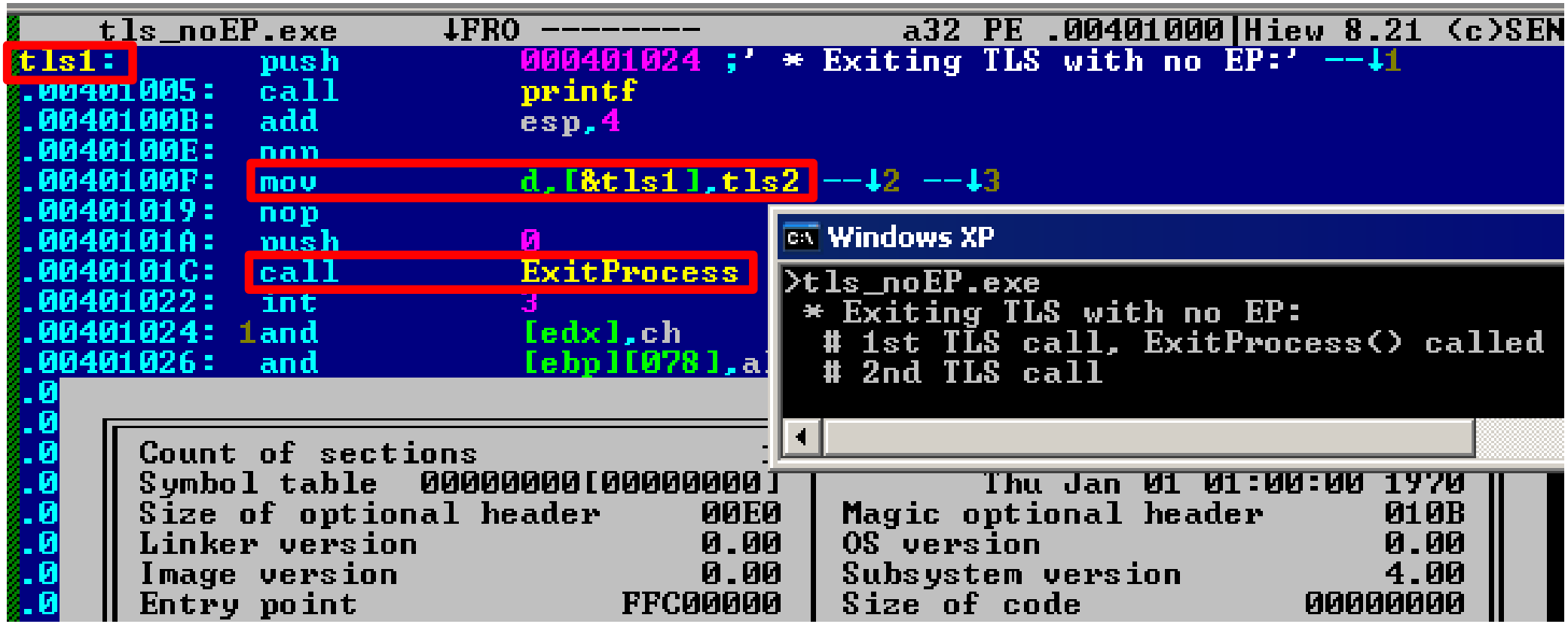
EntryPoint

- external
  - in a DLL / allocated via TLS



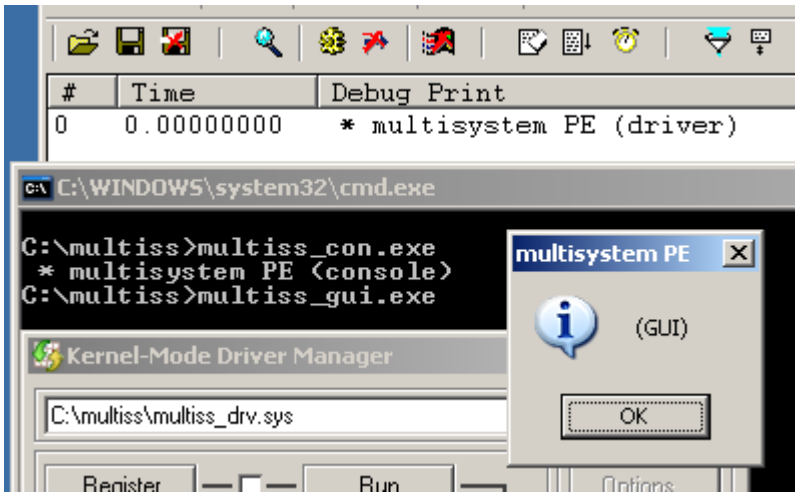
EntryPoint

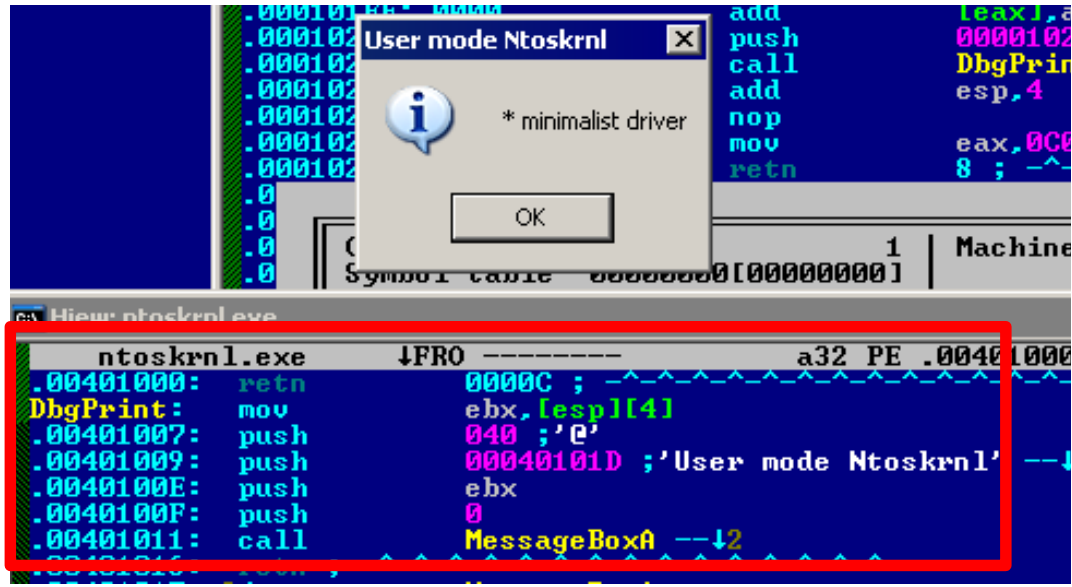
- ignored
  - via TLS



Subsystem

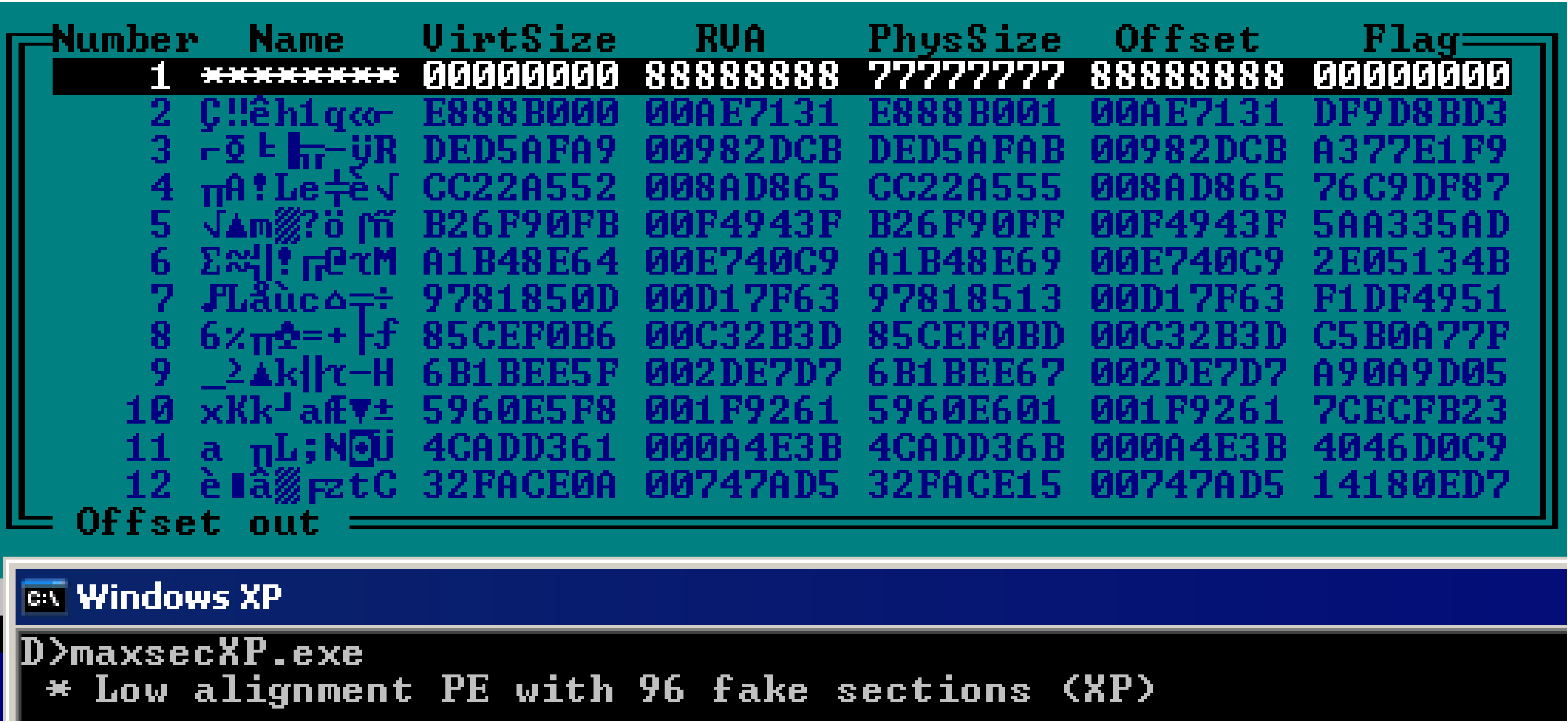
- **no** trick :(
  - last required element of the header
- no specific requirements
  - low alignments
    - unpack drivers in user-mode
    - multi-subsystem PE





Sections

- 0-96/65536
- oversized or not (up to 0x74xx0000)
- sections in sections, duplicates, shuffled



Number	Name	VirtSize	RVA	PhysSize	Offset	Flag
1	**********	00000000	88888888	77777777	88888888	00000000
2	Ç‼êh1q«┌	E888B000	00AE7131	E888B001	00AE7131	DF9D8BD3
