Analyzing Files Statically

Dr. Jared DeMott
SECURITY RESEARCHER AND ENGINEER

@jareddemott   www.vdalabs.com

Overview

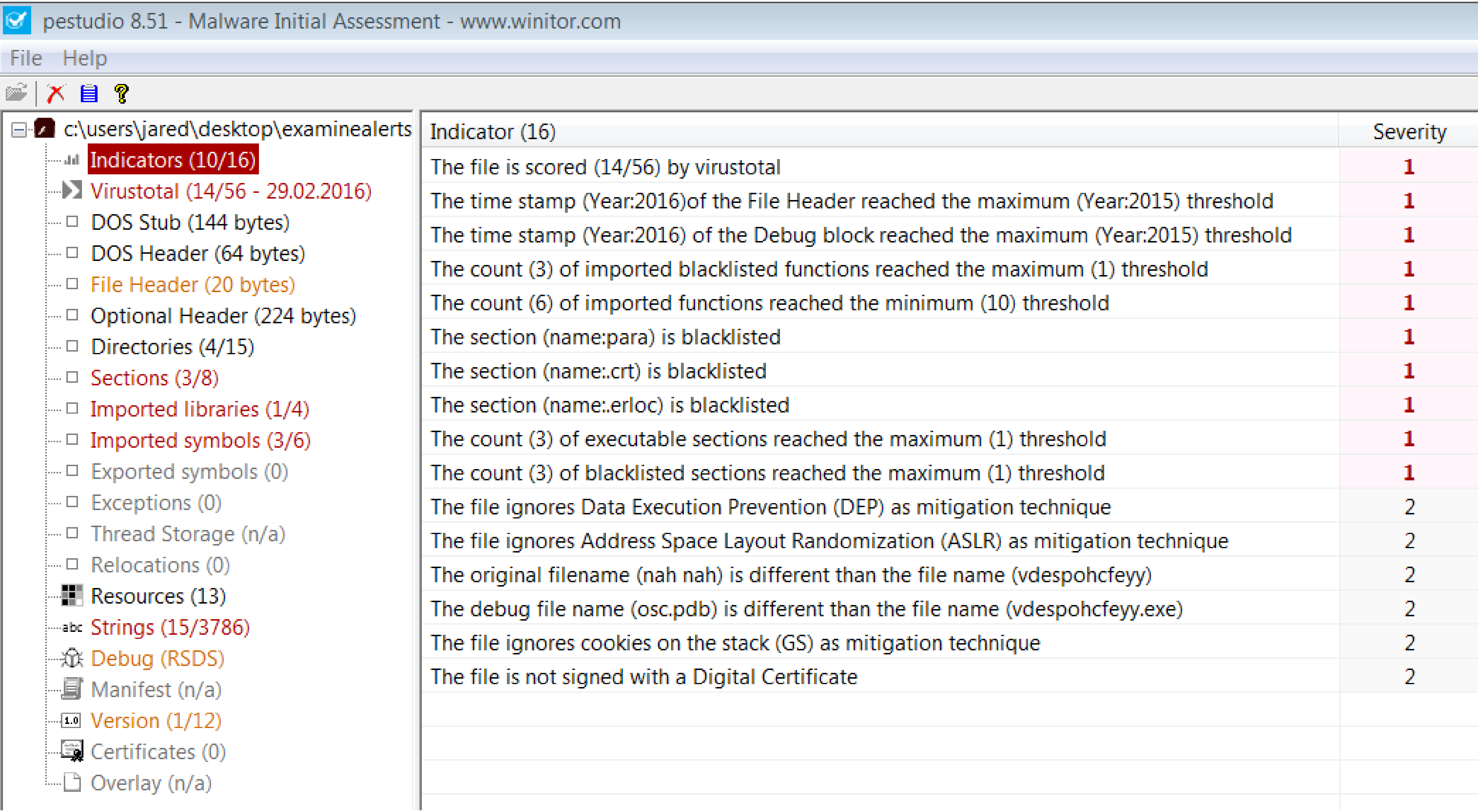
Static File Analysis

- Tools
- Techniques
- Malware Template Report

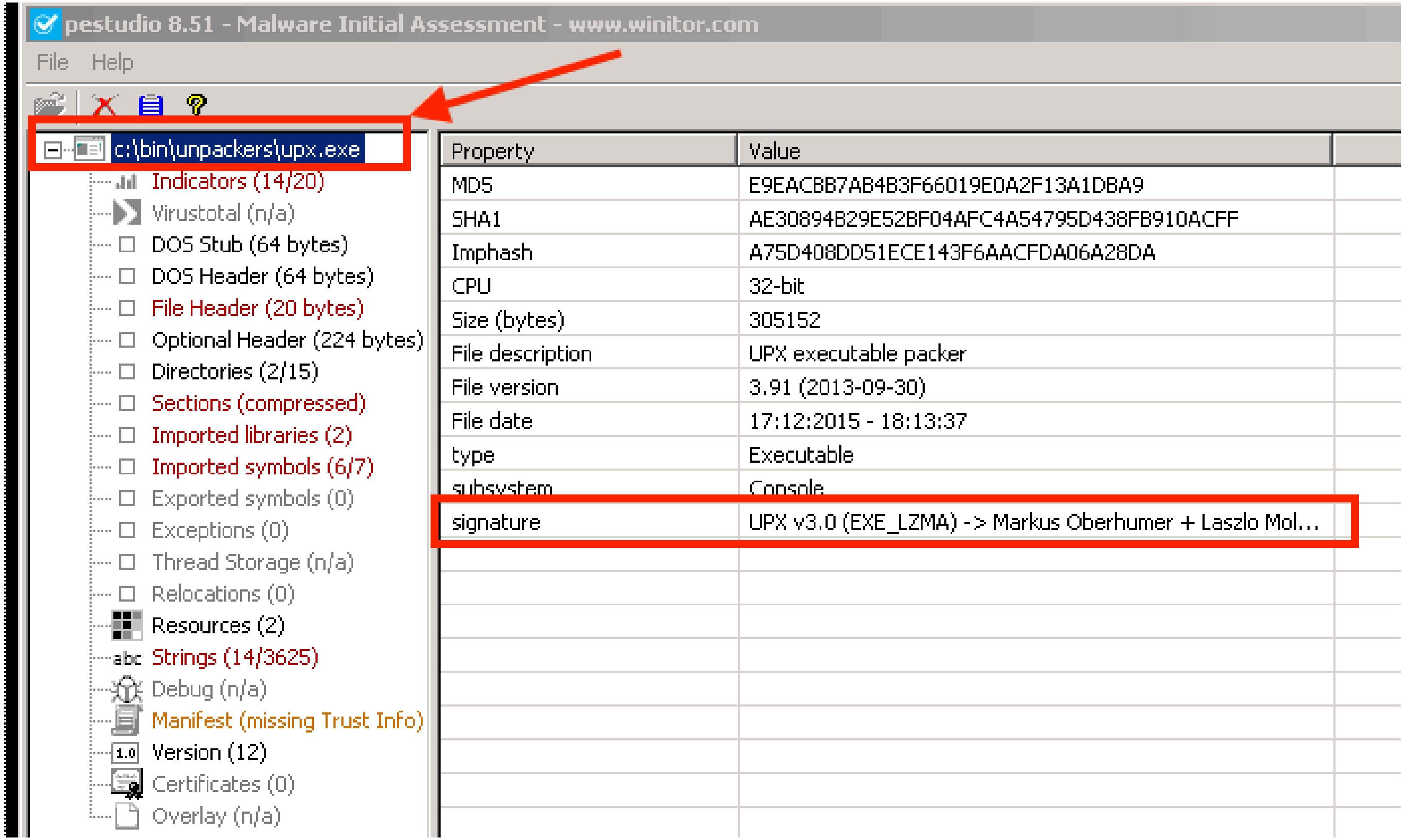
pestudio

Assess

- Unusual File attributes
- Safe



Indicator (16)	Severity
The file is scored (14/56) by virustotal	1
The time stamp (Year:2016)of the File Header reached the maximum (Year:2015) threshold	1
The time stamp (Year:2016) of the Debug block reached the maximum (Year:2015) threshold	1
The count (3) of imported blacklisted functions reached the maximum (1) threshold	1
The count (6) of imported functions reached the minimum (10) threshold	1
The section (name:para) is blacklisted	1
The section (name:.crt) is blacklisted	1
The section (name:.erloc) is blacklisted	1
The count (3) of executable sections reached the maximum (1) threshold	1
The count (3) of blacklisted sections reached the maximum (1) threshold	1
The file ignores Data Execution Prevention (DEP) as mitigation technique	2
The file ignores Address Space Layout Randomization (ASLR) as mitigation technique	2
The original filename (nah nah) is different than the file name (vdespohcfeyy)	2
The debug file name (osc.pdb) is different than the file name (vdespohcfeyy.exe)	2
The file ignores cookies on the stack (GS) as mitigation technique	2
The file is not signed with a Digital Certificate	2



