EXECUTABLE FILE FORMATS

Executable File Formats

- Portable Executable (PE)
  - Executable file format of choice for Windows
- Executable and Linkable Format (ELF)
  - Executable file format of choice for Linux

PE

- Portable Executable
  - Executable file format of choice for Windows
    - Including Windows CE
  - Modified version of Unix COFF (Common Object File Format)
  - .cpl, .exe, .dll, .ocx, .sys, .scr, .drv, .tlb

PE Addressing

- Virtual Address (VA)
  - Virtual address of an object once it is loaded into memory
- Relative Virtual Address (RVA)
  - Offset from the beginning of the loaded image

PE Tables

- Import Table
- Export Table
- Resource Table
- Exception Table
- Certificate Table
- Base Relocation Table
- Thread Local Storage Table
- …

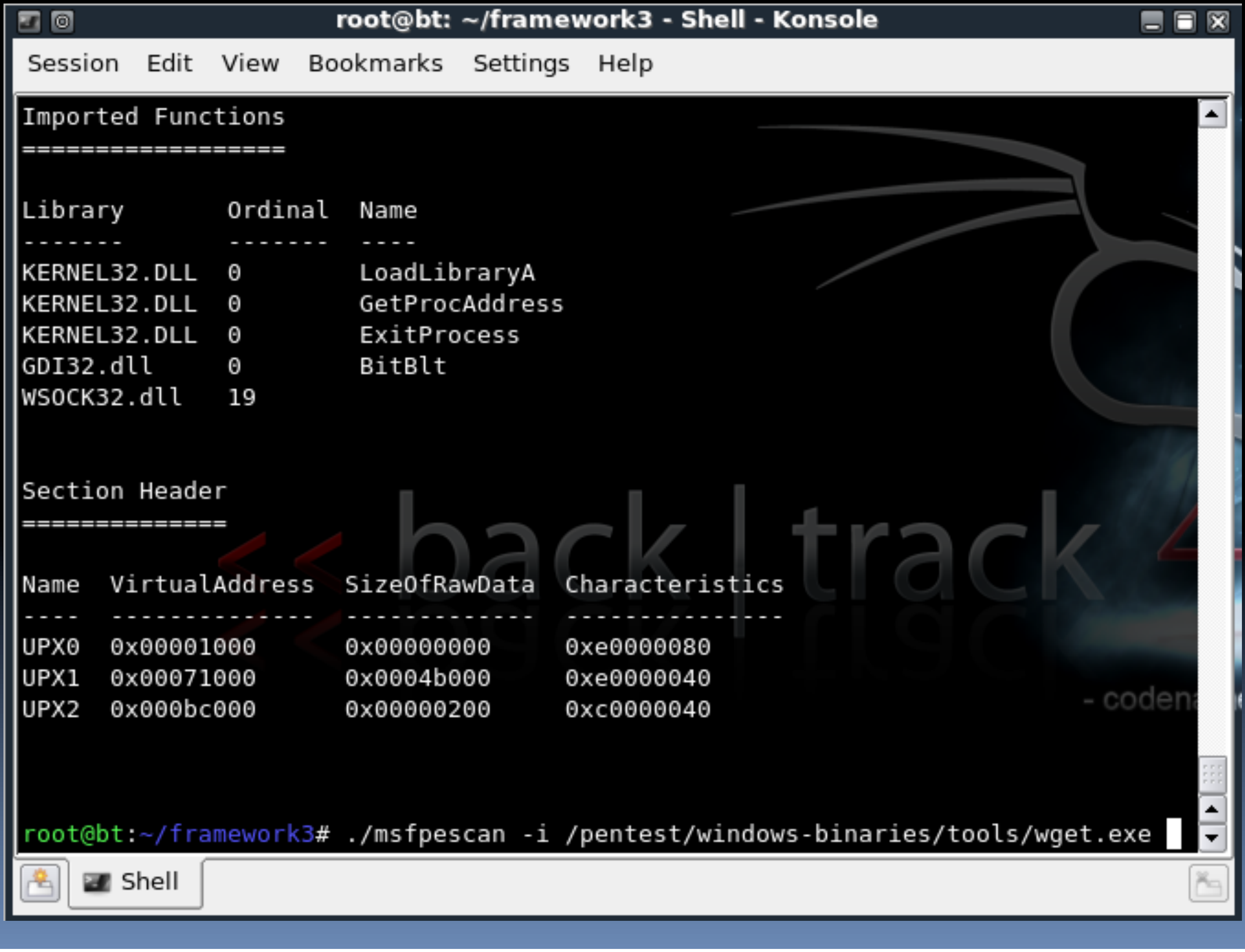
PE Import and Export Tables

- Import Table (.idata)
  - Used as a lookup table for external function addresses
  - Import by ordinal or name
- Export Table (.edata)
  - Used as a lookup table for internal function addresses
  - Export by ordinal or name

