Heaventools

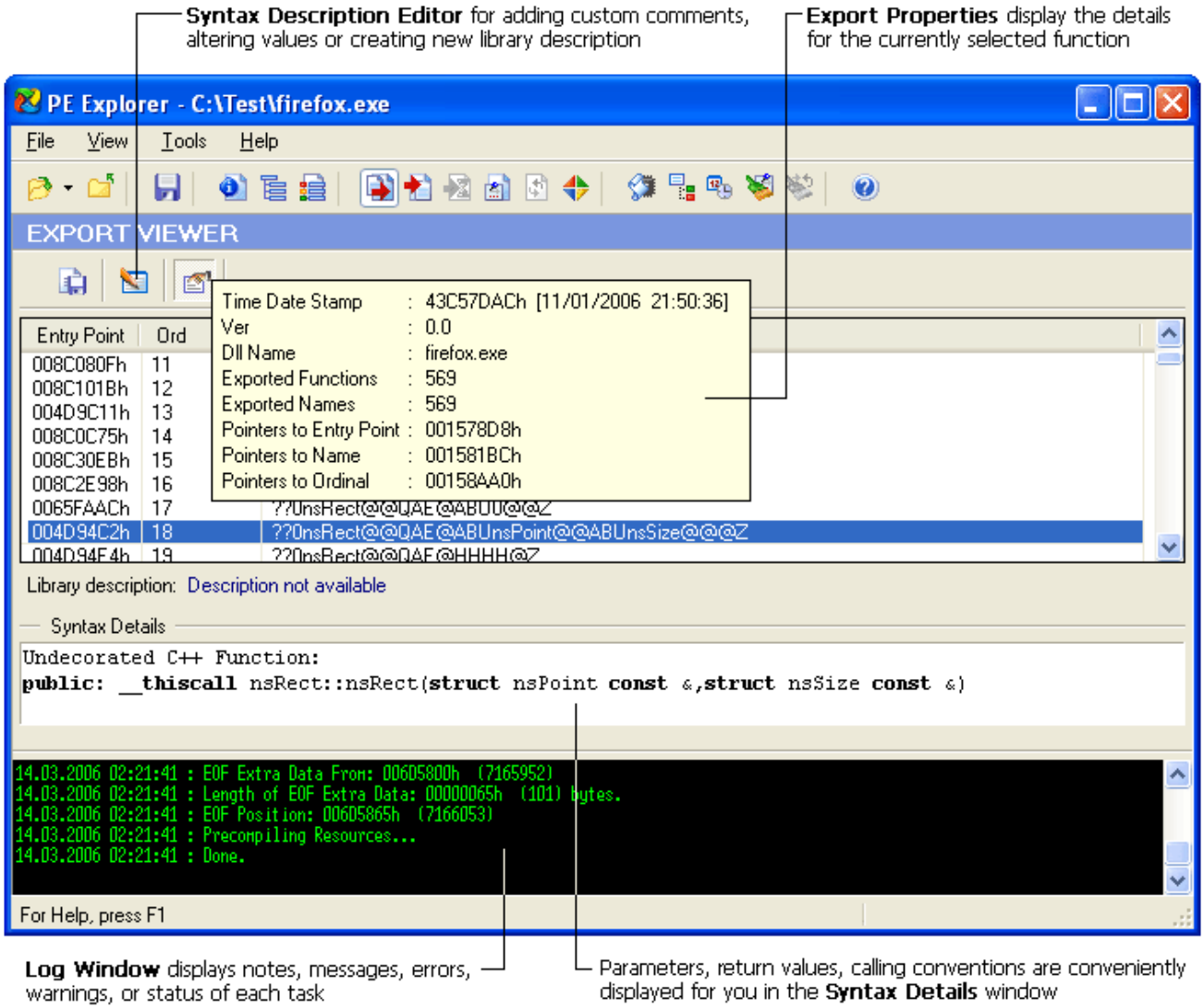
PE Explorer

Data Sheet

Malware Code Analysis Made Easy

Reverse engineers within the anti-virus, vulnerability research and forensics companies face the challenge of analysing a large number of maliciuos software appearing at an incredible rate. Software developers look for an effective way to safely inspect and dissect potentially harmful Windows executable files. Meeting this need, Heaventools offers PE Explorer, an integrated collection of tools that provide a framework for working with EXE, DLL, ActiveX controls, and other executable file formats that run on MS Windows 32-bit platforms.

