Cerbero Journal

*"They did not know it was impossible so they did it." – **Mark Twain***

ISSUE NR. 4 | CERBERO LABS | *JANUARY 8, 2024*

Since the last issue of our journal, there have been significant developments: the release of Cerbero Suite 7, accompanied by many new packages.

In this issue, we explore the major new features and improvements introduced by this major release and the extensive array of new packages now available for download on Cerbero Store.

Furthermore, this issue marks a first for us, being available exclusively as early access to our customers before its general public release.

CERBERO SUITE 7

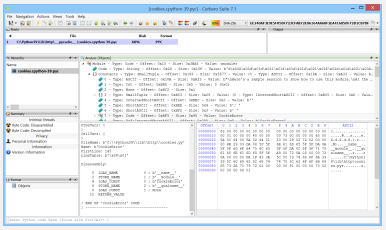
With the release of version 7 we have simplified our offering by unifying the editions of Cerbero Suite, thereby removing the distinction between the Standard and Advanced editions. Streamlining our software into a single edition represents our commitment to clarity and user-centric design. Multiple editions can often lead to confusion, making it challenging for users to discern the best fit for their needs. By offering just one, unified edition, we ensure that our users can navigate our platform with ease, fully understanding the breadth of features and tools available without the clutter of overlapping options. This simplicity not only enhances user experience but also fosters trust and transparency.

We have also introduced a more straightforward and customer-friendly licensing model. Every license purchased will now be valid for a full year from the date of purchase, regardless of when the acquisition is made. This one-year license also includes updates to any major new versions that are released within that year-long period.

In the first part of this issue, we delve into the exciting updates introduced in this major version. Highlights include significant UI enhancements, the introduction of the new Fast Text View, File Info View, and File System View, along with improvements to the Python Workspace.

ALL THINGS PYTHON

Need to reverse engineer Python bytecode? No problem, we got you covered! [read more]

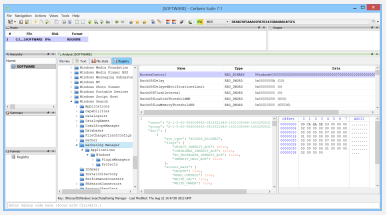


MORE ARCHIVES

Many new packages covering a vast number of additional archive formats: RAR, XAR, AR & RPM. [read more]

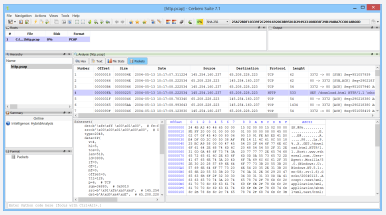
WINDOWS REGISTRY HIVES

Should you require the capability to delve into raw Windows Registry hives, a specialized package is now available! [read more]



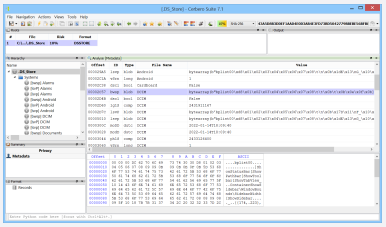
PCAP & PCAPNG

Our goal was to eliminate the need to always switch to Wireshark for analyzing PCAP files. [read more]



MACOS .DS_STORE

Exploring .DS_Store files for digital forensic purposes. [read more]



CERBERO STORE

For those not yet familiar with it, Cerbero Store is a simple way to install and update optional packages for Cerbero Suite and Cerbero Engine.

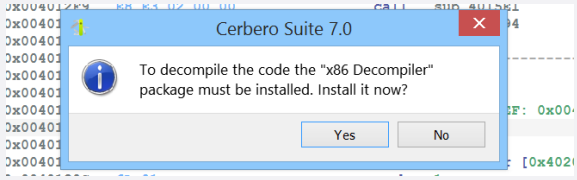
Updating specific parts of an application through Cerbero Store is notably more efficient than updating the entire application. This method also prevents users from having to install functionality they are not interested in.

Furthermore, our software operates across multiple platforms, meaning each update traditionally required the creation of multiple software packages. Cerbero Store addresses this issue effectively, as all platforms use the same package code, simplifying the update process and ensuring consistency across different operating systems.