PE Resource Table

- Resource Table (.rsrc)
  - Multi-level binary-sorted tree
    - Windows typically uses 3 levels
      1. Type
      2. Name
      3. Language
    - Leaves contain a description and raw data

msfpescan

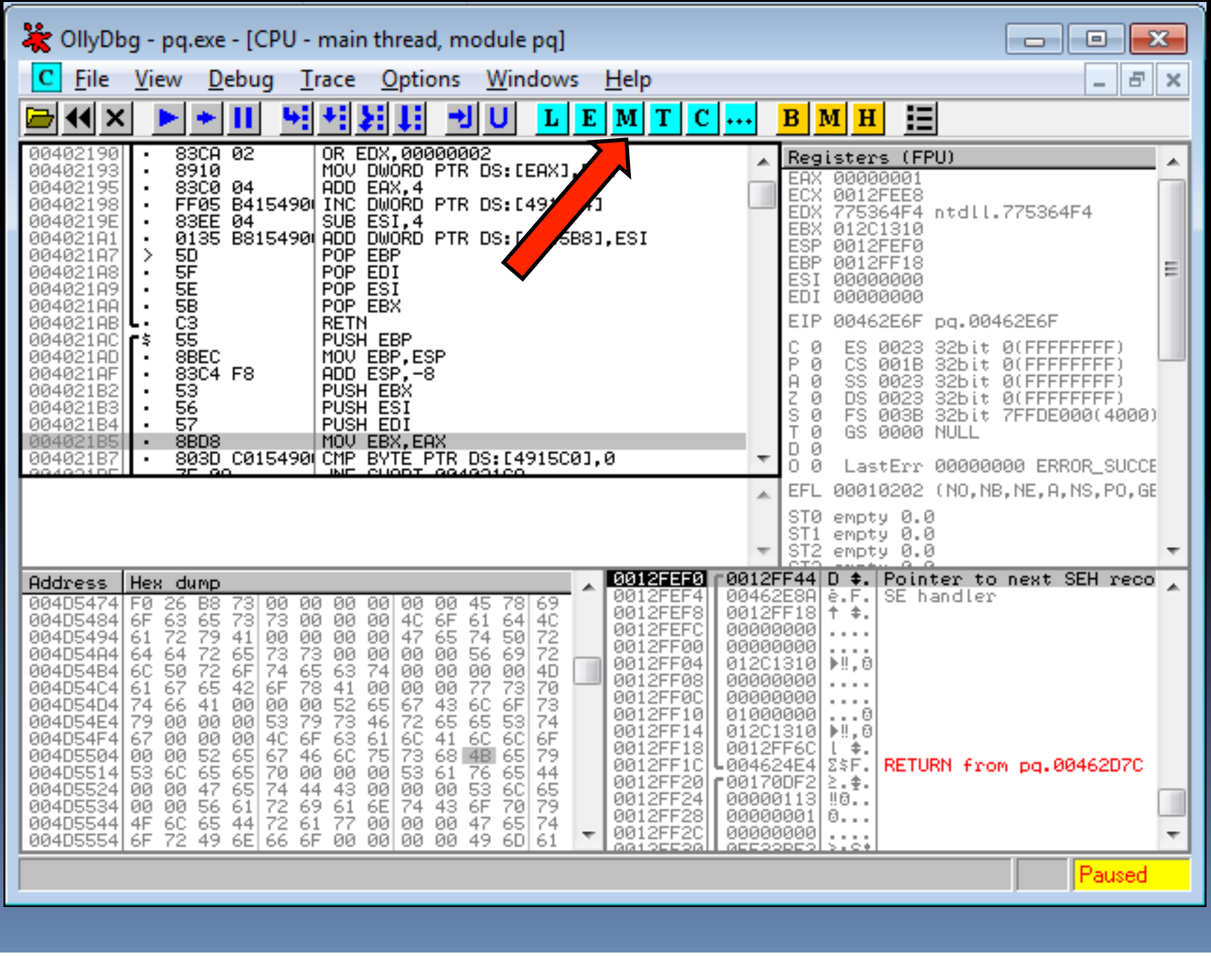


root@bt: ~/framework3 - Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell

```
Imported Functions
==================

Library        Ordinal  Name
-------        -------  ----
KERNEL32.DLL   0        LoadLibraryA
KERNEL32.DLL   0        GetProcAddress
KERNEL32.DLL   0        ExitProcess
GDI32.dll      0        BitBlt
WSOCK32.dll    19


Section Header
==============

Name  VirtualAddress  SizeOfRawData  Characteristics
----  --------------  -------------  ---------------
UPX0  0x00001000      0x00000000     0xe0000080
UPX1  0x00071000      0x0004b000     0xe0000040
UPX2  0x000bc000      0x00000200     0xc0000040


root@bt:~/framework3# ./msfpescan -i /pentest/windows-binaries/tools/wget.exe
```