3	┌Φ╘▌╥─ÿR	DED5AFA9	00982DCB	DED5AFAB	00982DCB	A377E1F9
4	πA!Le╪è√	CC22A552	008AD865	CC22A555	008AD865	76C9DF87
5	√▲m▒?ö ╓ñ	B26F90FB	00F4943F	B26F90FF	00F4943F	5AA335AD
6	Σ≈║!╓@τM	A1B48E64	00E740C9	A1B48E69	00E740C9	2E05134B
7	♪Låùc⌂╤÷	9781850D	00D17F63	97818513	00D17F63	F1DF4951
8	6%╥♠=+├ƒ	85CEF0B6	00C32B3D	85CEF0BD	00C32B3D	C5B0A77F
9	_≥▲k║╟τ─H	6B1BEE5F	002DE7D7	6B1BEE67	002DE7D7	A90A9D05
10	xKk┘aÆ▼±	5960E5F8	001F9261	5960E601	001F9261	7CECFB23
11	a ╥L;N◙ü	4CADD361	000A4E3B	4CADD36B	000A4E3B	4046D0C9
12	è▌â▒╒ztC	32FACE0A	00747AD5	32FACE15	00747AD5	14180ED7

Offset out

Windows XP

```
D>maxsecXP.exe
 * Low alignment PE with 96 fake sections (XP)
```