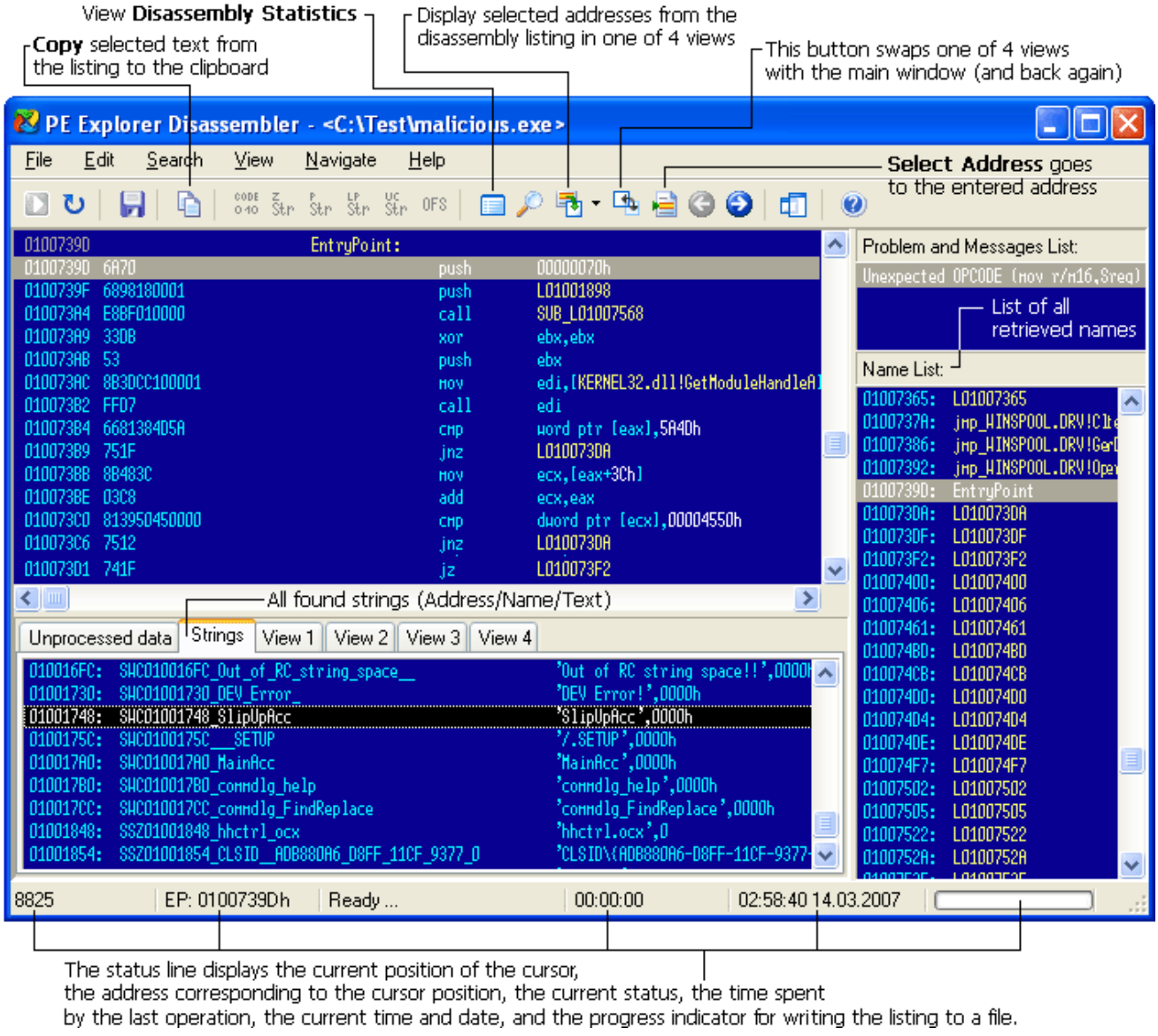
Though anti-virus software is continually getting better, a very significant percentage of malware escapes the automated screening process. PE Explorer offers an in-depth look at the inner workings of downloaded executable files, and helps software companies determine if a binary is harmful by examining it manually and without relying on the automated scanning engines.