OllyDbg PE Parsing

- Click on the “Modules” button



```
00402190 │ .  83CA 02          OR EDX,00000002
00402193 │ .  8910             MOV DWORD PTR DS:[EAX],
00402195 │ .  83C0 04          ADD EAX,4
00402198 │ .  FF05 B4154900    INC DWORD PTR DS:[49   4]
0040219E │ .  83EE 04          SUB ESI,4
004021A1 │ .  0135 B8154900    ADD DWORD PTR DS:[   5B8],ESI
004021A7 │ >  5D               POP EBP
004021A8 │ .  5F               POP EDI
004021A9 │ .  5E               POP ESI
004021AA │ .  5B               POP EBX
004021AB └ .  C3               RETN
004021AC ┌ $  55               PUSH EBP
004021AD │ .  8BEC             MOV EBP,ESP
004021AF │ .  83C4 F8          ADD ESP,-8
004021B2 │ .  53               PUSH EBX
004021B3 │ .  56               PUSH ESI
004021B4 │ .  57               PUSH EDI
004021B5 │ .  8BD8             MOV EBX,EAX
004021B7 │ .  803D C0154900    CMP BYTE PTR DS:[4915C0],0
```

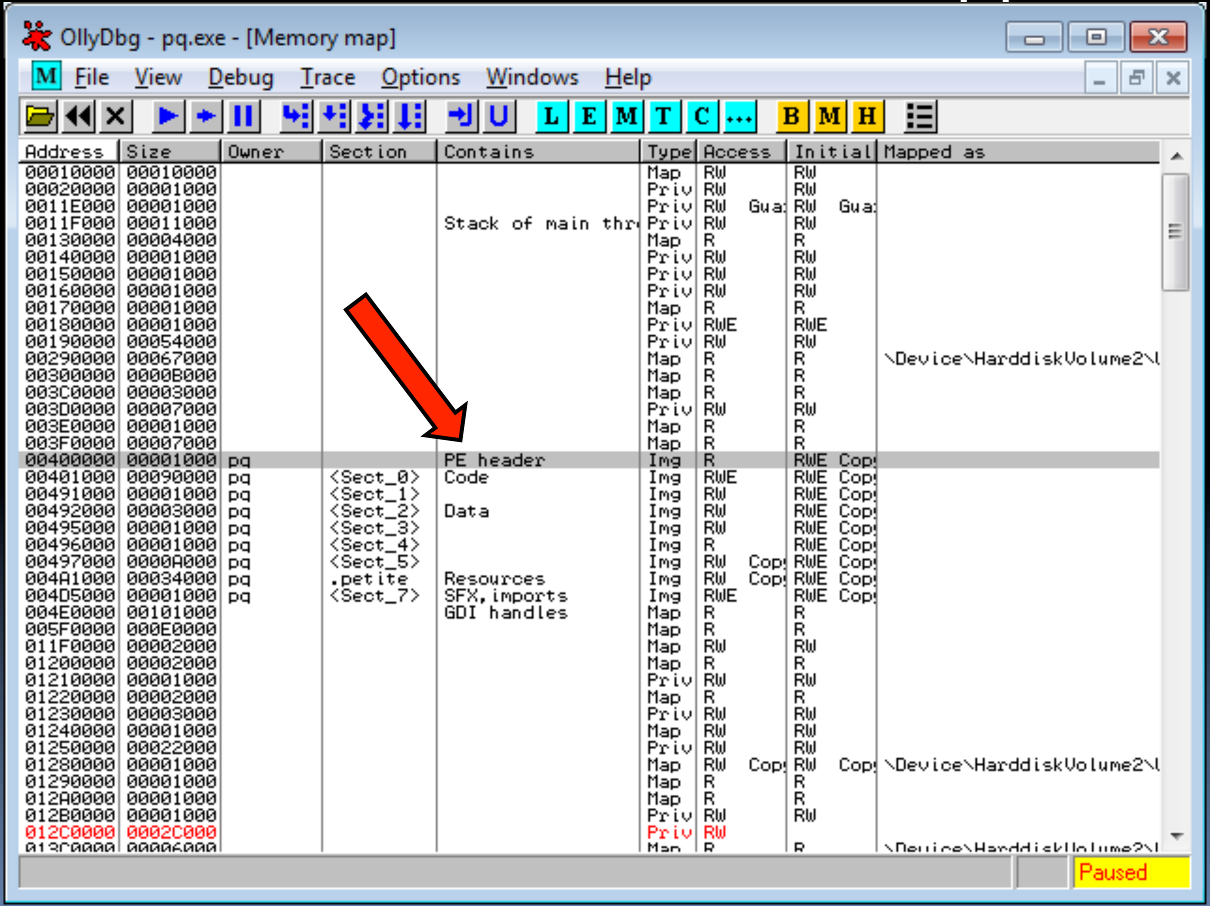
```
Registers (FPU)
EAX 00000001
ECX 0012FEE8
EDX 775364F4 ntdll.775364F4
EBX 012C1310
ESP 0012FEF0
EBP 0012FF18
ESI 00000000
EDI 00000000

EIP 00462E6F pq.00462E6F

C 0  ES 0023 32bit 0(FFFFFFFF)
P 0  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDE000(4000)
T 0  GS 0000 NULL
D 0
O 0  LastErr 00000000 ERROR_SUCCE