c:\bin\unpackers\upx.exe

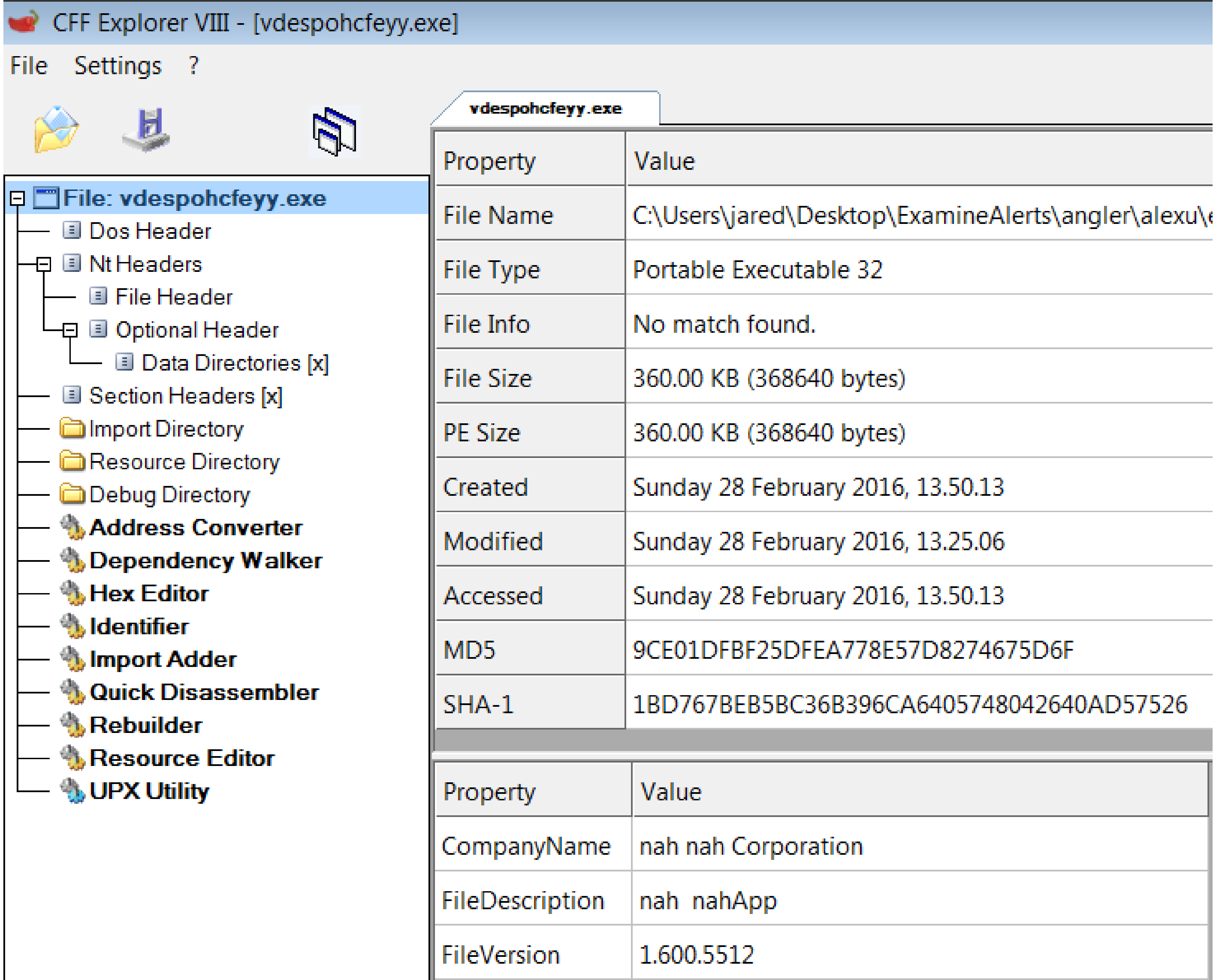
Property	Value
MD5	E9EACBB7AB4B3F66019E0A2F13A1DBA9
SHA1	AE30894B29E52BF04AFC4A54795D438FB910ACFF
Imphash	A75D408DD51ECE143F6AACFDA06A28DA
CPU	32-bit
Size (bytes)	305152
File description	UPX executable packer
File version	3.91 (2013-09-30)
File date	17:12:2015 - 18:13:37
type	Executable
subsystem	Console
signature	UPX v3.0 (EXE_LZMA) -> Markus Oberhumer + Laszlo Mol...

Malware Obfuscation

Packer

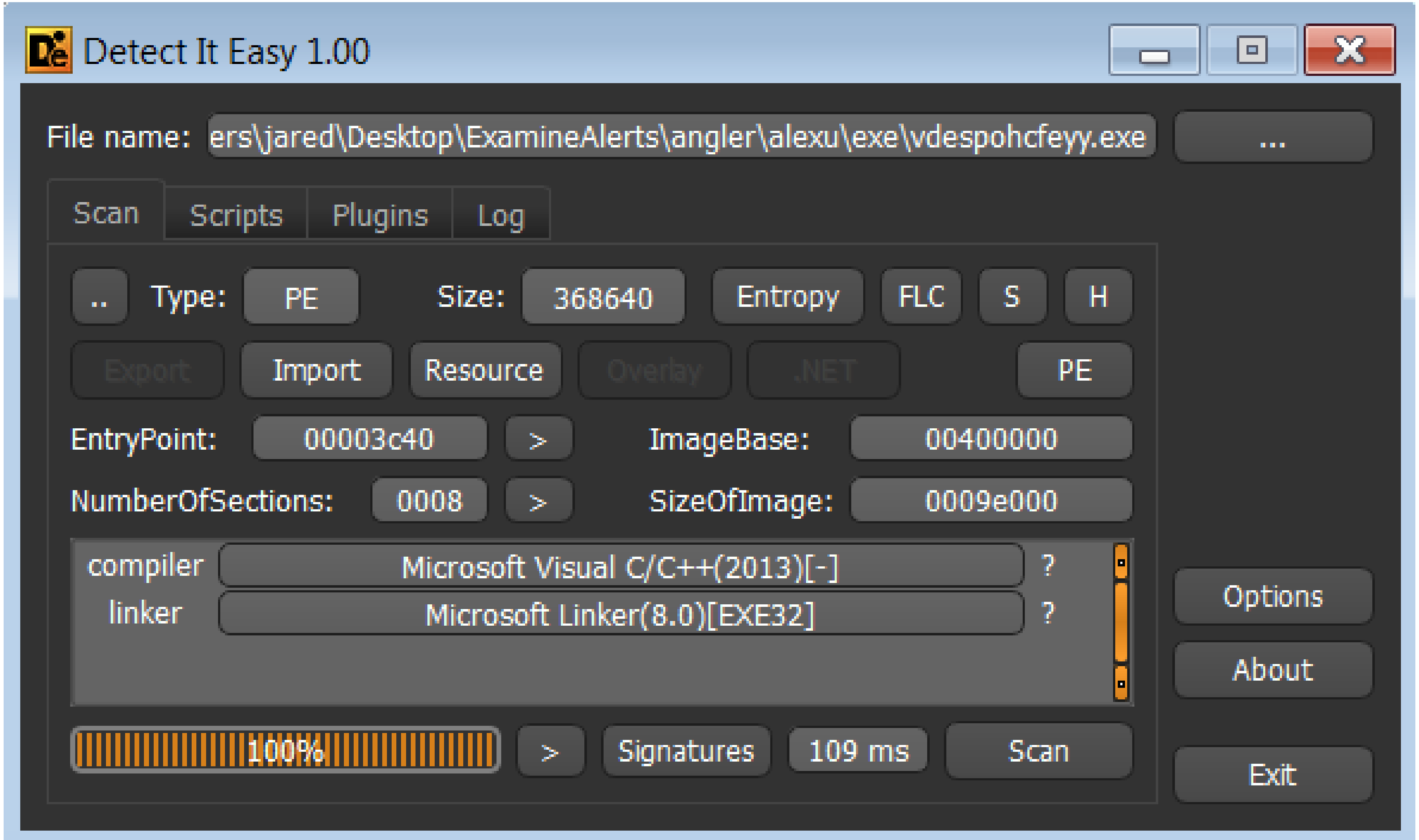
```
LODS BYTE PTR DS:[ESI]
MOV EBX,EDX
AND EBX,0FF
XOR BL,AL
SHR EDX,8
AND EDX,0FFFFFF
PUSH ECX
MOV ECX,8
SHR EBX,1
JNB SHORT skype.004012B6
XOR EBX,EDB88320
```

```
CALL DWORD PTR DS:[<&KERNEL32.
OR EAX,EAX
JNS SHORT skype.00401017
PUSH 1150
CALL DWORD PTR DS:[<&KERNEL32.
D PTR DS:[<&KERNEL32.
PTR DS:[<&KERNEL32.
```



Property	Value
File Name	C:\Users\jared\Desktop\ExamineAlerts\angler\alexu\
File Type	Portable Executable 32
File Info	No match found.
File Size	360.00 KB (368640 bytes)
PE Size	360.00 KB (368640 bytes)
Created	Sunday 28 February 2016, 13.50.13
Modified	Sunday 28 February 2016, 13.25.06
Accessed	Sunday 28 February 2016, 13.50.13
MD5	9CE01DFBF25DFEA778E57D8274675D6F
SHA-1	1BD767BEB5BC36B396CA6405748042640AD57526

Property	Value
CompanyName	nah nah Corporation
FileDescription	nah nahApp
FileVersion	1.600.5512