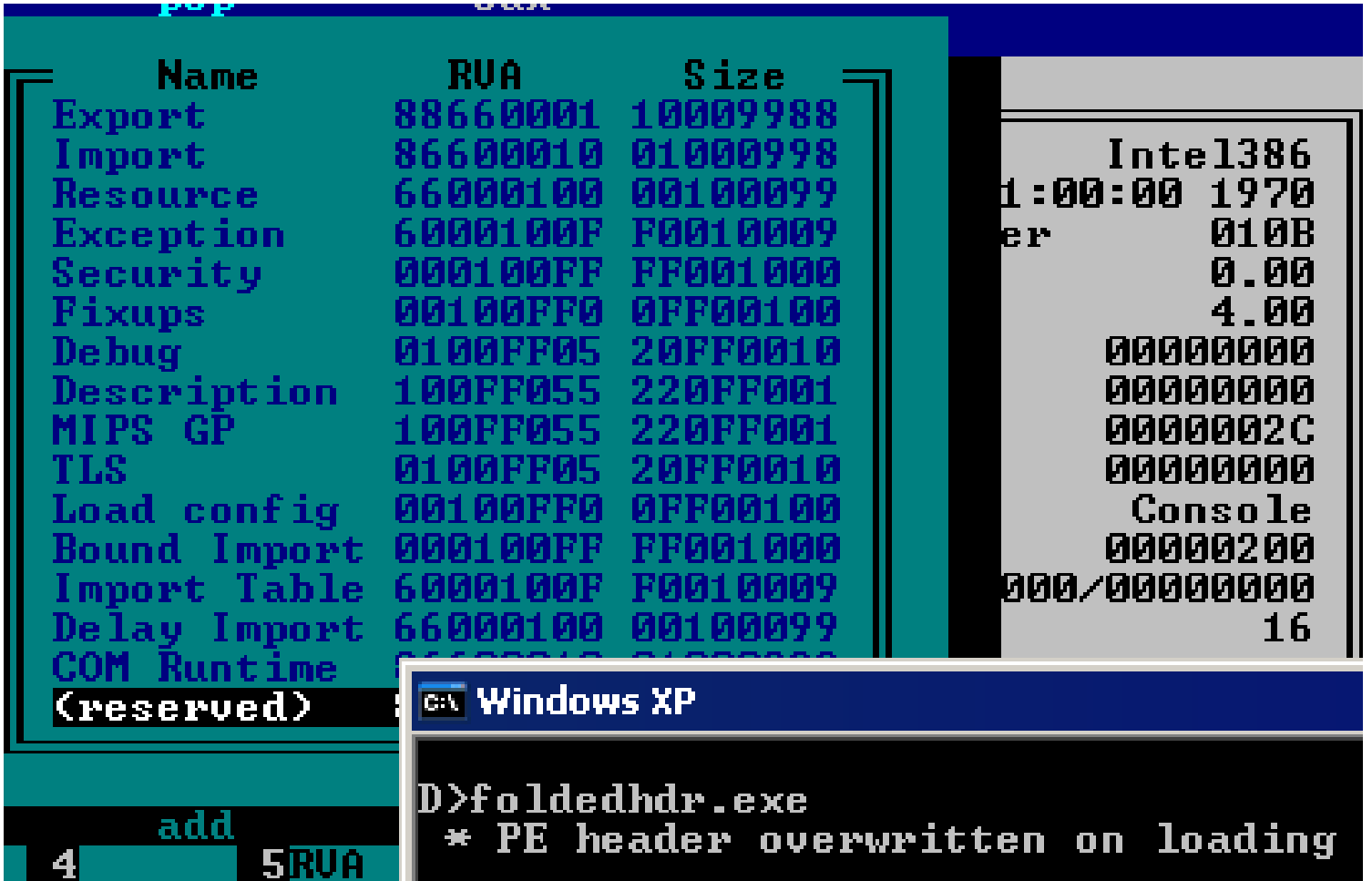
Dynamic oddities

loading process 1/2

- Headers are parsed on disk
- Data directories are parsed in memory
  - **after** section mapping

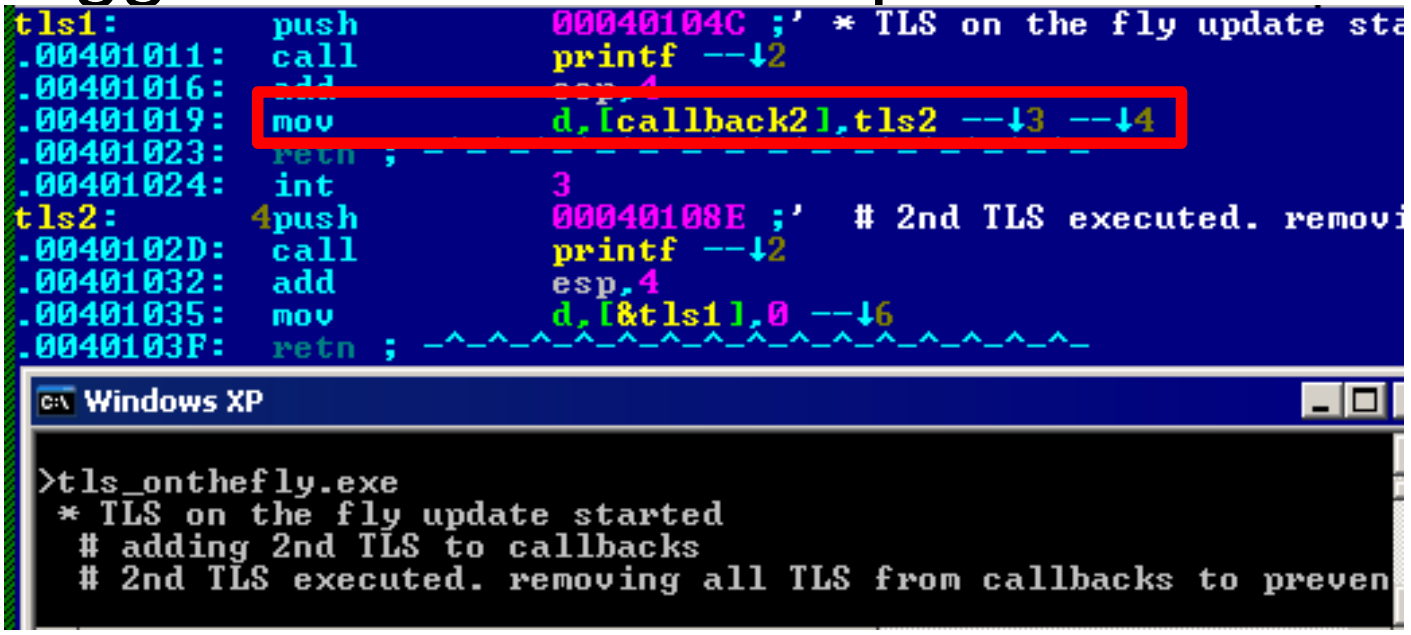
loading process 2/2

- sections overlap header
  - true Data directories are revealed



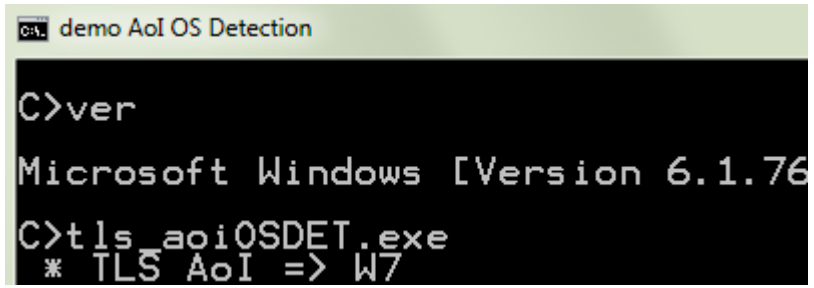
TLS 1/2

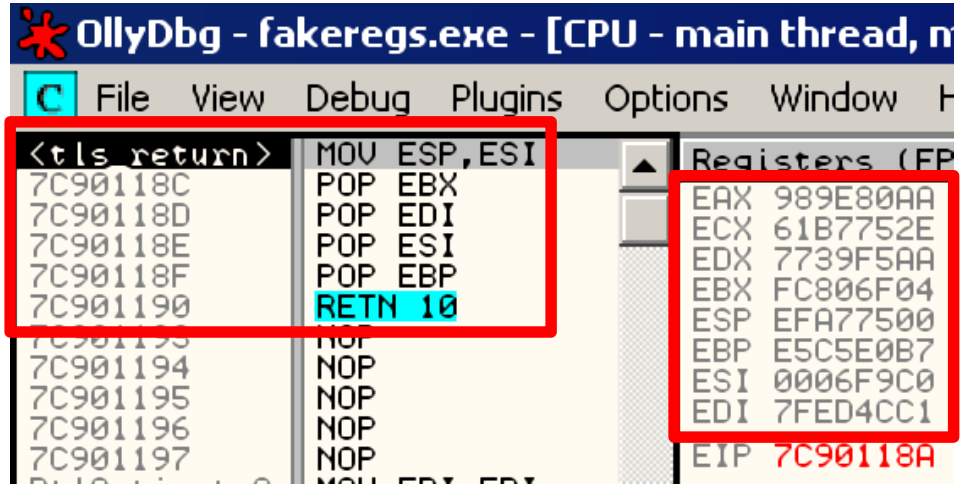
- list of callbacks, updated on the fly
- executed at threat start/stop
  - before EntryPoint
  - after ExitProcess
- can trigger unhandled exceptions