EFL 00010202 (NO,NB,NE,A,NS,PO,GE

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
```

```
Address  Hex dump
004D5474 F0 26 B8 73 00 00 00 00 00 00 45 78 69
004D5484 6F 63 65 73 73 00 00 00 4C 6F 61 64 4C
004D5494 61 72 79 41 00 00 00 00 47 65 74 50 72
004D54A4 64 64 72 65 73 73 00 00 00 00 56 69 72
004D54B4 6C 50 72 6F 74 65 63 74 00 00 00 00 4D
004D54C4 61 67 65 42 6F 78 41 00 00 00 77 73 70
004D54D4 74 66 41 00 00 00 52 65 67 43 6C 6F 73
004D54E4 79 00 00 00 53 79 73 46 72 65 65 53 74
004D54F4 67 00 00 00 4C 6F 63 61 6C 41 6C 6C 6F
004D5504 00 00 52 65 67 46 6C 75 73 68 4B 65 79
004D5514 53 6C 65 65 70 00 00 00 53 61 76 65 44
004D5524 00 00 47 65 74 44 43 00 00 00 53 6C 65
004D5534 00 00 56 61 72 69 61 6E 74 43 6F 70 79
004D5544 4F 6C 65 44 72 61 77 00 00 00 47 65 74
004D5554 6F 72 49 6E 66 6F 00 00 00 00 49 6D 61
```

```
0012FEF0 ┌0012FF44 D ‡.  Pointer to next SEH reco
0012FEF4 │00462E8A è.F.  SE handler
0012FEF8 │0012FF18 ↑ ‡.
0012FEFC │00000000 ....
0012FF00 │00000000 ....
0012FF04 │012C1310 ▶‼,0
0012FF08 │00000000 ....
0012FF0C │00000000 ....
0012FF10 │01000000 ...0
0012FF14 │012C1310 ▶‼,0
0012FF18 │0012FF6C l ‡.
0012FF1C └004624E4 Σ$F.  RETURN from pq.00462D7C
0012FF20 ┌00170DF2 ≥.‡.
0012FF24 │00000113 ‼0..
0012FF28 │00000001 0...
0012FF2C │00000000 ....
```