Detect It Easy 1.00

File name: ers\jared\Desktop\ExamineAlerts\angler\alexu\exe\vdespohcfeyy.exe

Type: PE

Size: 368640

EntryPoint: 00003c40

ImageBase: 00400000

NumberOfSections: 0008

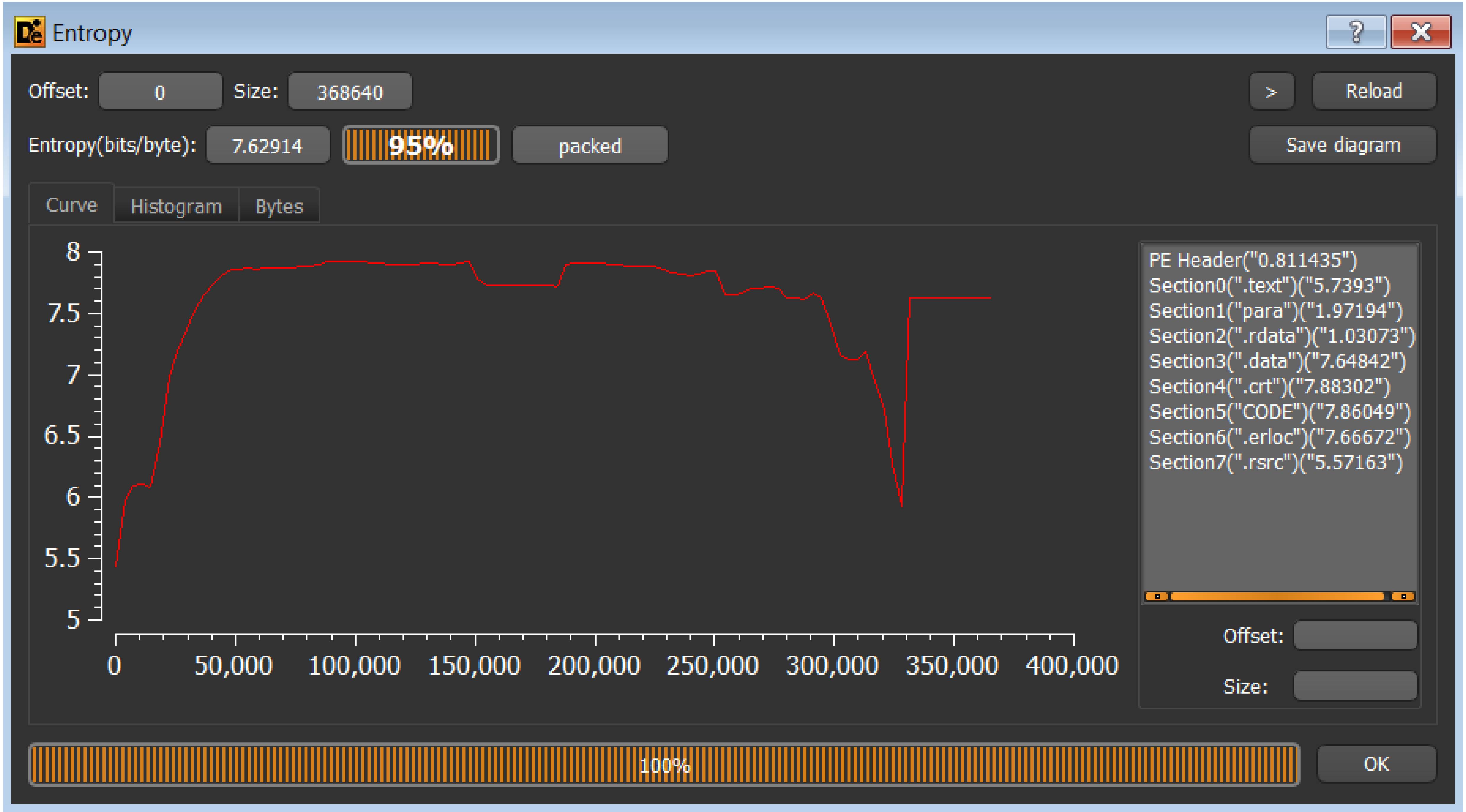
SizeOfImage: 0009e000

compiler Microsoft Visual C/C++(2013)[-] ?

linker Microsoft Linker(8.0)[EXE32] ?

100%

109 ms



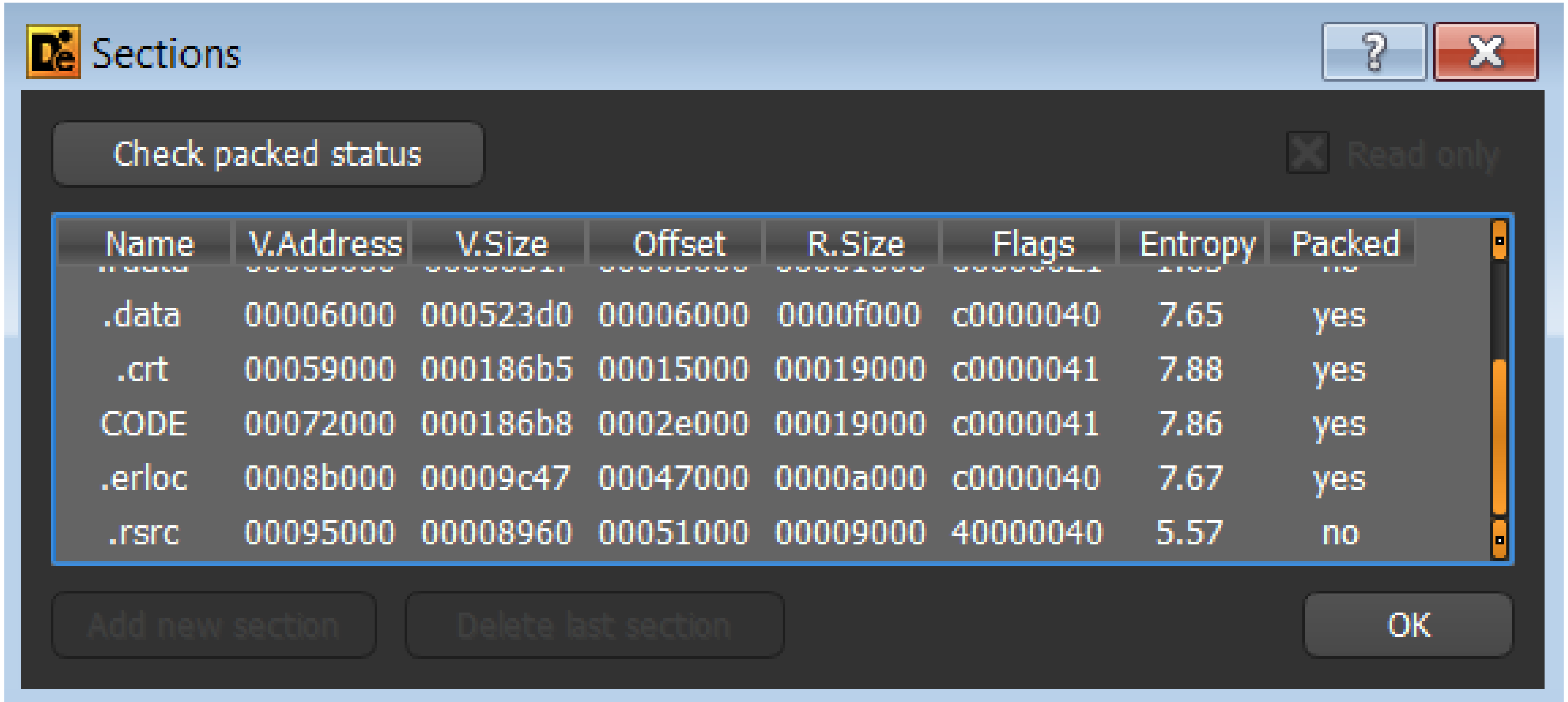
Offset: 0 Size: 368640

Entropy(bits/byte): 7.62914 95% packed

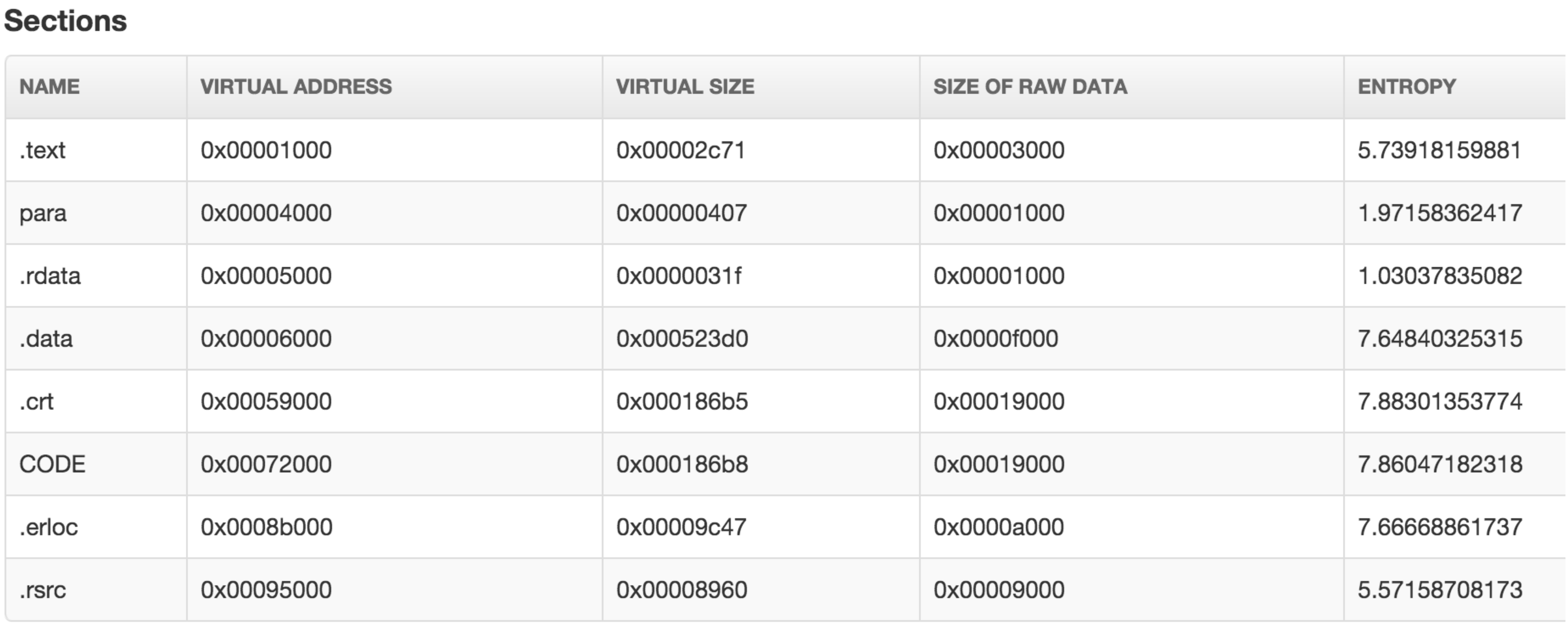
PE Header("0.811435")
Section0(".text")("5.7393")
Section1("para")("1.97194")
Section2(".rdata")("1.03073")
Section3(".data")("7.64842")
Section4(".crt")("7.88302")
Section5("CODE")("7.86049")
Section6(".erloc")("7.66672")
Section7(".rsrc")("5.57163")

Offset:

Size:

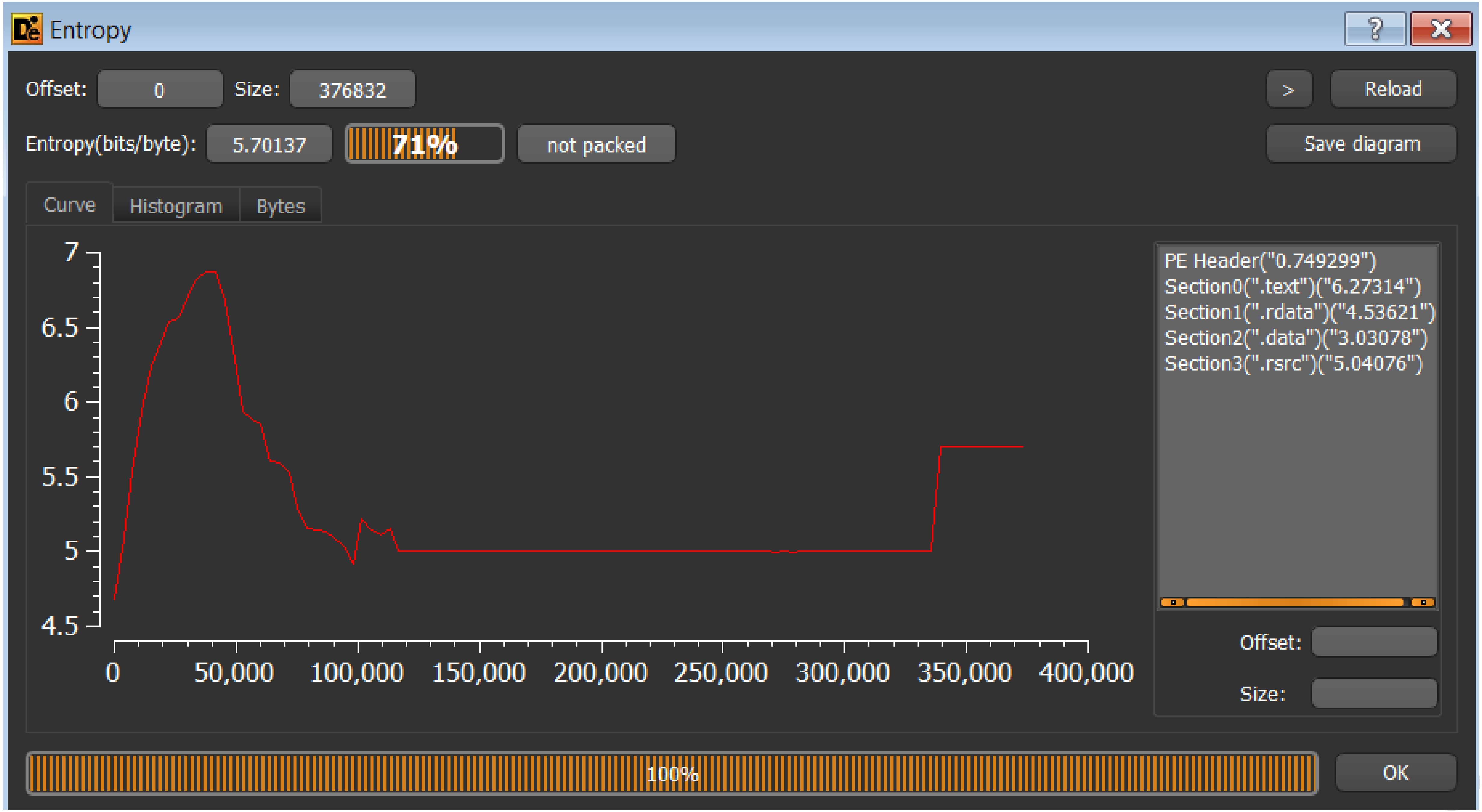


Name	V.Address	V.Size	Offset	R.Size	Flags	Entropy	Packed
.data	00006000	000523d0	00006000	0000f000	c0000040	7.65	yes
.crt	00059000	000186b5	00015000	00019000	c0000041	7.88	yes
CODE	00072000	000186b8	0002e000	00019000	c0000041	7.86	yes
.erloc	0008b000	00009c47	00047000	0000a000	c0000040	7.67	yes
.rsrc	00095000	00008960	00051000	00009000	40000040	5.57	no



Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	SIZE OF RAW DATA	ENTROPY
.text	0x00001000	0x00002c71	0x00003000	5.73918159881
para	0x00004000	0x00000407	0x00001000	1.97158362417
.rdata	0x00005000	0x0000031f	0x00001000	1.03037835082
.data	0x00006000	0x000523d0	0x0000f000	7.64840325315
.crt	0x00059000	0x000186b5	0x00019000	7.88301353774
CODE	0x00072000	0x000186b8	0x00019000	7.86047182318
.erloc	0x0008b000	0x00009c47	0x0000a000	7.66668861737
.rsrc	0x00095000	0x00008960	0x00009000	5.57158708173



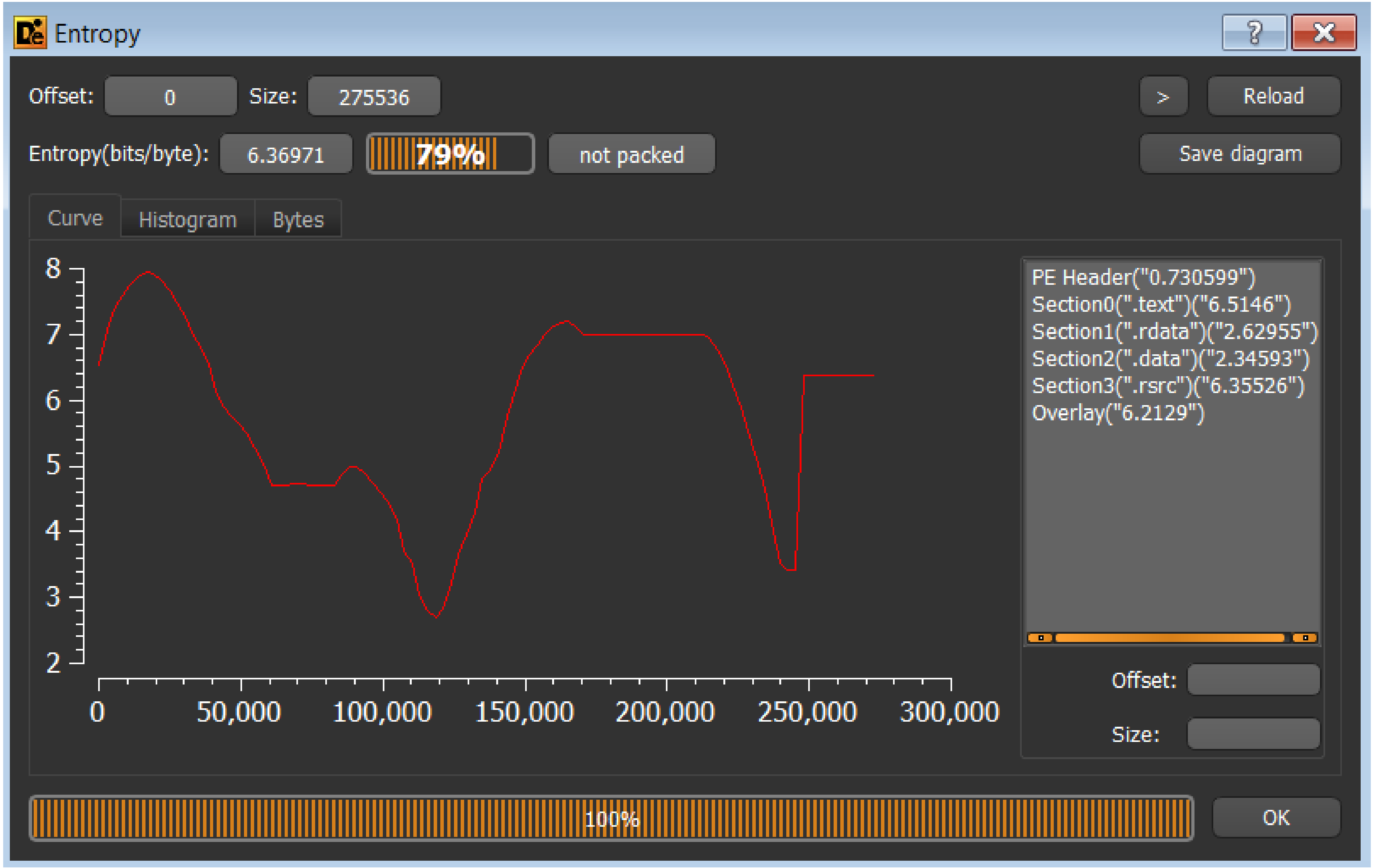
Offset: 0 Size: 376832

Entropy(bits/byte): 5.70137 71% not packed

PE Header("0.749299")
Section0(".text")("6.27314")
Section1(".rdata")("4.53621")
Section2(".data")("3.03078")
Section3(".rsrc")("5.04076")

Offset:

Size:



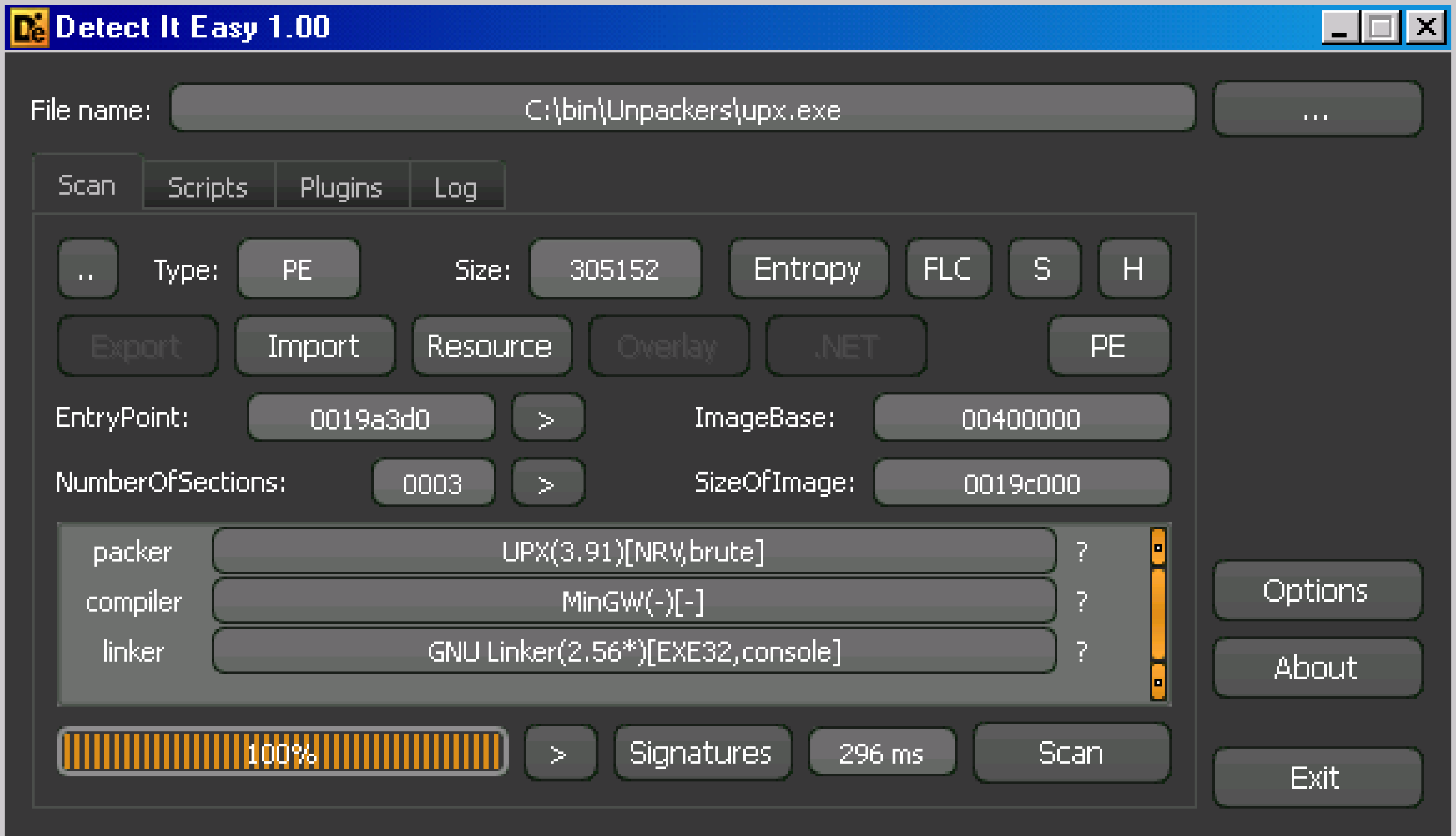
Offset: 0 Size: 275536

Entropy(bits/byte): 6.36971 79% not packed

PE Header("0.730599")
Section0(".text")("6.5146")
Section1(".rdata")("2.62955")
Section2(".data")("2.34593")
Section3(".rsrc")("6.35526")
Overlay("6.2129")

Offset:

Size:



File name: C:\bin\Unpackers\upx.exe

Type: PE

Size: 305152

EntryPoint: 0019a3d0

ImageBase: 00400000

NumberOfSections: 0003

SizeOfImage: 0019c000

packer UPX(3.91)[NRV,brute]

compiler MinGW(-)[-]

linker GNU Linker(2.56*)[EXE32,console]

100%

296 ms

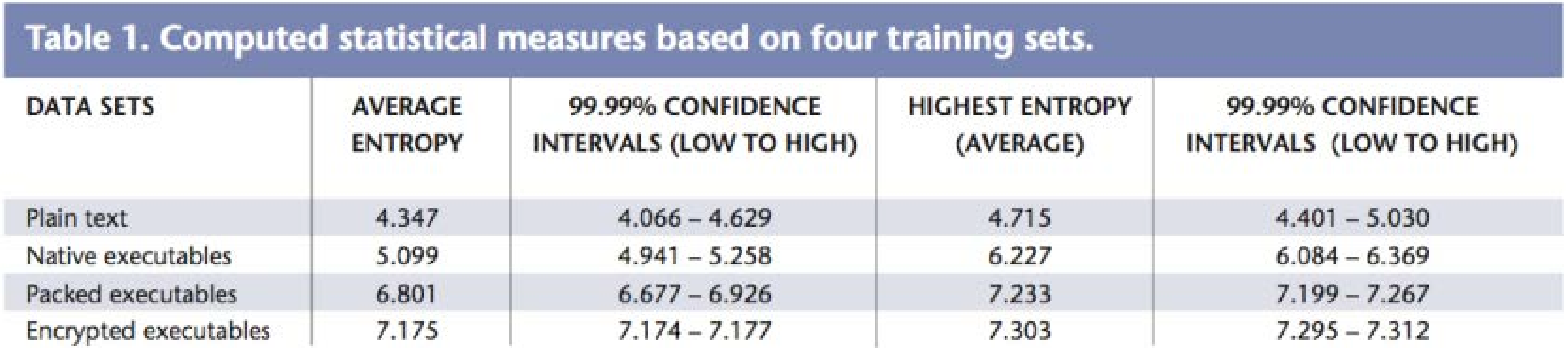
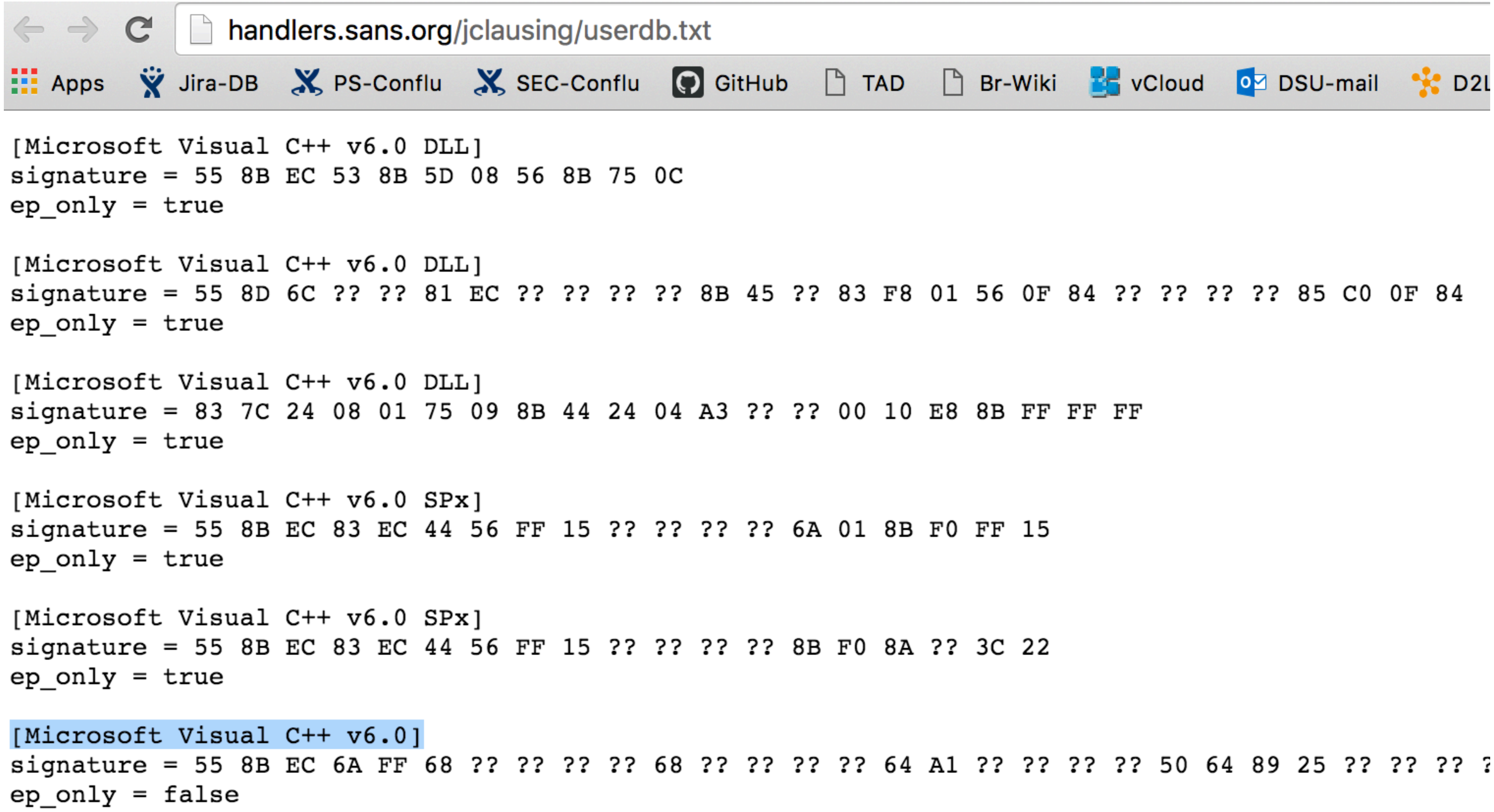
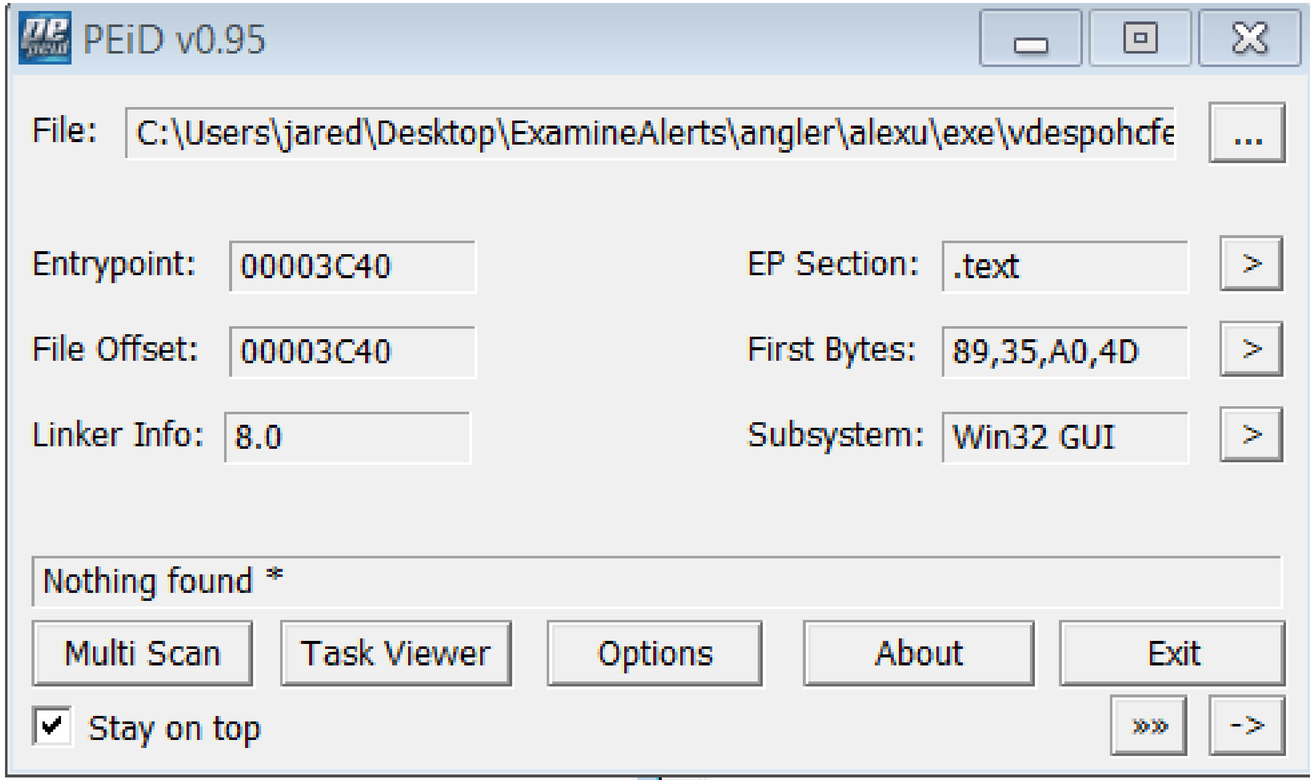


Table 1. Computed statistical measures based on four training sets.