PE Explorer greatly reduces the time needed to understand the structure of complex malware. This application unfolds each header, section and table found in an executable file to reveal the values stored inside those structures and reduce the numerous internal information sources of the binary file into a more convenient viewing format, providing the user with easy-to-read information about the function of the executable. PE Explorer exposes entire structure and all resources in suspect file in order to research and reverse engineer it. With PE Explorer, the user can rapidly analyze the procedures and libraries a malware executable uses without ever activating the executable itself - a great advantage over debuggers where malicious code needs to be run to be analyzed.

Disassembler

Dissassembling the code makes it possible to study exactly how the program works, and even identify potential vulnerabilities. If you reverse engineer spyware on a system, you could determine exactly what type of information the application was trying to snoop, as well as its other capabilities. Other uses for reverse engineering include the discovery of undocumented APIs or porting drivers, and for software patch analysis.



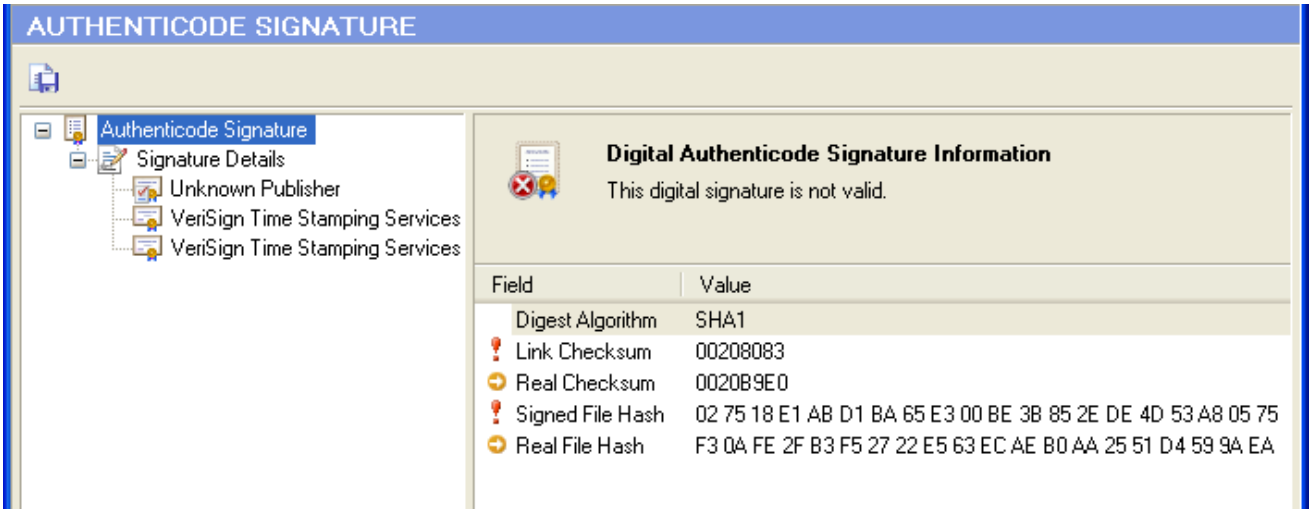
PE Explorer is designed to be easy to use compared with other disassemblers. While as powerful as the more expensive, dedicated disassemblers, PE Explorer focuses on ease of

use, clarity and navigation. It supports the common Intel x86 instruction sets along with extensions such as MMX, 3D Now!, SSE, SSE2 and SSE3, and utilizes a qualitative algorithm designed to reconstruct the assembly language source code of target binary win32 PE files with the highest degree of accuracy possible.

The disassembler also extracts ASCII text strings from the data portion of the executable file. Unlike the various strings utilities that search and extract the text strings from a file, PE Explorer is much more accurate and detailed in extracting these strings out from specified memory locations instead of searching. The output of strings found in the binary gives the user a good knowledge of what some of the functions and subroutines called by this binary are.