OllyDbg PE Parsing

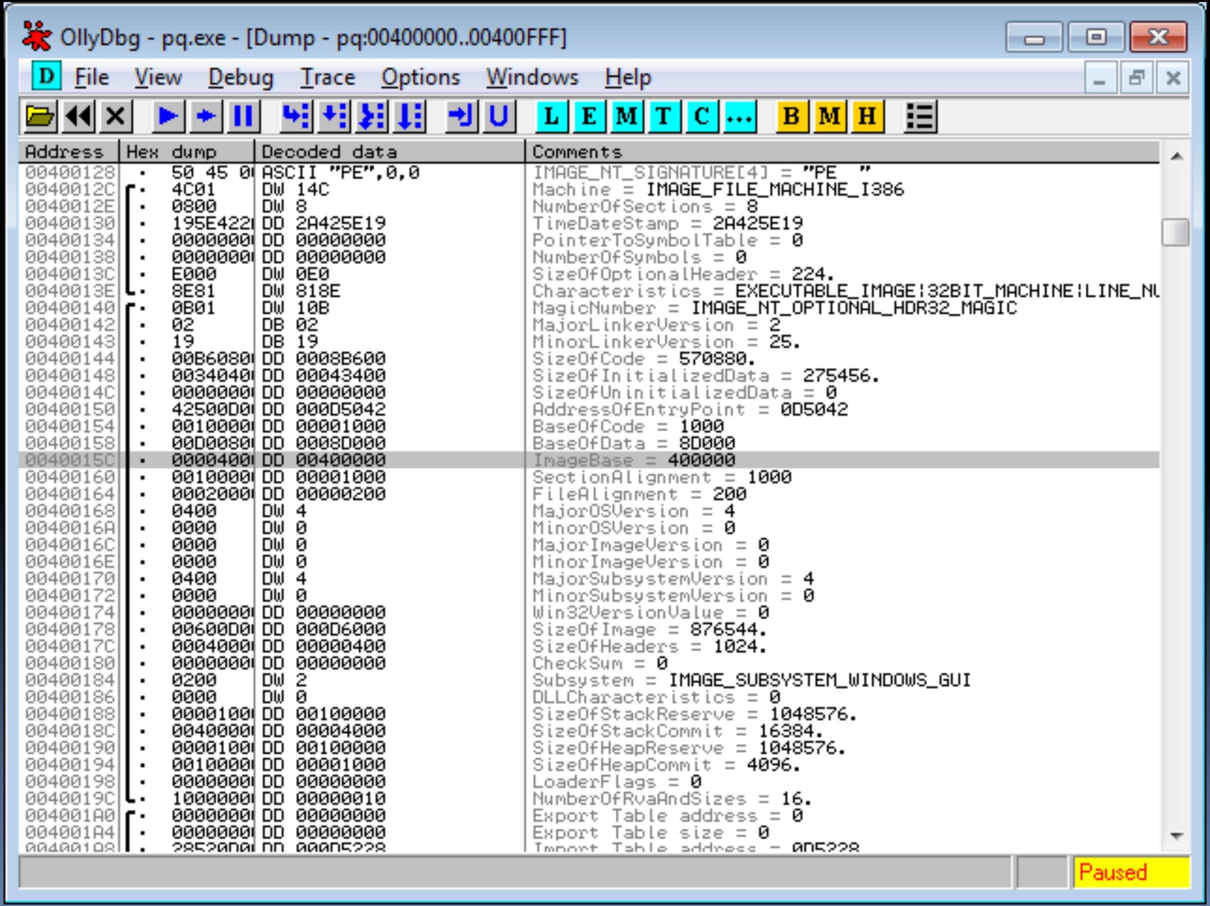
- Find where the PE header is mapped



Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	RW	RW	
00020000	00001000				Priv	RW	RW	
0011E000	00001000				Priv	RW Gua:	RW Gua:	
0011F000	00011000			Stack of main thr	Priv	RW	RW	
00130000	00004000				Map	R	R	
00140000	00001000				Priv	RW	RW	
00150000	00001000				Priv	RW	RW	
00160000	00001000				Priv	RW	RW	
00170000	00001000				Map	R	R	
00180000	00001000				Priv	RWE	RWE	
00190000	00054000				Priv	RW	RW	
00290000	00067000				Map	R	R	\Device\HarddiskVolume2\l
00300000	0000B000				Map	R	R	
003C0000	00003000				Map	R	R	
003D0000	00007000				Priv	RW	RW	
003E0000	00001000				Map	R	R	
003F0000	00007000				Map	R	R	
00400000	00001000	pq		PE header	Img	R	RWE Cop	
00401000	00090000	pq	<Sect_0>	Code	Img	RWE	RWE Cop	
00491000	00001000	pq	<Sect_1>		Img	RW	RWE Cop	
00492000	00003000	pq	<Sect_2>	Data	Img	RW	RWE Cop	
00495000	00001000	pq	<Sect_3>		Img	RW	RWE Cop	
00496000	00001000	pq	<Sect_4>		Img	R	RWE Cop	
00497000	0000A000	pq	<Sect_5>		Img	RW Cop	RWE Cop	
004A1000	00034000	pq	.petite	Resources	Img	RW Cop	RWE Cop	
004D5000	00001000	pq	<Sect_7>	SFX,imports	Img	RWE	RWE Cop	
004E0000	00101000			GDI handles	Map	R	R	
005F0000	000E0000				Map	R	R	
011F0000	00002000				Map	RW	RW	
01200000	00002000				Map	R	R	
01210000	00001000				Priv	RW	RW	
01220000	00002000				Map	R	R	
01230000	00003000				Priv	RW	RW	
01240000	00001000				Map	RW	RW	
01250000	00022000				Priv	RW	RW	
01280000	00001000				Map	RW Cop	RW Cop	\Device\HarddiskVolume2\l
01290000	00001000				Map	R	R	
012A0000	00001000				Map	R	R	
012B0000	00001000				Priv	RW	RW	
012C0000	0002C000				Priv	RW		
013C0000	00006000				Map	R	R	\Device\HarddiskVolume2\l