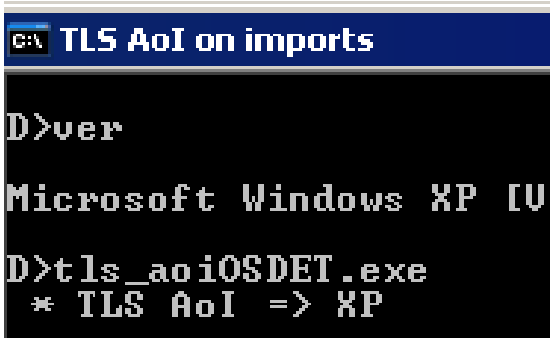


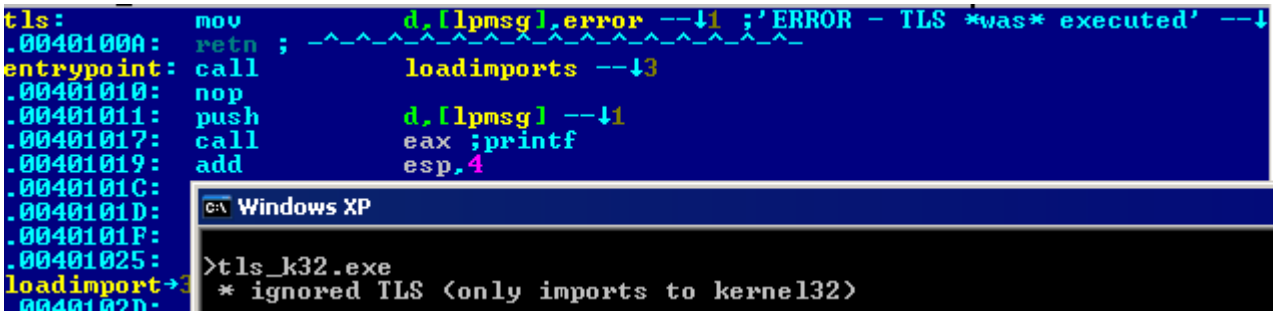
TLS 2/2

- points to import
- tricky execution conditions
- different loading order
- 'anything but ESI'