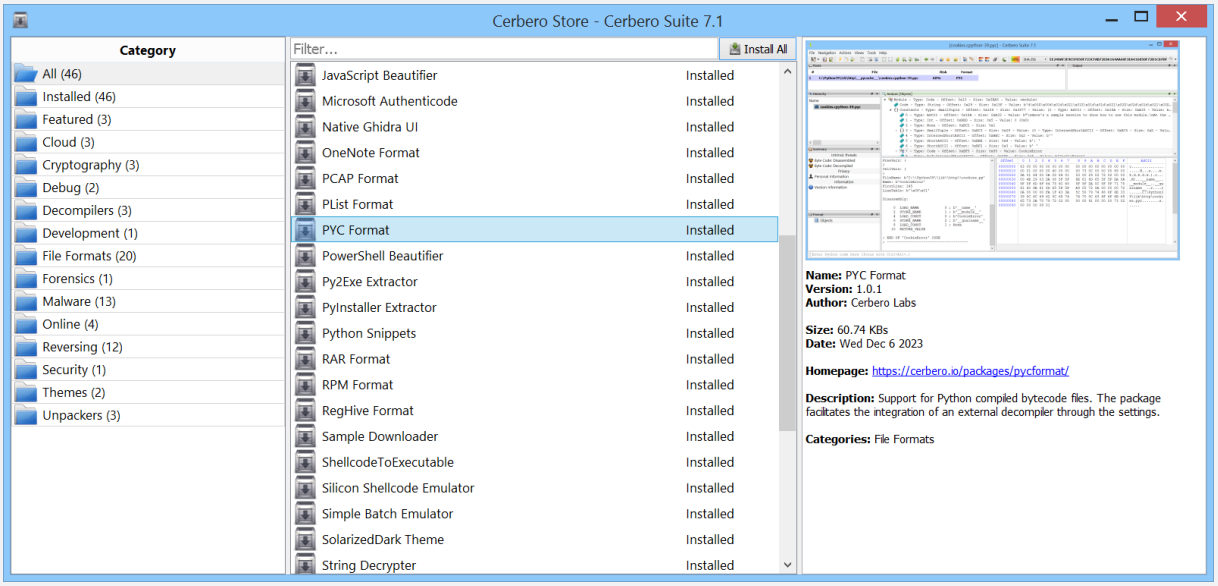
Since the release of Cerbero Suite 7, Cerbero Store has expanded significantly, adding a variety of new packages. We will delve into these additions in the subsequent pages.

It is worth mentioning, that we have moved some tools and formats to the store to reduce the overall size of the main binary package. All decompilers, for example, have been transitioned to individual packages within Cerbero Store. This move aims to facilitate installations based on necessity.

When trying to decompile code without the required decompiler, Cerbero Suite will ask you if you wish to install the decompiler.



After installing the required decompiler package, Cerbero Suite will then move forward with the code decompilation process.