OllyDbg PE Parsing

- Double-click to view the PE Header dump

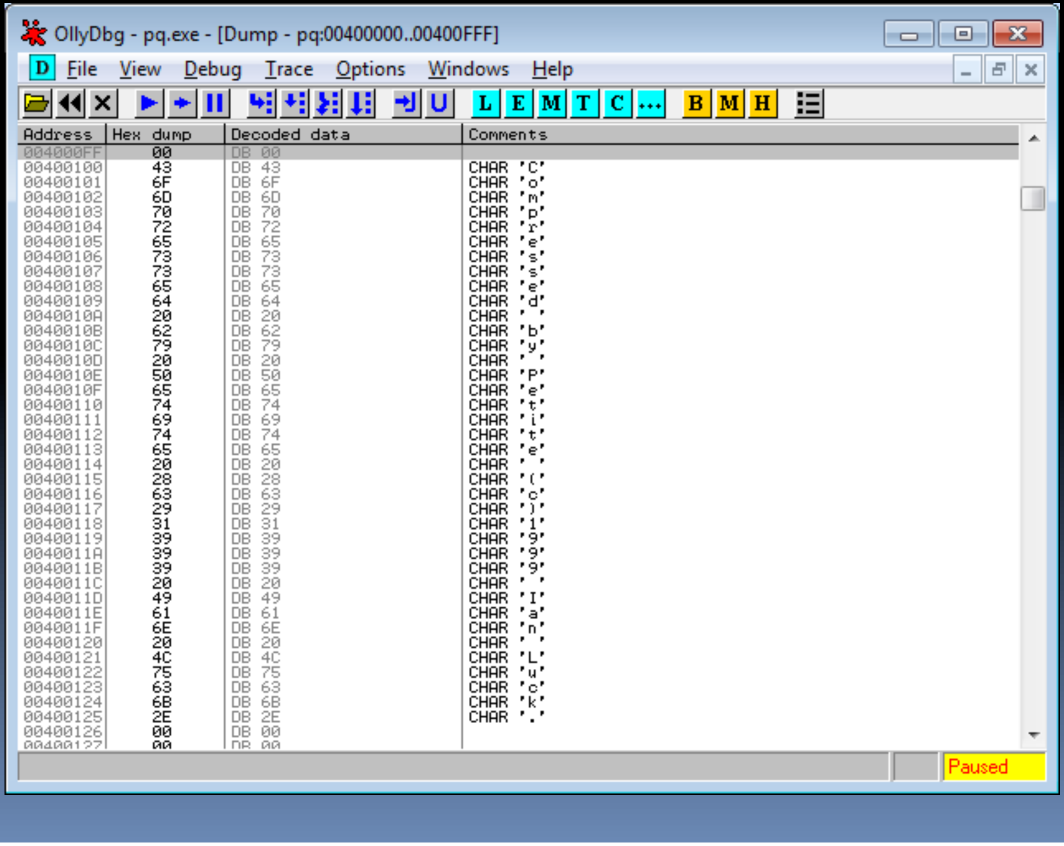


OllyDbg - pq.exe - [Dump - pq:00400000..00400FFF]
D File View Debug Trace Options Windows Help
L E M T C ... B M H
Paused

```
Address  Hex dump    Decoded data       Comments
00400128  .  50 45 0  ASCII "PE",0,0     IMAGE_NT_SIGNATURE[4] = "PE  "
0040012C  .  4C01     DW 14C             Machine = IMAGE_FILE_MACHINE_I386
0040012E  .  0800     DW 8               NumberOfSections = 8
00400130  .  195E422  DD 2A425E19        TimeDateStamp = 2A425E19
00400134  .  0000000  DD 00000000        PointerToSymbolTable = 0
00400138  .  0000000  DD 00000000        NumberOfSymbols = 0
0040013C  .  E000     DW 0E0             SizeOfOptionalHeader = 224.
0040013E  .  8E81     DW 818E            Characteristics = EXECUTABLE_IMAGE|32BIT_MACHINE|LINE_NU
00400140  .  0B01     DW 10B             MagicNumber = IMAGE_NT_OPTIONAL_HDR32_MAGIC
00400142  .  02       DB 02              MajorLinkerVersion = 2
00400143  .  19       DB 19              MinorLinkerVersion = 25.
00400144  .  00B6080  DD 0008B600        SizeOfCode = 570880.
00400148  .  0034040  DD 00043400        SizeOfInitializedData = 275456.
0040014C  .  0000000  DD 00000000        SizeOfUninitializedData = 0
00400150  .  42500D0  DD 000D5042        AddressOfEntryPoint = 0D5042
00400154  .  0010000  DD 00001000        BaseOfCode = 1000
00400158  .  00D0080  DD 0008D000        BaseOfData = 8D000
0040015C  .  0000400  DD 00400000        ImageBase = 400000
00400160  .  0010000  DD 00001000        SectionAlignment = 1000
00400164  .  0002000  DD 00000200        FileAlignment = 200
00400168  .  0400     DW 4               MajorOSVersion = 4
0040016A  .  0000     DW 0               MinorOSVersion = 0
0040016C  .  0000     DW 0               MajorImageVersion = 0
0040016E  .  0000     DW 0               MinorImageVersion = 0
00400170  .  0400     DW 4               MajorSubsystemVersion = 4
00400172  .  0000     DW 0               MinorSubsystemVersion = 0
00400174  .  0000000  DD 00000000        Win32VersionValue = 0
00400178  .  00600D0  DD 000D6000        SizeOfImage = 876544.
0040017C  .  0004000  DD 00000400        SizeOfHeaders = 1024.
00400180  .  0000000  DD 00000000        CheckSum = 0
00400184  .  0200     DW 2               Subsystem = IMAGE_SUBSYSTEM_WINDOWS_GUI
00400186  .  0000     DW 0               DLLCharacteristics = 0
00400188  .  0000100  DD 00100000        SizeOfStackReserve = 1048576.
0040018C  .  0040000  DD 00004000        SizeOfStackCommit = 16384.
00400190  .  0000100  DD 00100000        SizeOfHeapReserve = 1048576.
00400194  .  0010000  DD 00001000        SizeOfHeapCommit = 4096.
00400198  .  0000000  DD 00000000        LoaderFlags = 0
0040019C  .  1000000  DD 00000010        NumberOfRvaAndSizes = 16.