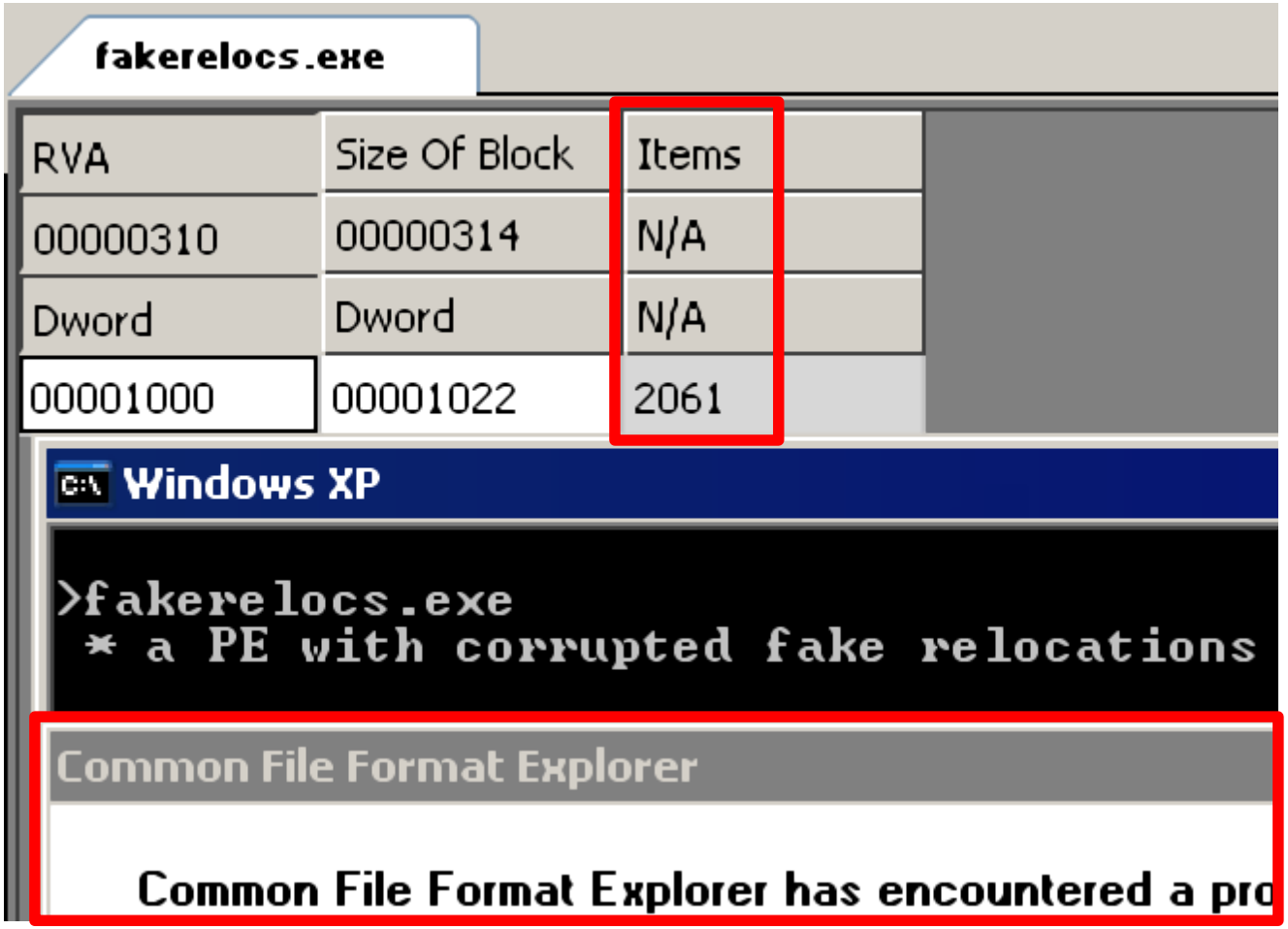




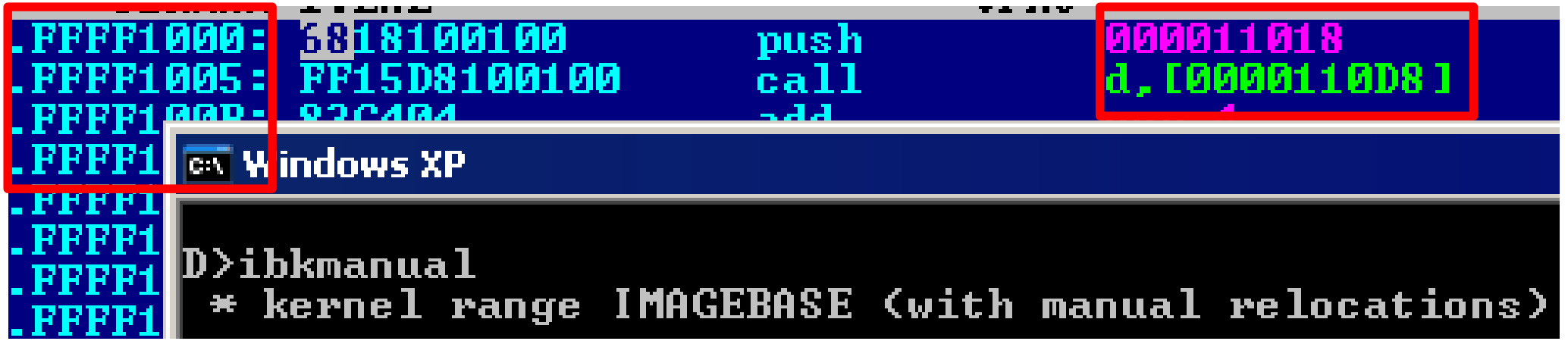
Relocations

- rebase code if loaded at different address
- not required in x64
  - empty relocations still in x64b binaries