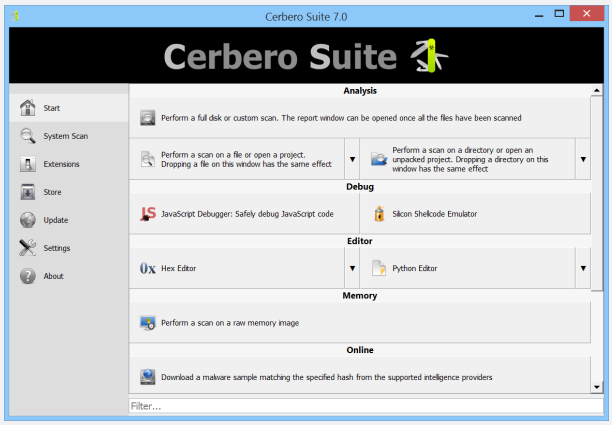
INDEX

COMMERCIAL-ONLY PACKAGES

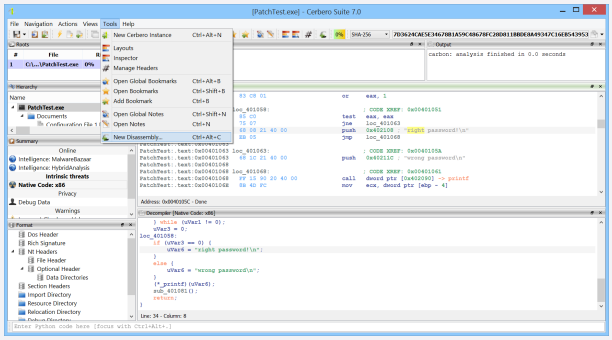
Holders of the Personal license for Cerbero Suite have access to a wide range of packages on Cerbero Store. Nevertheless, certain packages, like the Silicon Shellcode Emulator package, are exclusively reserved for commercial licenses. We make a conscious effort to limit the number of packages restricted to commercial licenses, focusing on those that we believe are primarily used for commercial activities.

UI ENHANCEMENTS

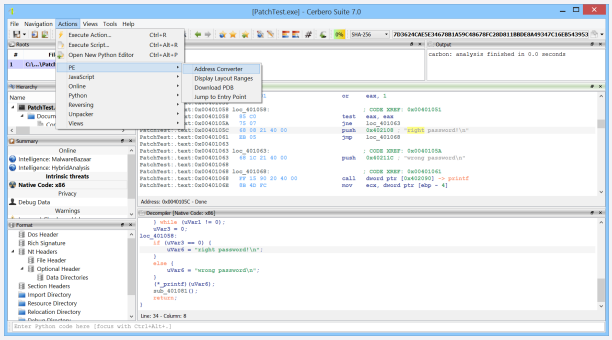
As the array of tools in Cerbero Suite continues to expand, we recognized the need for a more intuitive and accessible interface. Hence, we've revamped the main window to feature a scrollable interface, enabling easier navigation. For added convenience, tools can also be filtered by name, ensuring a smoother user experience.



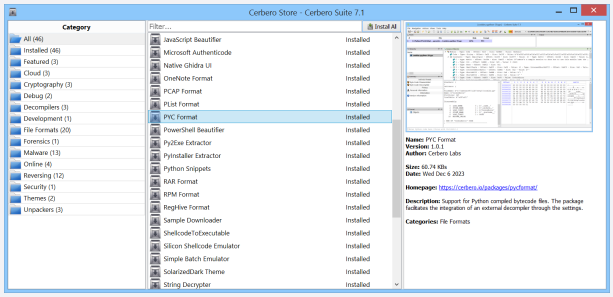
We've introduced a top bar menu in the analysis workspace. This new feature offers a clearer overview of available global shortcuts, streamlining navigation and bolstering overall intuitiveness.



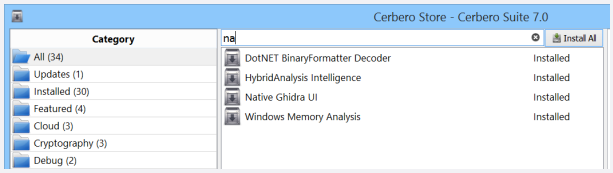
In addition, we've made the list of context-specific actions readily accessible through the new top bar menu, ensuring all pertinent tools are just a click away.



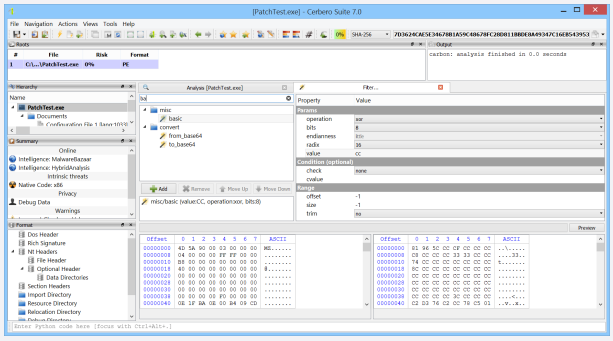
Cerbero Store has undergone a transformation, enhancing its interface for better user navigation and more streamlined package installations. Notably, the revamped interface now showcases thumbnails for each package, offers direct web URLs to dedicated package pages, and introduces name-based filtering.



Moreover, users now have the convenience of installing all packages displayed in the current list with a single click.