Publisher Verification

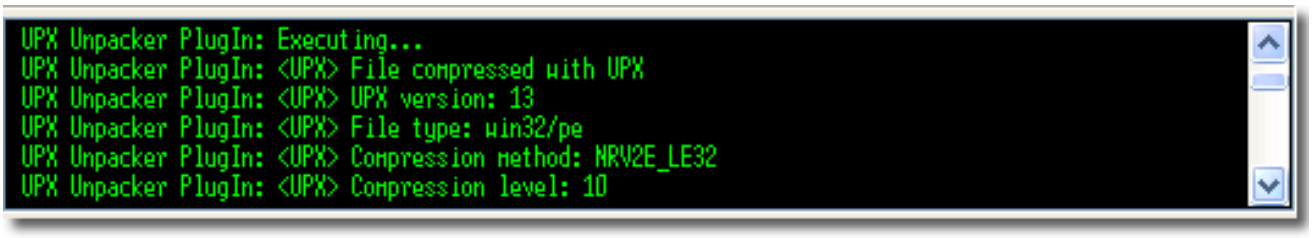
A great tool for detecting viruses, malware, and other executable nasties, the user can use PE Explorer to review and validate the Microsoft Authenticode digital signature, if present, in the loaded executable file.



This is a powerful way to examine a certificate-based digital signature of the executable, validate the identity of the software publisher, and verify that the signature is valid.

Reversing Packed Worms and Trojans

PE Explorer can open a variety of file types ranging from the common, such as EXEs and DLLs, to the less familiar types, such as DPL and CPL files. But, in real life, viruses, worms and trojans are often compressed, obfuscated and protected from reverse engineering.



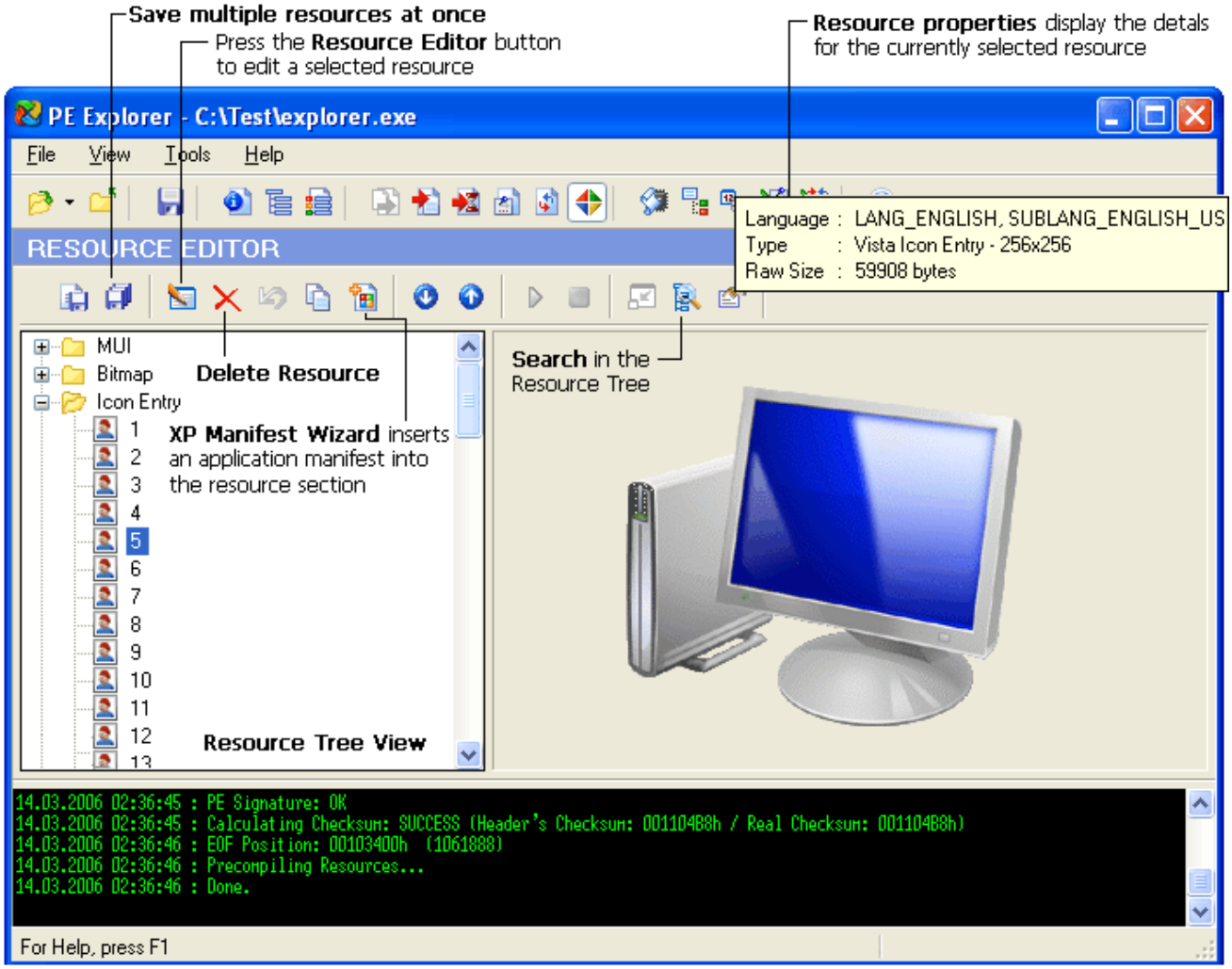
PE Explorer works on packed malware executables and can handle a file even if it has been packed and modified manually so that the standard uncompressing method cannot be used