DATA SETS	AVERAGE ENTROPY	99.99% CONFIDENCE INTERVALS (LOW TO HIGH)	HIGHEST ENTROPY (AVERAGE)	99.99% CONFIDENCE INTERVALS (LOW TO HIGH)
Plain text	4.347	4.066 – 4.629	4.715	4.401 – 5.030
Native executables	5.099	4.941 – 5.258	6.227	6.084 – 6.369
Packed executables	6.801	6.677 – 6.926	7.233	7.199 – 7.267
Encrypted executables	7.175	7.174 – 7.177	7.303	7.295 – 7.312



```
[Microsoft Visual C++ v6.0 DLL]
signature = 55 8B EC 53 8B 5D 08 56 8B 75 0C
ep_only = true

[Microsoft Visual C++ v6.0 DLL]
signature = 55 8D 6C ?? ?? 81 EC ?? ?? ?? ?? 8B 45 ?? 83 F8 01 56 0F 84 ?? ?? ?? ?? 85 C0 0F 84
ep_only = true

[Microsoft Visual C++ v6.0 DLL]
signature = 83 7C 24 08 01 75 09 8B 44 24 04 A3 ?? ?? 00 10 E8 8B FF FF FF
ep_only = true

[Microsoft Visual C++ v6.0 SPx]
signature = 55 8B EC 83 EC 44 56 FF 15 ?? ?? ?? ?? 6A 01 8B F0 FF 15
ep_only = true

[Microsoft Visual C++ v6.0 SPx]
signature = 55 8B EC 83 EC 44 56 FF 15 ?? ?? ?? ?? 8B F0 8A ?? 3C 22
ep_only = true

[Microsoft Visual C++ v6.0]
signature = 55 8B EC 6A FF 68 ?? ?? ?? ?? 68 ?? ?? ?? ?? 64 A1 ?? ?? ?? ?? 50 64 89 25 ?? ?? ?? ?
ep_only = false
```



File: C:\Users\jared\Desktop\ExamineAlerts\angler\alexu\exe\vdespohcfe

Entrypoint: 00003C40

File Offset: 00003C40

Linker Info: 8.0

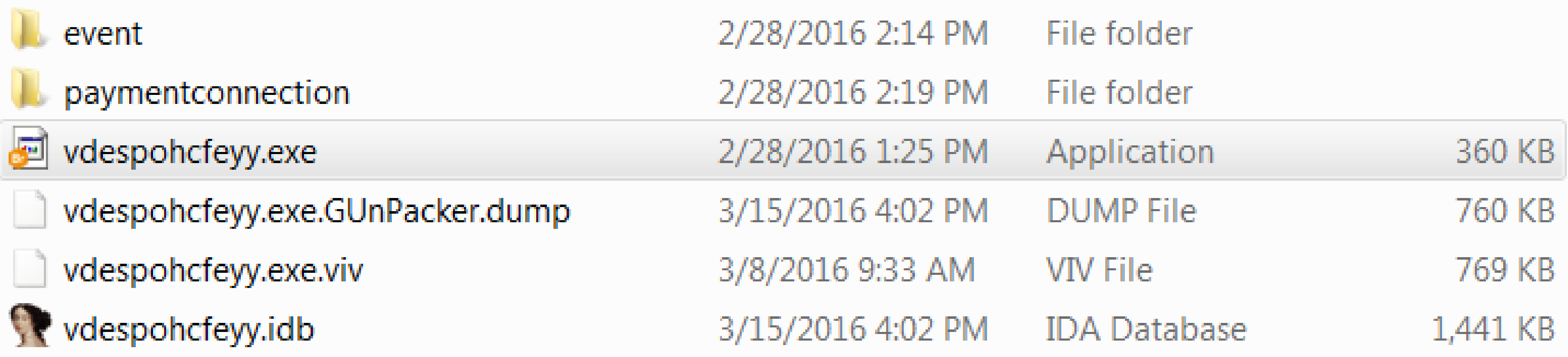
EP Section: .text

First Bytes: 89,35,A0,4D

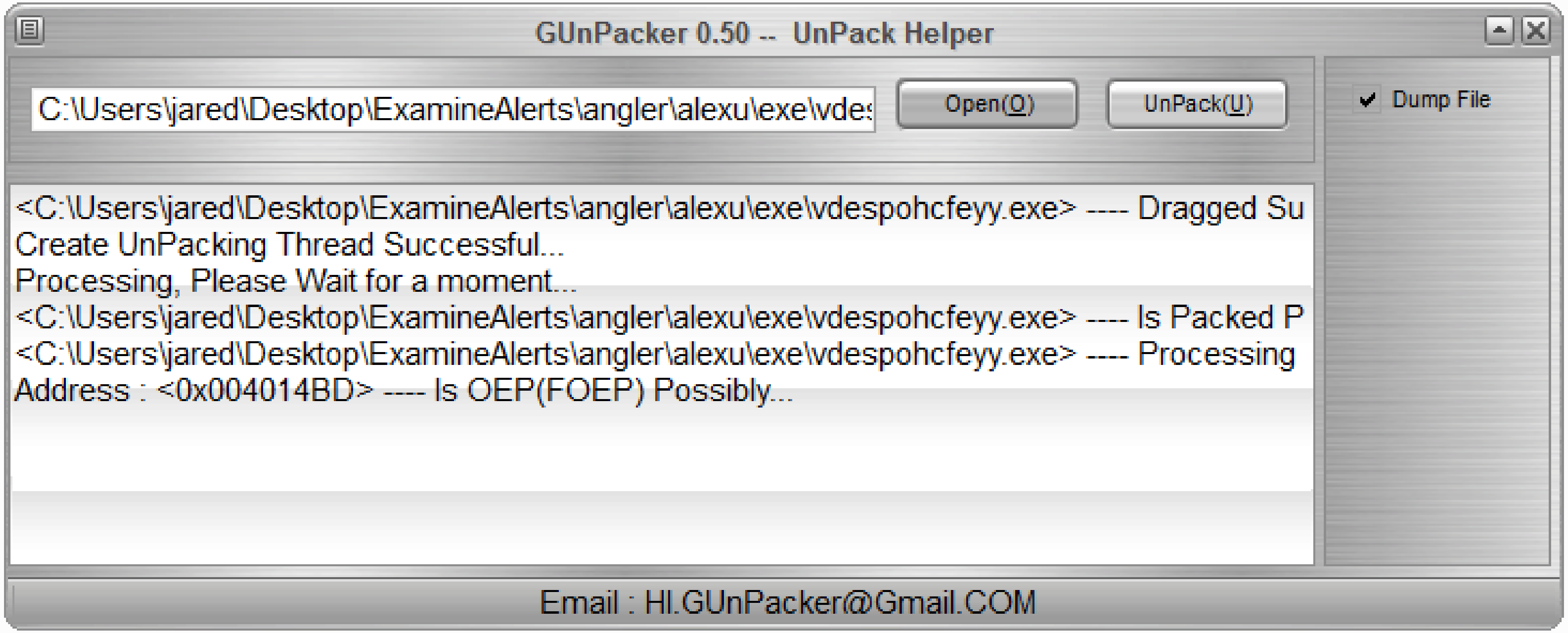
Subsystem: Win32 GUI

Nothing found *

☑ Stay on top



event	2/28/2016 2:14 PM	File folder	
paymentconnection	2/28/2016 2:19 PM	File folder	
vdespohcfeyy.exe	2/28/2016 1:25 PM	Application	360 KB
vdespohcfeyy.exe.GUnPacker.dump	3/15/2016 4:02 PM	DUMP File	760 KB
vdespohcfeyy.exe.viv	3/8/2016 9:33 AM	VIV File	769 KB
vdespohcfeyy.idb	3/15/2016 4:02 PM	IDA Database	1,441 KB