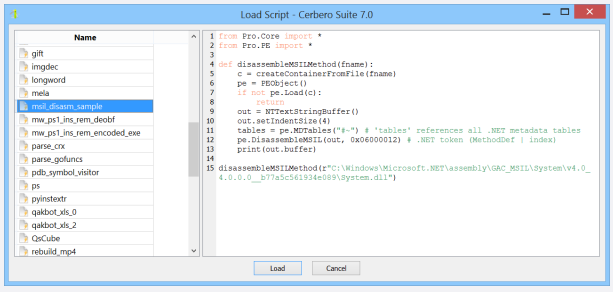


The user interface for filters has been refined, now allowing users to conveniently search and filter the filters by name.



Similarly to the filters view, actions can now too be filtered by their name.

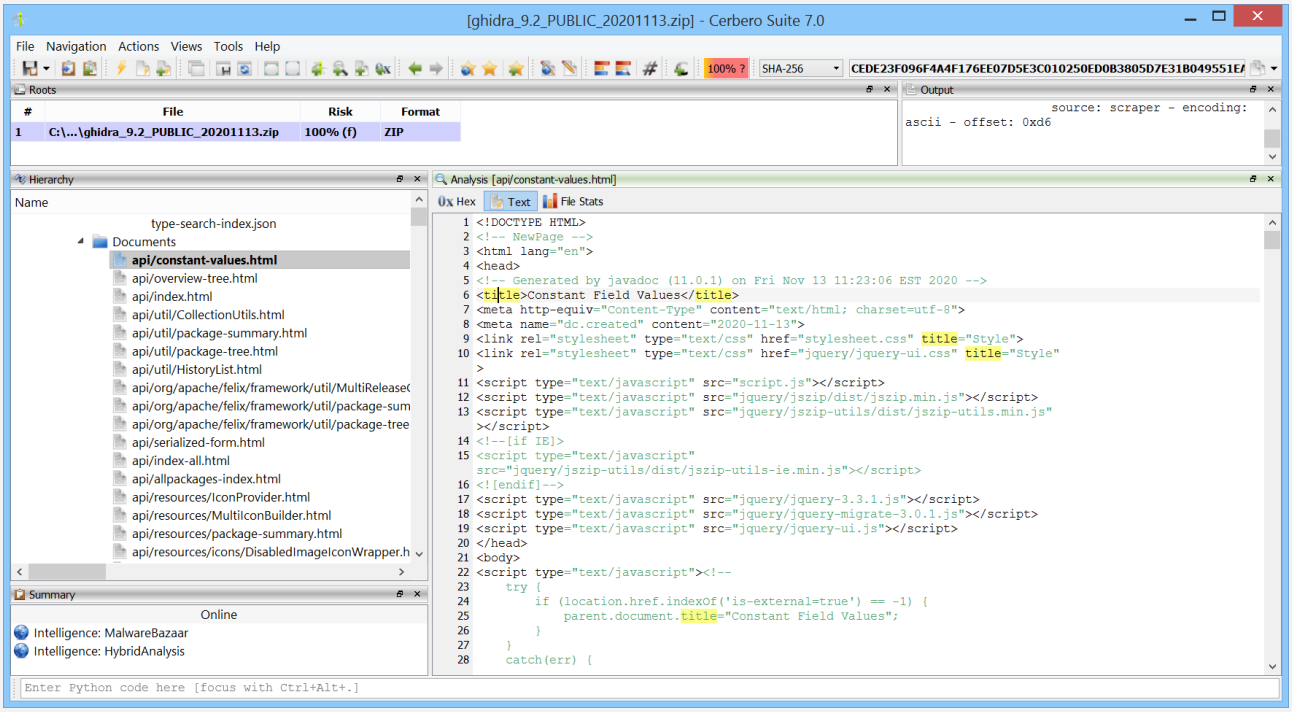
We've given a fresh facelift to the dialog for loading internally stored scripts. Now, it offers a preview, allowing users to conveniently glimpse the available scripts before selection.



These enhancements represent the minor improvements. In the following pages, we will explore the key additions introduced in Cerbero Suite 7.