directly to unpack the file. PE Explorer supports for files modified with Upack and many UPX scramblers. Now the user can open these obfuscated files with PE Explorer even without knowing that: the files will be unpacked automatically. Additionally, the product provides an open interface for plugging in custom start-up processing modules for crypted files handling.

Visual Resource Editor

PE Explorer combines a resource viewer, extractor, and a resource editor. Once the file is open, you will see a directory-like structure of the embedded resources, such as icons, images, sounds, strings, dialogs, menus, XML data, HTML data, and toolbars.

With PE Explorer, you can view, extract, replace, edit, and delete the resources of your own software. More importantly, this application lets you rebrand third party applications and libraries for which you do not have source code with new icons, strings and version numbers.



Keeping pace with changes to the Windows Operating System, PE Explorer helps your legacy applications take advantage of the new common control styles and appearances first featured in Windows XP and Vista, and mark pre-Vista applications with a requested execution level, providing the way to deploy the same builds of the applications on newer Windows versions.

Dependency Scanner

Another feature is the Dependency Scanner, which scans all the modules that the executable file links to statically and those that are delay-loaded, and it then displays them in a hierarchal tree structure, showing where the executable reaches to. PE Explorer can help you learn the minimum set of DLL files required for the EXE file to load and run, and the complete path to modules loaded by the EXE file. It is helpful in discovering missing or invalid modules, import/export mismatches, circular dependencies and other module-related problems, and in troubleshooting system errors caused by the loading or executing of modules.

Industry Feedback

“I use PE Explorer on .SYS files as I am an NT/XP device driver system architect. I was interested in understanding the way .SYS files interact with one another and this tool enabled me to understand that interaction a bit better.” *- Dominick Cafarelli, Sniffer Technologies, Network Associates*

“I've been using PE Explorer for a while, and am very impressed with the latest version's functions – especially the disassembler.” *- Conrad Herrmann, Zone Labs, Inc.*

Minimum System Requirements

PE Explorer runs on all versions of Windows from 95 through XP, Vista, 7, 8, 10 and 11.

- Intel Pentium® or AMD K5 processor with 166 MHz
- 16 MB RAM
- 15 MB free hard disk space

Users working with large file sizes will benefit from system requirements that exceed those listed above. This will ensure a faster disassembling.

Product Maintenance

PE Explorer comes with 18 months of maintenance and support included, beginning with the date of purchase.

Ordering Information

We offer a free trial version, so you can try the software, risk free. We encourage you to try out PE Explorer and basic technical support free of charge for 30 days before you make a decision regarding the purchase. When you are ready to buy, we welcome you to www.heaventools.com to order directly from us, or through our resellers.

Heaventools Software

http://www.heaventools.com
101-1001 West Broadway Dept. 381
Vancouver, BC, V6H4E4, Canada

Email: sales@heaventools.com
Fax: +1 (206) 984-3919