faked relocations

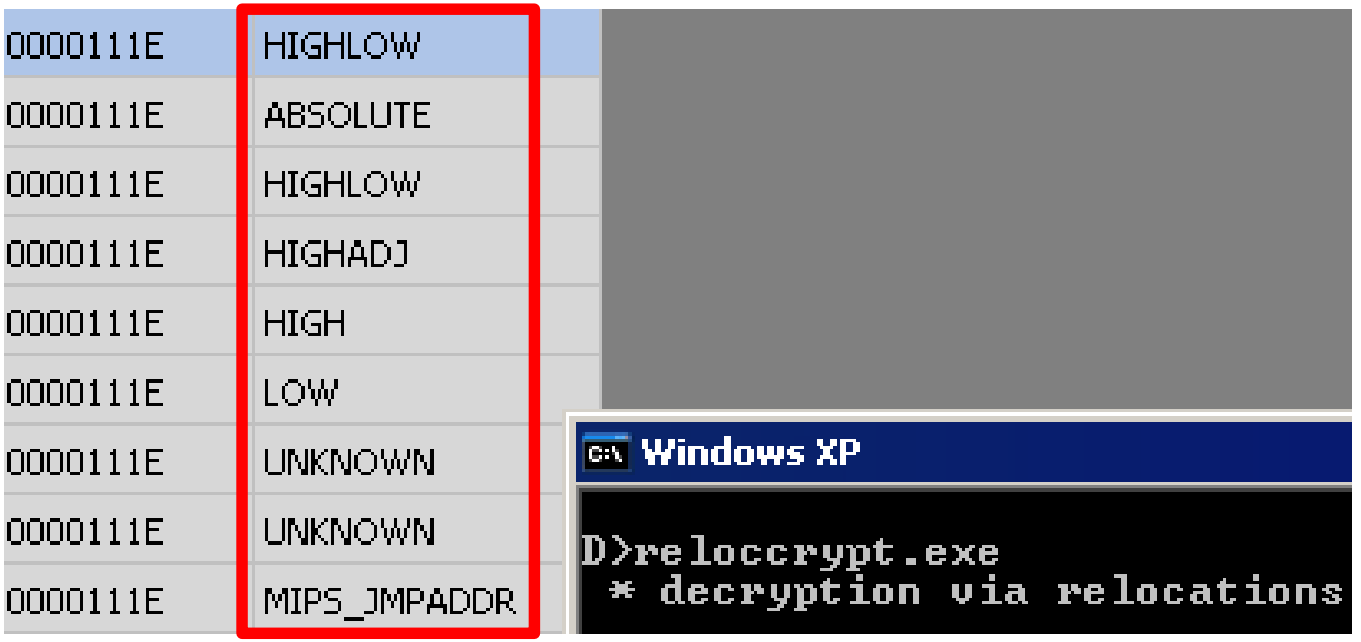


manual relocations



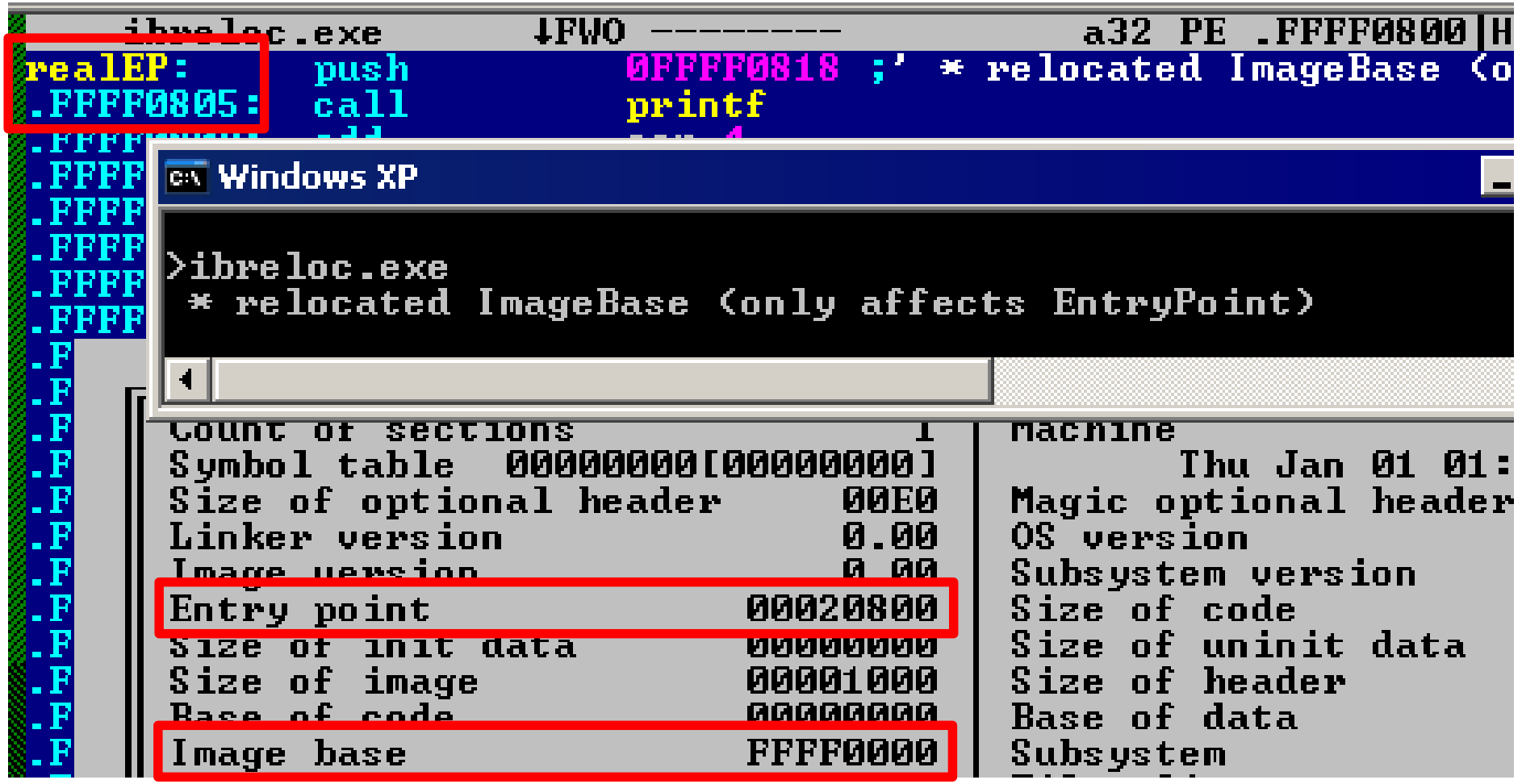
Relocations encryption

- applied anywhere
  - encryption
  - on itself!
- MIPS supported on Intel OS+PE

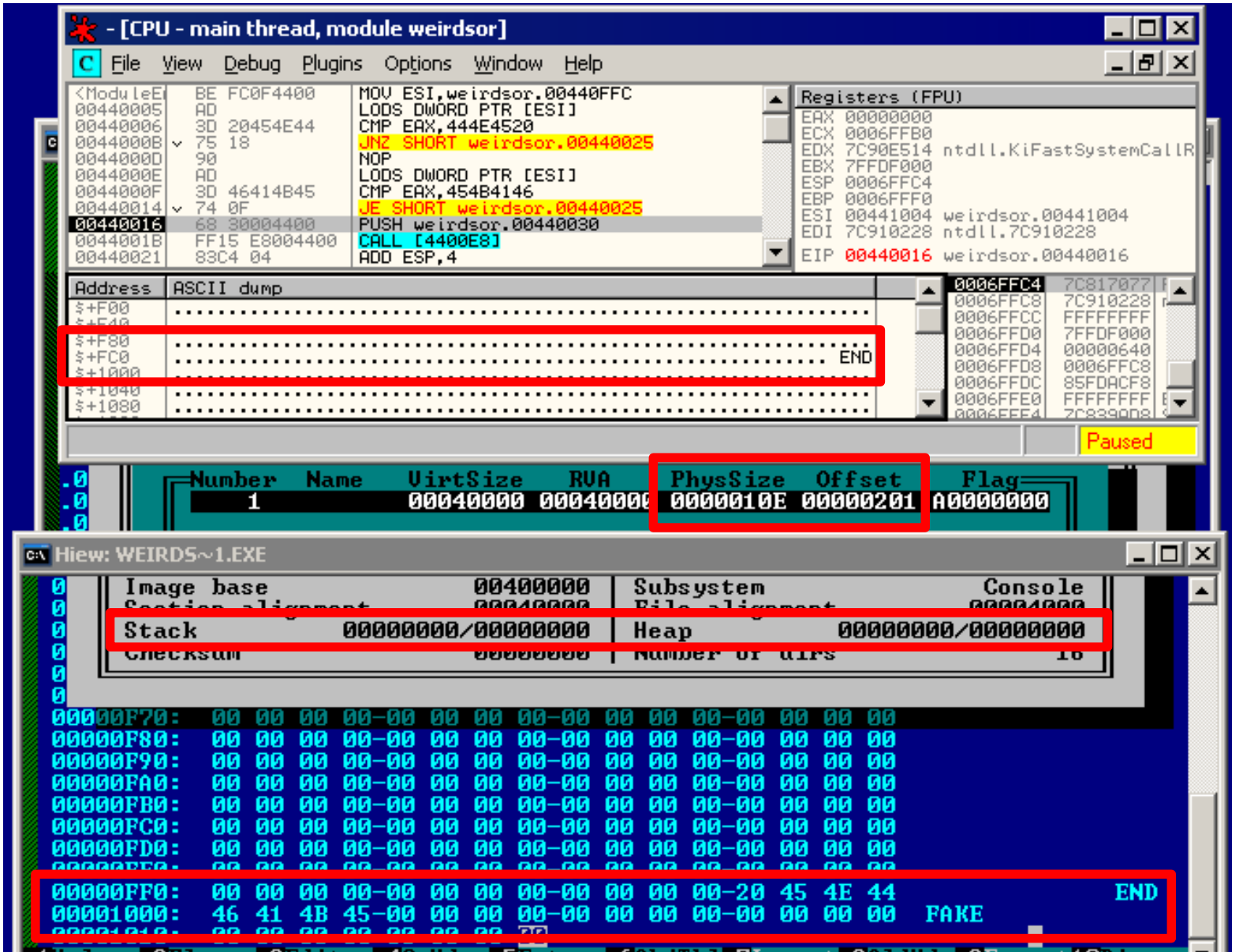


Relocations on ImageBase

- affects the EntryPoint



one last...


- [CPU - main thread, module weirdsor]
File View Debug Plugins Options Window Help
00440016 68 30004400 PUSH weirdsor.00440030
0044001B FF15 E8004400 CALL [4400E8]
00440021 83C4 04 ADD ESP,4
Registers (FPU)
EIP 00440016 weirdsor.00440016
Address ASCII dump
$+F80
$+FC0 END
Paused
Number Name VirtSize RVA PhysSize Offset Flag
1 00040000 00040000 0000010E 00000201 A0000000
Hiew: WEIRDS~1.EXE
Image base 00400000 Subsystem Console
Stack 00000000/00000000 Heap 00000000/00000000
00000FF0: 00 00 00 00-00 00 00 00-00 00 00 00-20 45 4E 44 END
00001000: 46 41 4B 45-00 00 00 00-00 00 00 00-00 00 00 00 FAKE

Conclusion

- PE is a mess
  - different OSes, different parsers
  - no doc/tool is perfect
- still many unknowns
- simple http://pe101.corkami.com
- advanced http://pe.corkami.com
  - 160+ PoCs