FAST TEXT VIEW

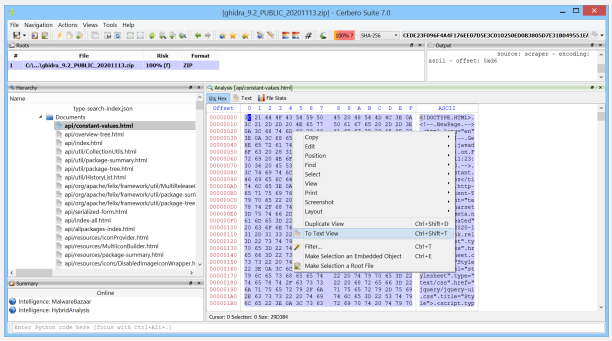
One of the standout features of Cerbero Suite 7 is the addition of a fast text view designed for previewing sizable files. Not only does this view support syntax highlighting, but its integration is seamlessly woven throughout the entirety of Cerbero Suite, enhancing functionality across the board.



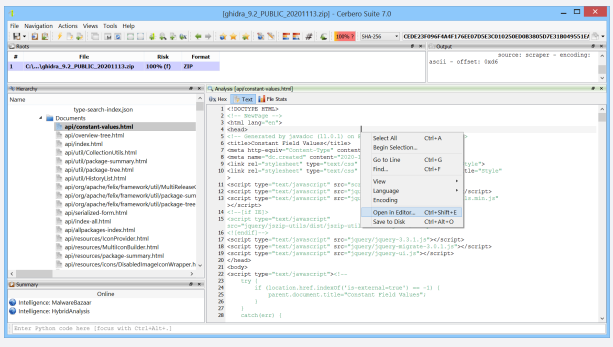
The new fast text view.

Leveraging cutting-edge technology, the view intelligently auto-detects the codec of input data. Moreover, it offers automatic syntax highlighting tailored to the specific file extension.

You can simply press Ctrl+Shift+T while in a hex view, and you'll instantly activate the fast text view, presenting the selected bytes in a readable text format.



Additionally, from within the fast text view, pressing Ctrl+Shift+E will launch a text editor, allowing you to seamlessly edit the text.



Naturally, the fast text view isn't just for end-users; plugin developers can fully harness its capabilities too.

CHALLENGE: PAYLOAD URL

This challenge is very easy and can be tackled by beginners.

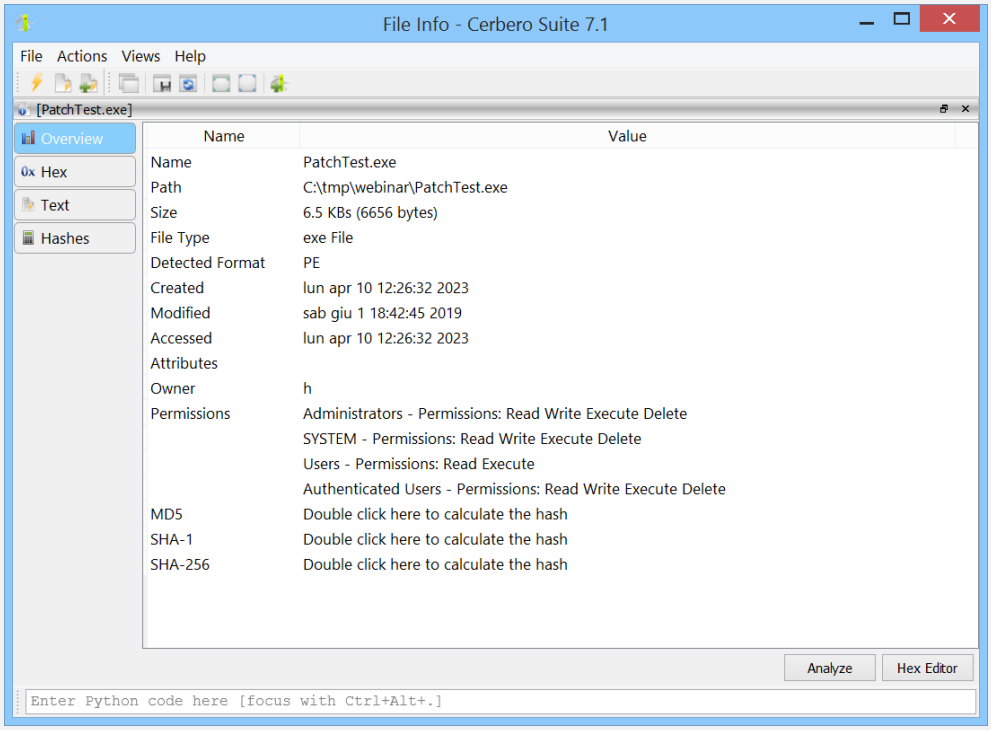
Download the following malware sample and debug or deobfuscate the JavaScript to extract the payload URL.