004001A0  .  0000000  DD 00000000        Export Table address = 0
004001A4  .  0000000  DD 00000000        Export Table size = 0
004001A8  .  28520D0  DD 000D5228        Import Table address = 0D5228
```

OllyDbg PE Parsing

- In this case, the compressor left behind some identifying information



```
Address   Hex dump    Decoded data                    Comments
004000FF      00      DB 00
00400100      43      DB 43                           CHAR 'C'
00400101      6F      DB 6F                           CHAR 'o'
00400102      6D      DB 6D                           CHAR 'm'
00400103      70      DB 70                           CHAR 'p'
00400104      72      DB 72                           CHAR 'r'
00400105      65      DB 65                           CHAR 'e'
00400106      73      DB 73                           CHAR 's'
00400107      73      DB 73                           CHAR 's'
00400108      65      DB 65                           CHAR 'e'
00400109      64      DB 64                           CHAR 'd'
0040010A      20      DB 20                           CHAR ' '
0040010B      62      DB 62                           CHAR 'b'
0040010C      79      DB 79                           CHAR 'y'
0040010D      20      DB 20                           CHAR ' '
0040010E      50      DB 50                           CHAR 'P'
0040010F      65      DB 65                           CHAR 'e'
00400110      74      DB 74                           CHAR 't'
00400111      69      DB 69                           CHAR 'i'
00400112      74      DB 74                           CHAR 't'
00400113      65      DB 65                           CHAR 'e'
00400114      20      DB 20                           CHAR ' '
00400115      28      DB 28                           CHAR '('
00400116      63      DB 63                           CHAR 'c'
00400117      29      DB 29                           CHAR ')'
00400118      31      DB 31                           CHAR '1'
00400119      39      DB 39                           CHAR '9'
0040011A      39      DB 39                           CHAR '9'
0040011B      39      DB 39                           CHAR '9'
0040011C      20      DB 20                           CHAR ' '
0040011D      49      DB 49                           CHAR 'I'
0040011E      61      DB 61                           CHAR 'a'
0040011F      6E      DB 6E                           CHAR 'n'
00400120      20      DB 20                           CHAR ' '
00400121      4C      DB 4C                           CHAR 'L'
00400122      75      DB 75                           CHAR 'u'
00400123      63      DB 63                           CHAR 'c'
00400124      6B      DB 6B                           CHAR 'k'
00400125      2E      DB 2E                           CHAR '.'
00400126      00      DB 00
00400127      00      DB 00
```