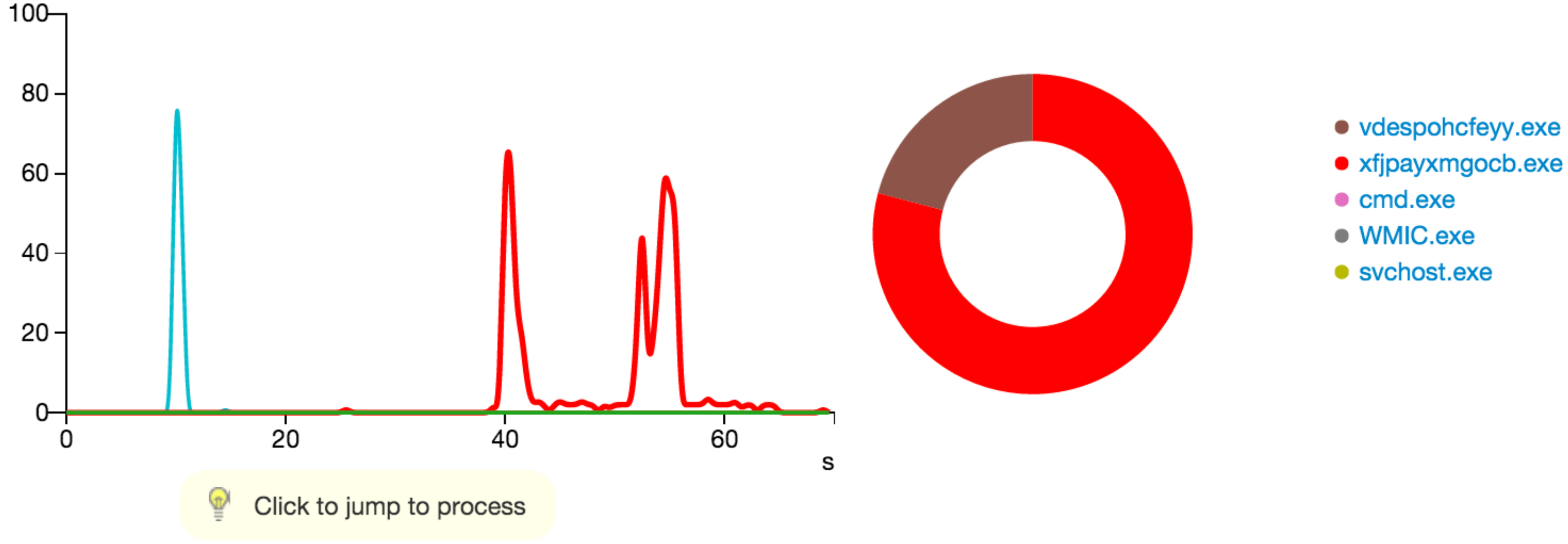


GUnPacker 0.50 -- UnPack Helper
C:\Users\jared\Desktop\ExamineAlerts\angler\alexu\exe\vdes
Open(O)
UnPack(U)
☑ Dump File

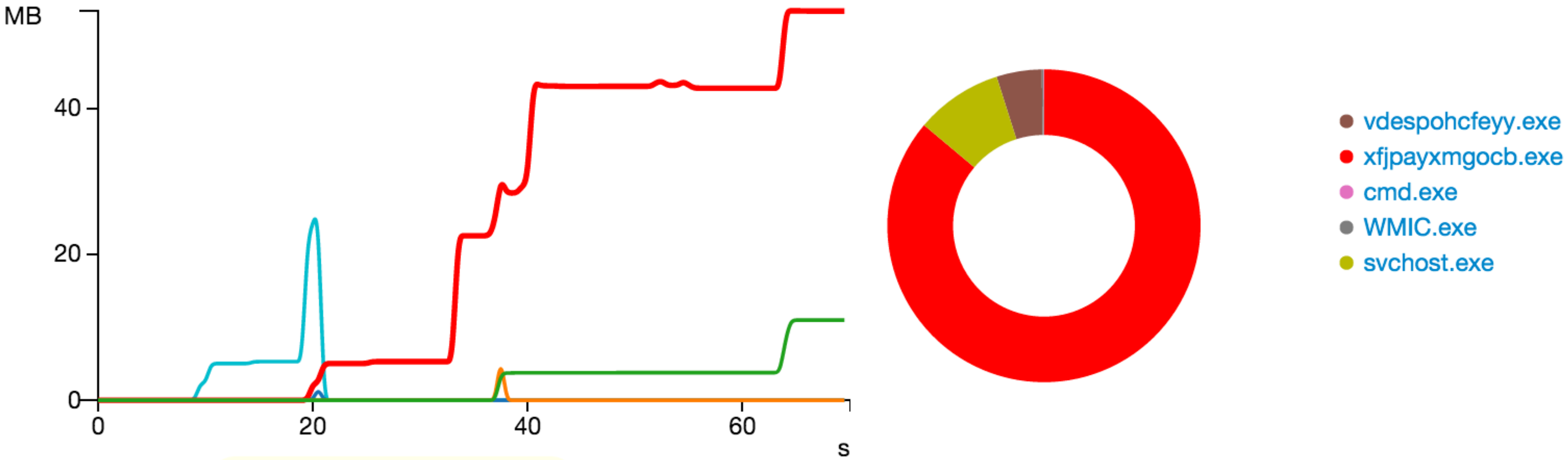
```
<C:\Users\jared\Desktop\ExamineAlerts\angler\alexu\exe\vdespohcfeyy.exe> ---- Dragged Su
Create UnPacking Thread Successful...
Processing, Please Wait for a moment...
<C:\Users\jared\Desktop\ExamineAlerts\angler\alexu\exe\vdespohcfeyy.exe> ---- Is Packed P
<C:\Users\jared\Desktop\ExamineAlerts\angler\alexu\exe\vdespohcfeyy.exe> ---- Processing
Address : <0x004014BD> ---- Is OEP(FOEP) Possibly...
```

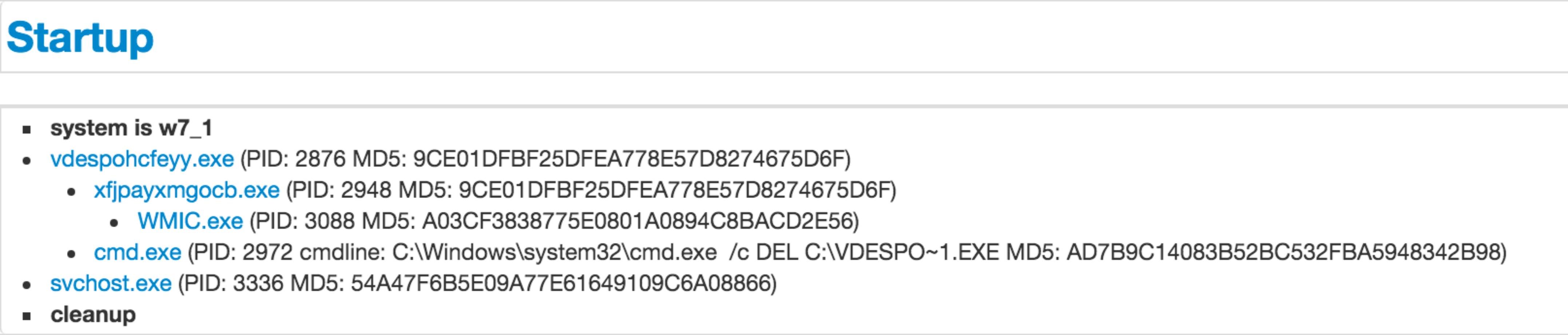
Email : HI.GUnPacker@Gmail.COM

CPU Usage



Memory Usage



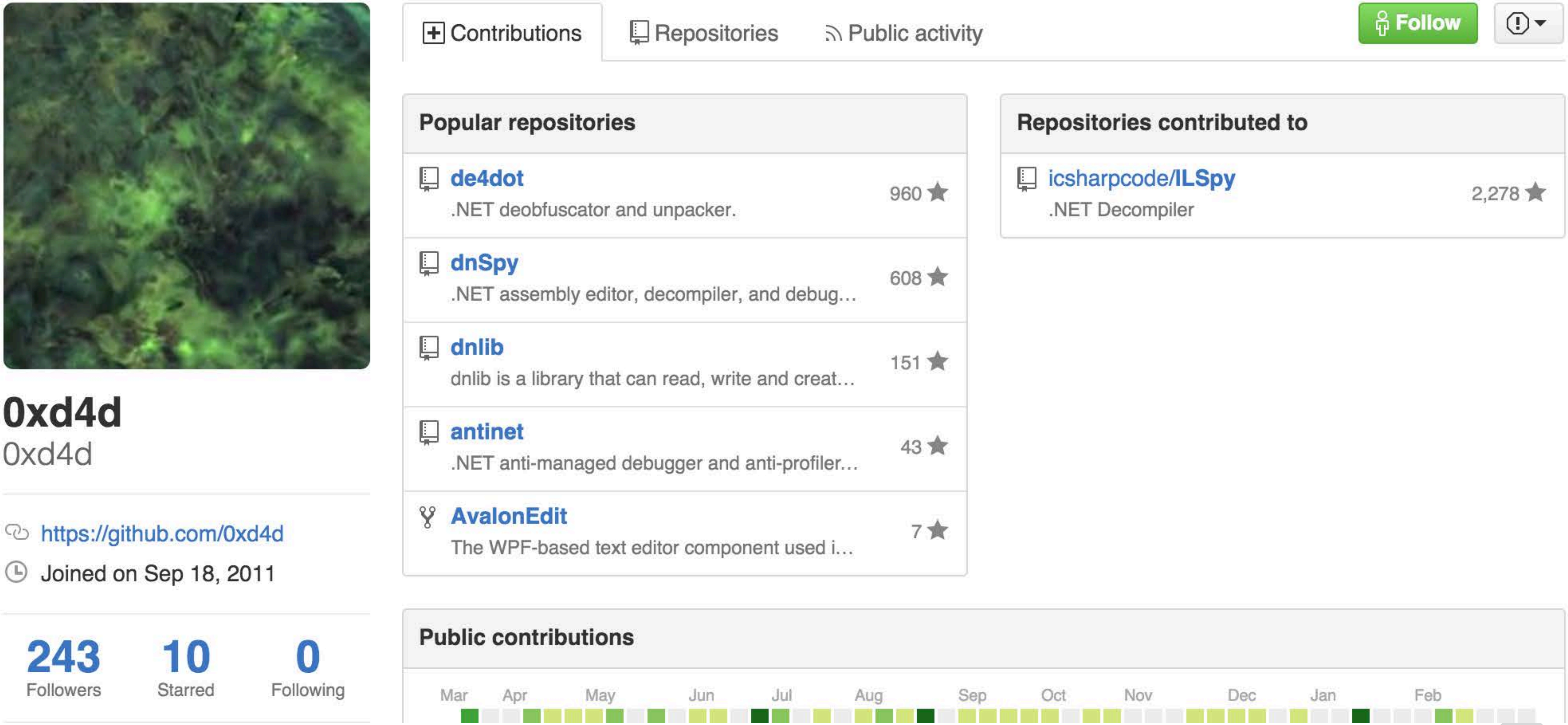


Startup

- **system is w7_1**
- vdespohcfeyy.exe (PID: 2876 MD5: 9CE01DFBF25DFEA778E57D8274675D6F)
  - xfjpayxmgocb.exe (PID: 2948 MD5: 9CE01DFBF25DFEA778E57D8274675D6F)
    - WMIC.exe (PID: 3088 MD5: A03CF3838775E0801A0894C8BACD2E56)
  - cmd.exe (PID: 2972 cmdline: C:\Windows\system32\cmd.exe /c DEL C:\VDESPO~1.EXE MD5: AD7B9C14083B52BC532FBA5948342B98)
- svchost.exe (PID: 3336 MD5: 54A47F6B5E09A77E61649109C6A08866)
- **cleanup**

DE4DOT

A free, open source .net deobfuscator.