SHA256: 8FD31EC311D7AED033E8405EE5D6EBD562B363B8BB18B4E4C04D1F86D7DE81B7

Payload: c2NyaXB0OmhUdFA6Ly9qcGFqdy5qb3VybmV5ZWRnZS5teS5pZC8/MS8=

FILE INFO VIEW

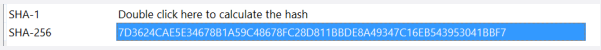
This versatile view provides you with a detailed list of a file's properties and an array of other valuable information.



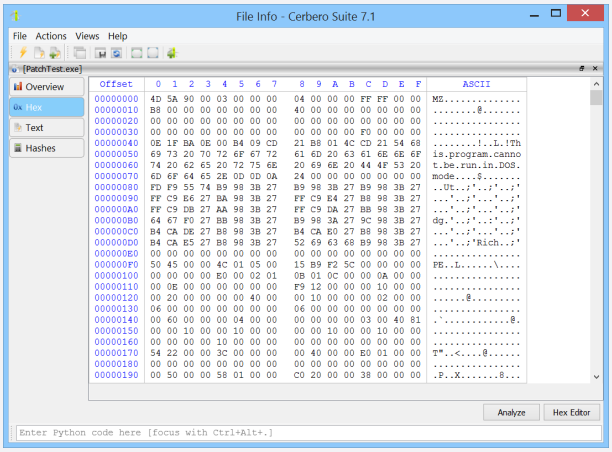
The new file info view.

What makes this particularly useful is the introduction of an additional workspace in Cerbero Suite. This new workspace leverages the file info view and can be accessed via the shell context menu, giving you immediate access to essential file details and its content.

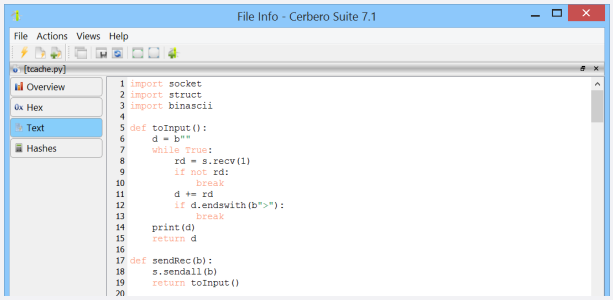
The overview of the file displays the most common cryptographic hashes. By activating the items via double-click or keyboard, the hash is calculated and shown.



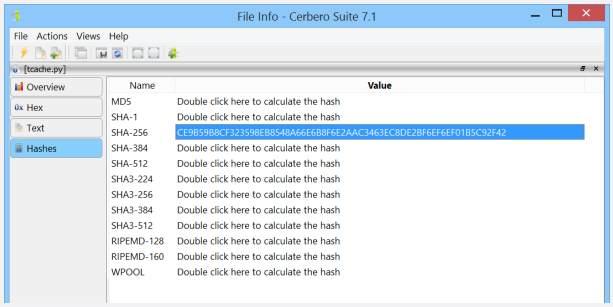
Beyond hashes, the file info view shows the hex content of the file.



Thanks to the fast text view, text previewing is also available, even for large files.

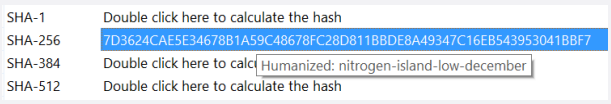


Of course, you can also retrieve less commonly used cryptographic hashes.

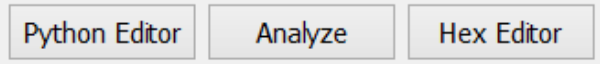


Hovering over a calculated hash shows its humanized form.