Acknowledgments

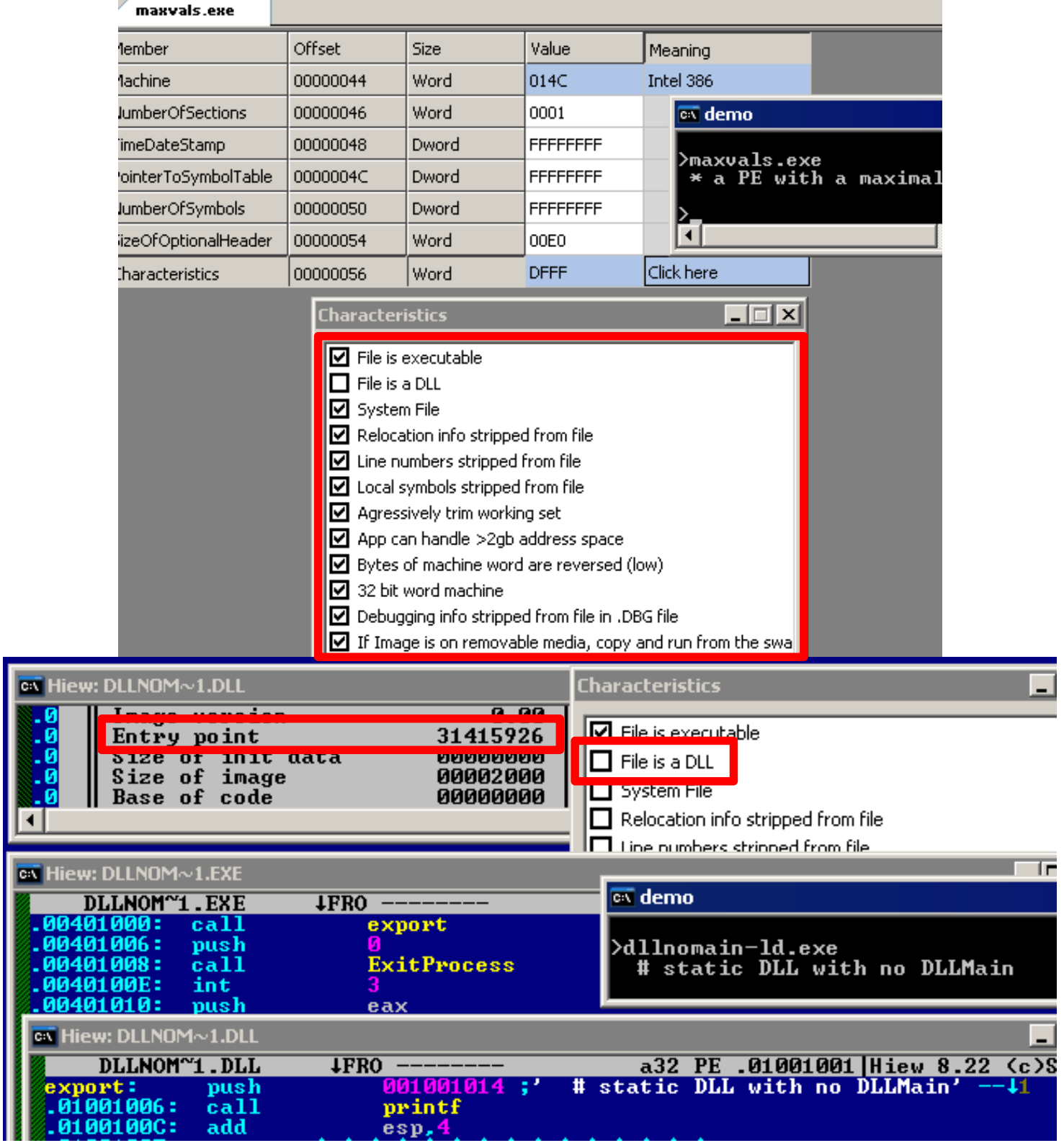
- Peter Ferrie
- Bernhard Treutwein, Costin Ionescu, Deroko, Ivanlef0u, Kris Kaspersky, Moritz Kroll, ReversingLabs, Walied Assar, ...

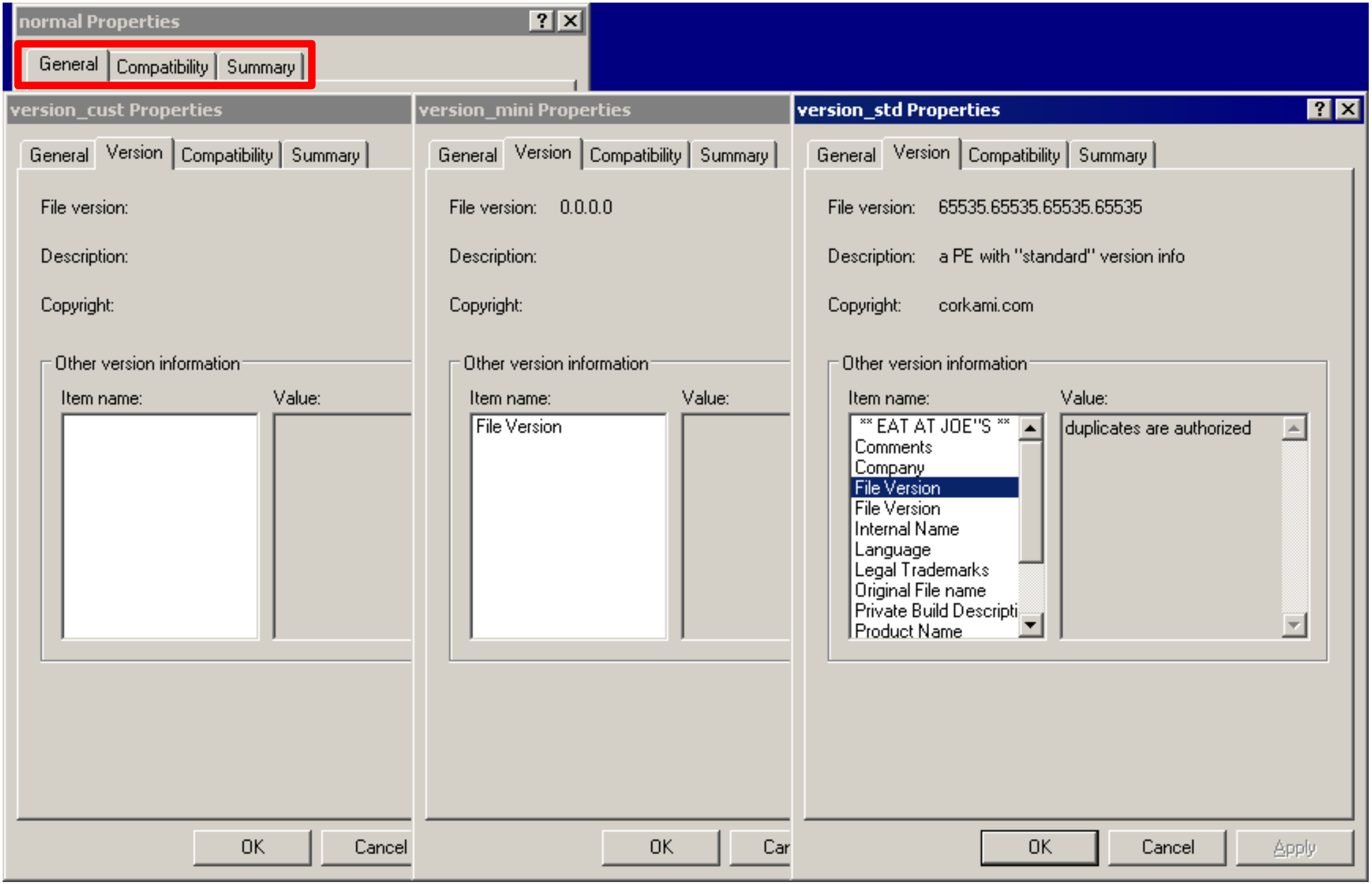
Questions?