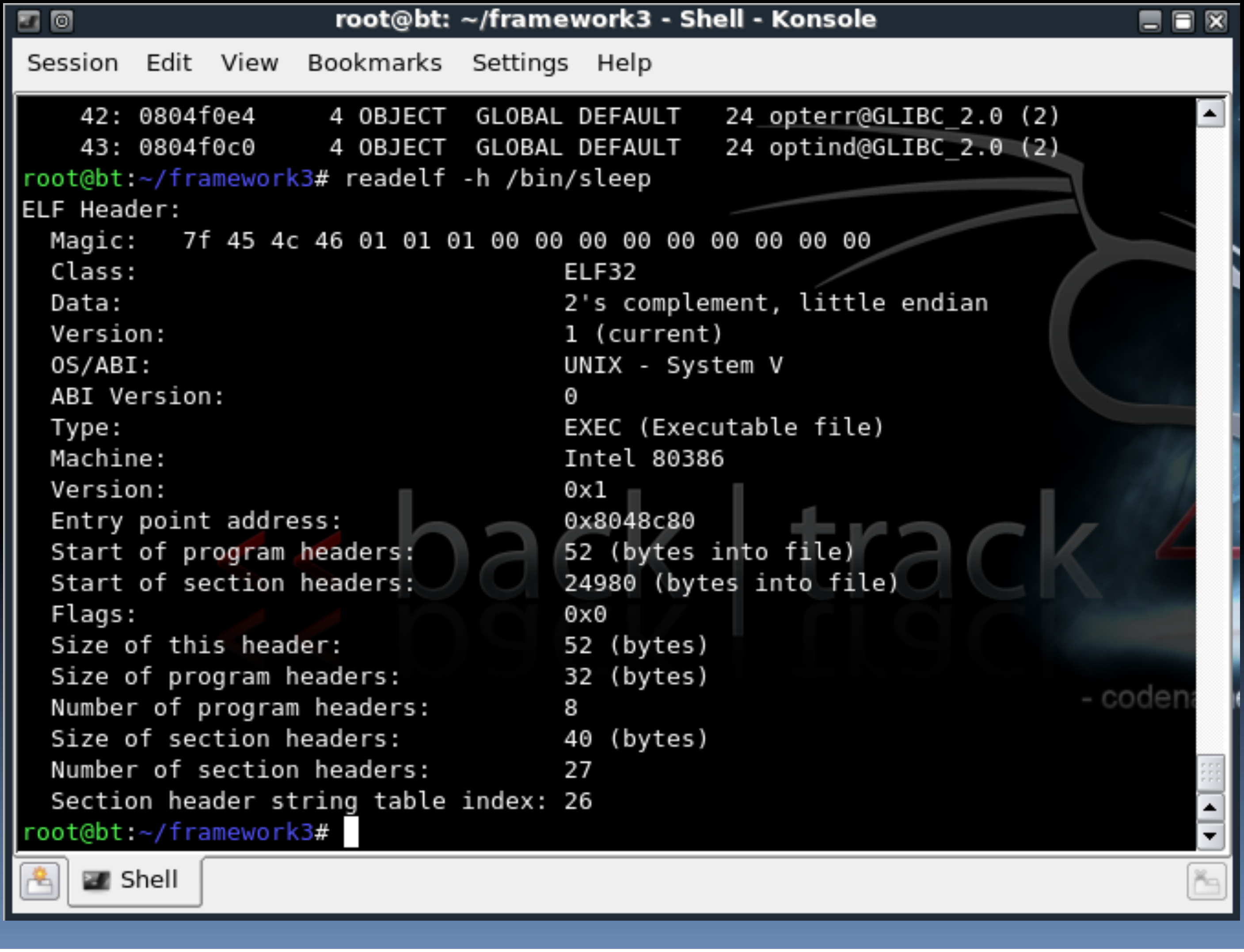
ELF

- Executable and Linkable Format
  - Executable file format of choice for Linux
  - none, .o, .so, .elf, .exe

ELF Construction

- ELF Header
- Program Header Table
  - Describes segments
- Section Header Table
  - Describes sections

readelf



root@bt: ~/framework3 - Shell - Konsole
Session Edit View Bookmarks Settings Help
Shell

```
    42: 0804f0e4     4 OBJECT  GLOBAL DEFAULT   24 opterr@GLIBC_2.0 (2)
    43: 0804f0c0     4 OBJECT  GLOBAL DEFAULT   24 optind@GLIBC_2.0 (2)
root@bt:~/framework3# readelf -h /bin/sleep
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF32
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              EXEC (Executable file)
  Machine:                           Intel 80386
  Version:                           0x1
  Entry point address:               0x8048c80
  Start of program headers:          52 (bytes into file)
  Start of section headers:          24980 (bytes into file)
  Flags:                             0x0
  Size of this header:               52 (bytes)
  Size of program headers:           32 (bytes)
  Number of program headers:         8
  Size of section headers:           40 (bytes)
  Number of section headers:         27
  Section header string table index: 26
root@bt:~/framework3# 
```

Questions/Comments?