0xd4d
0xd4d

https://github.com/0xd4d
Joined on Sep 18, 2011

243	10	0
Followers	Starred	Following

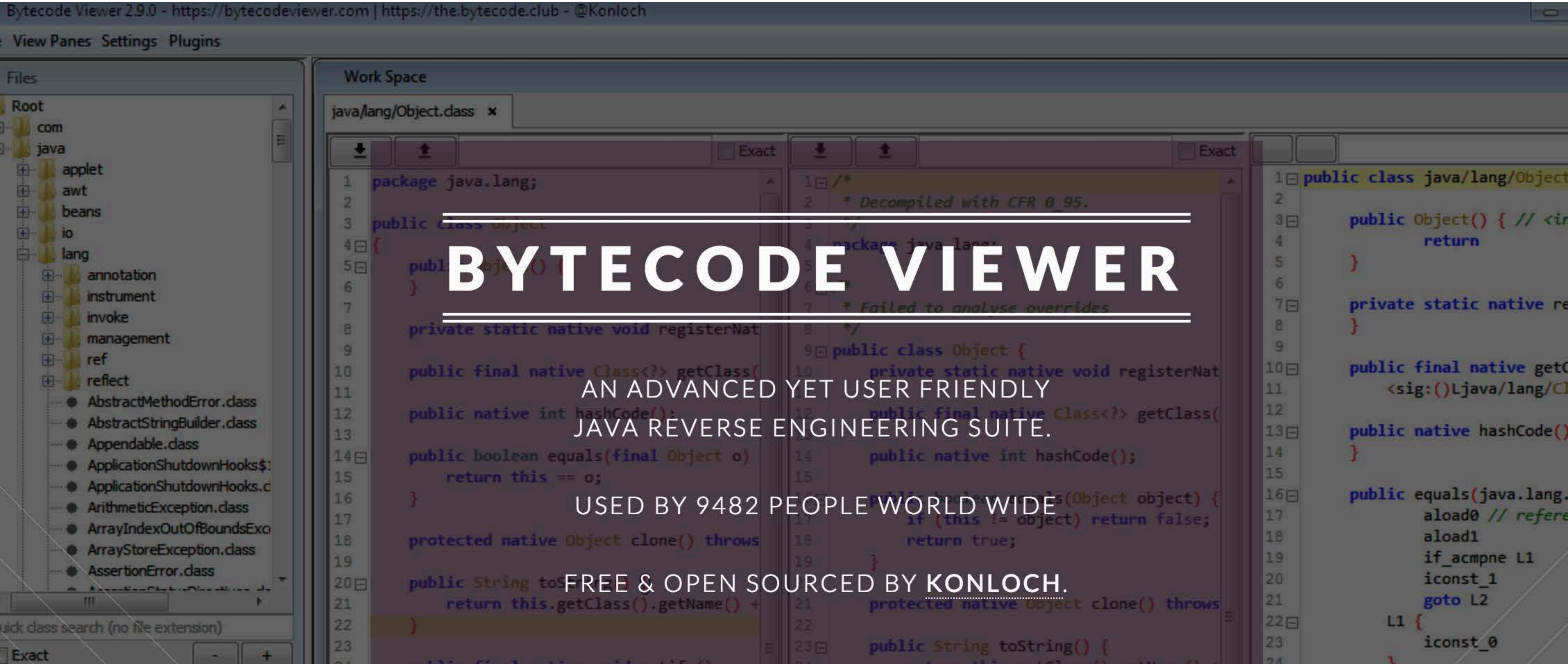
Popular repositories

Repository	Stars
de4dot .NET deobfuscator and unpacker.	960 ★
dnSpy .NET assembly editor, decompiler, and debug…	608 ★
dnlib dnlib is a library that can read, write and creat…	151 ★
antinet .NET anti-managed debugger and anti-profiler…	43 ★
AvalonEdit The WPF-based text editor component used i…	7 ★

Repositories contributed to

Repository	Stars
icsharpcode/**ILSpy** .NET Decompiler	2,278 ★

Public contributions

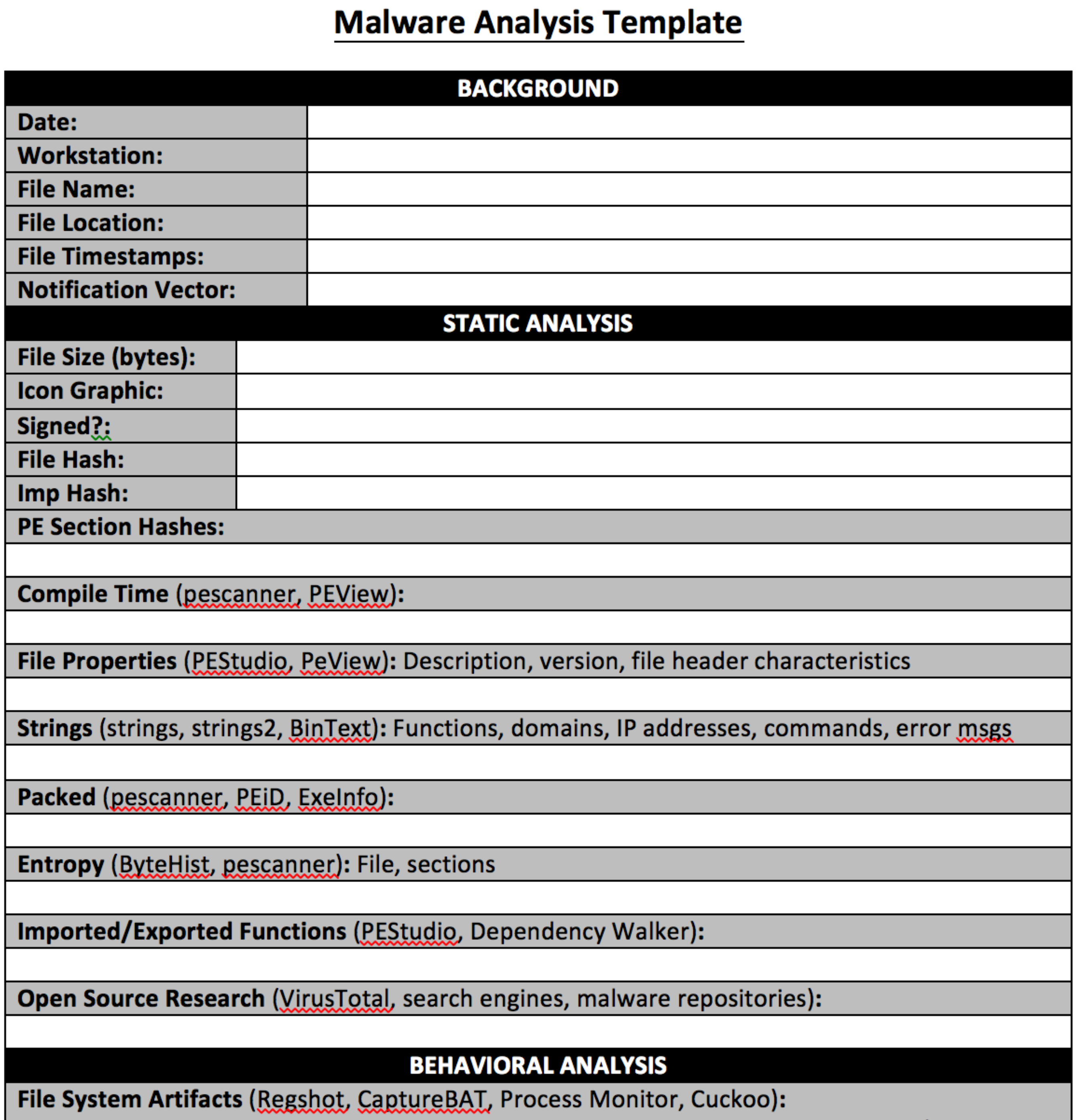

Bytecode Viewer 2.9.0 - https://bytecodeviewer.com | https://the.bytecode.club - @Konloch
View Panes
Settings
Plugins
Files
Work Space
java/lang/Object.class
Exact
Root
com
java
applet
awt
beans
io
lang
annotation
instrument
invoke
management
ref
reflect
AbstractMethodError.class
AbstractStringBuilder.class
Appendable.class
ArithmeticException.class
ArrayStoreException.class
AssertionError.class
uick class search (no file extension)

BYTECODE VIEWER

AN ADVANCED YET USER FRIENDLY
JAVA REVERSE ENGINEERING SUITE.

USED BY 9482 PEOPLE WORLD WIDE

FREE & OPEN SOURCED BY KONLOCH.



Malware Analysis Template

BACKGROUND	
Date:	
Workstation:	
File Name:	
File Location:	
File Timestamps:	
Notification Vector:	
STATIC ANALYSIS	
File Size (bytes):	
Icon Graphic:	
Signed?:	
File Hash:	
Imp Hash:	
PE Section Hashes:	
Compile Time (pescanner, PEView)**:**	
File Properties (PEStudio, PeView)**:** Description, version, file header characteristics	
Strings (strings, strings2, BinText)**:** Functions, domains, IP addresses, commands, error msgs	
Packed (pescanner, PEiD, ExeInfo)**:**	
Entropy (ByteHist, pescanner)**:** File, sections	
Imported/Exported Functions (PEStudio, Dependency Walker)**:**	
Open Source Research (VirusTotal, search engines, malware repositories)**:**	
BEHAVIORAL ANALYSIS	
File System Artifacts (Regshot, CaptureBAT, Process Monitor, Cuckoo)**:**	

Summary

Learned how to use File investigation tools

- Run samples
- Report