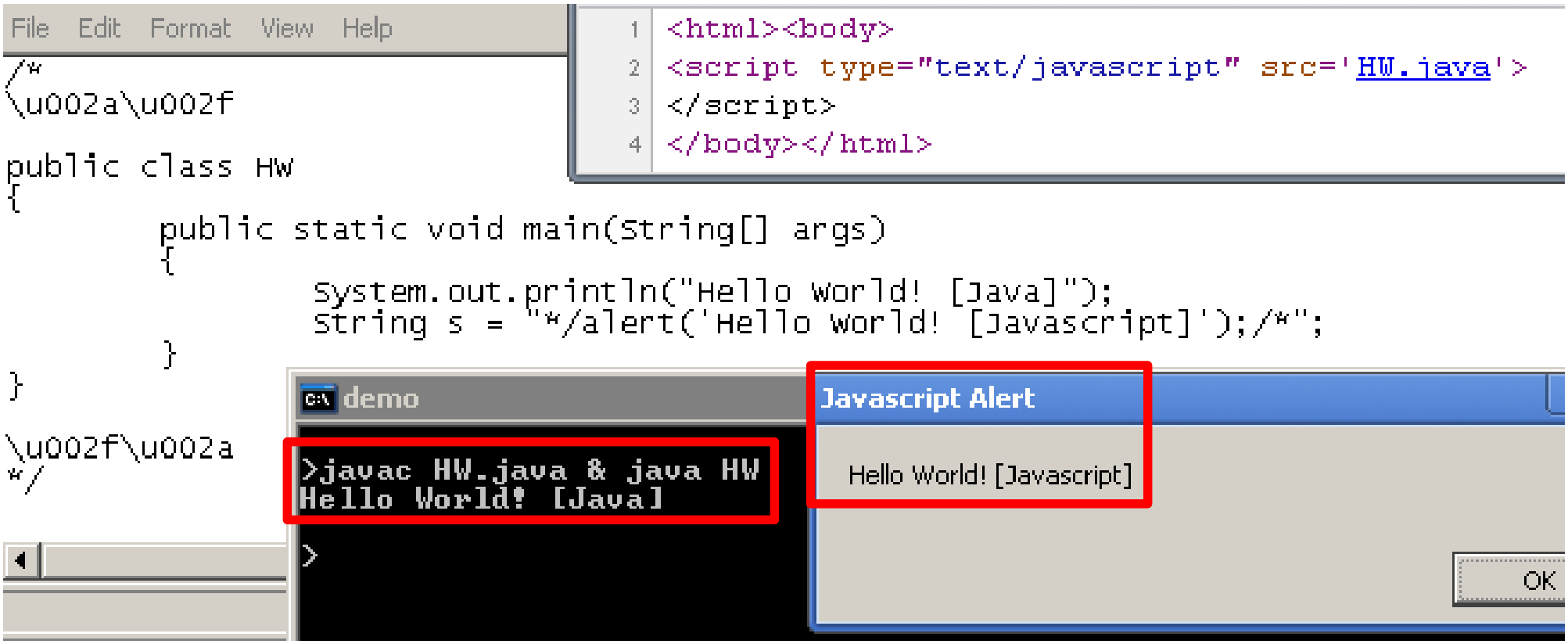
Thank YOU!

Ange Albertini @gmail.com

@ange4771


maxvals.exe
Member | Offset | Size | Value | Meaning
Machine | 00000044 | Word | 014C | Intel 386
NumberOfSections | 00000046 | Word | 0001
TimeDateStamp | 00000048 | Dword | FFFFFFFF
PointerToSymbolTable | 0000004C | Dword | FFFFFFFF
NumberOfSymbols | 00000050 | Dword | FFFFFFFF
SizeOfOptionalHeader | 00000054 | Word | 00E0
Characteristics | 00000056 | Word | DFFF | Click here
demo
>maxvals.exe
* a PE with a maximal
Characteristics
File is executable
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)
32 bit word machine
Debugging info stripped from file in .DBG file
If Image is on removable media, copy and run from the swa
Hiew: DLLNOM~1.DLL
Entry point 31415926
Size of image 00002000
Base of code 00000000
Characteristics
File is executable
File is a DLL
System File
Relocation info stripped from file
Hiew: DLLNOM~1.EXE
DLLNOM~1.EXE ↓FRO --------
.00401000: call export
.00401006: push 0
.00401008: call ExitProcess
.0040100E: int 3
.00401010: push eax
demo
>dllnomain-ld.exe
static DLL with no DLLMain
Hiew: DLLNOM~1.DLL
DLLNOM~1.DLL ↓FRO -------- a32 PE .01001001 Hiew 8.22 (c)S
export: push 001001014 ;' # static DLL with no DLLMain' --↓1
.01001006: call printf
.0100100C: add esp,4


normal Properties
General
Compatibility
Summary
version_cust Properties
General
Version
Compatibility
Summary
File version:
Description:
Copyright:
Other version information
Item name:
Value:
OK
Cancel
version_mini Properties
General
Version
Compatibility
Summary
File version: 0.0.0.0
Description:
Copyright:
Other version information
Item name:
Value:
File Version
OK
Car
version_std Properties
General
Version
Compatibility
Summary
File version: 65535.65535.65535.65535
Description: a PE with "standard" version info
Copyright: corkami.com
Other version information
Item name:
Value:
** EAT AT JOE'S **
Comments
Company
File Version
File Version
Internal Name
Language
Legal Trademarks
Original File name
Private Build Descripti
Product Name
duplicates are authorized
OK
Cancel
Apply


File Edit Format View Help
/*
\u002a\u002f
public class HW
{
public static void main(String[] args)
{
System.out.println("Hello World! [Java]");
String s = "*/alert('Hello World! [Javascript]');/*";
}
}
\u002f\u002a
*/
1 <html><body>
2 <script type="text/javascript" src='HW.java'>
3 </script>
4 </body></html>
demo
>javac HW.java & java HW
Hello World! [Java]
>
Javascript Alert
Hello World! [Javascript]
OK