. . . continued from page 5.

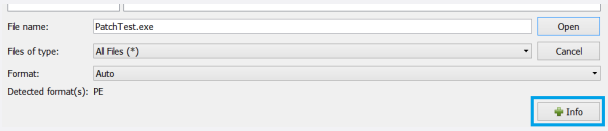


When exploring files on disk, a quick launch panel appears at the bottom, offering a hassle-free way to open the current file with another tool that supports its type.

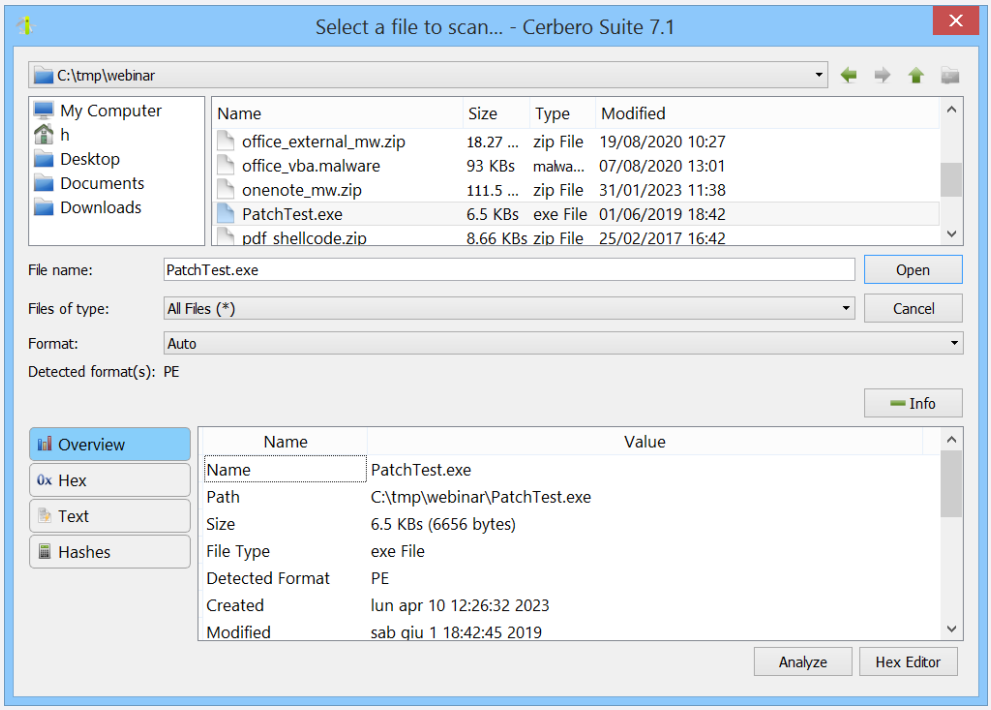


The file info view is completely exposed to the SDK, and it can be further extended via plugins using the UI hook extension type via the ”fileinfo” category.

To improve performance, we've completely rewritten the file dialogs, but we didn't stop there: when opening a file, an ”Info” button is visible.



When clicked, this button displays a file info view for the currently selected file, so that before opening a file we can inspect its information and content if necessary.



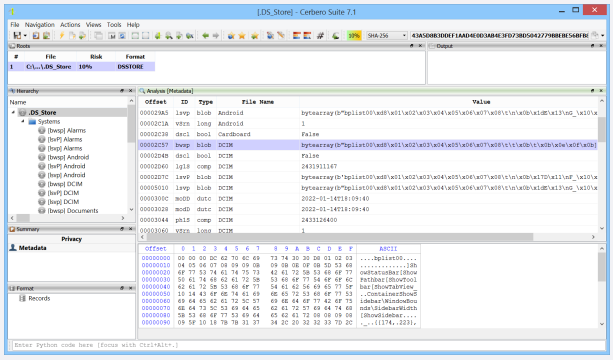
A file dialog displaying and embedded file info view.

THREATPULSE

In response to the rapidly changing and sophisticated nature of cyber threats, we have released the ThreatPulse package, a critical tool designed to combat the latest and potentially unforeseen threats.

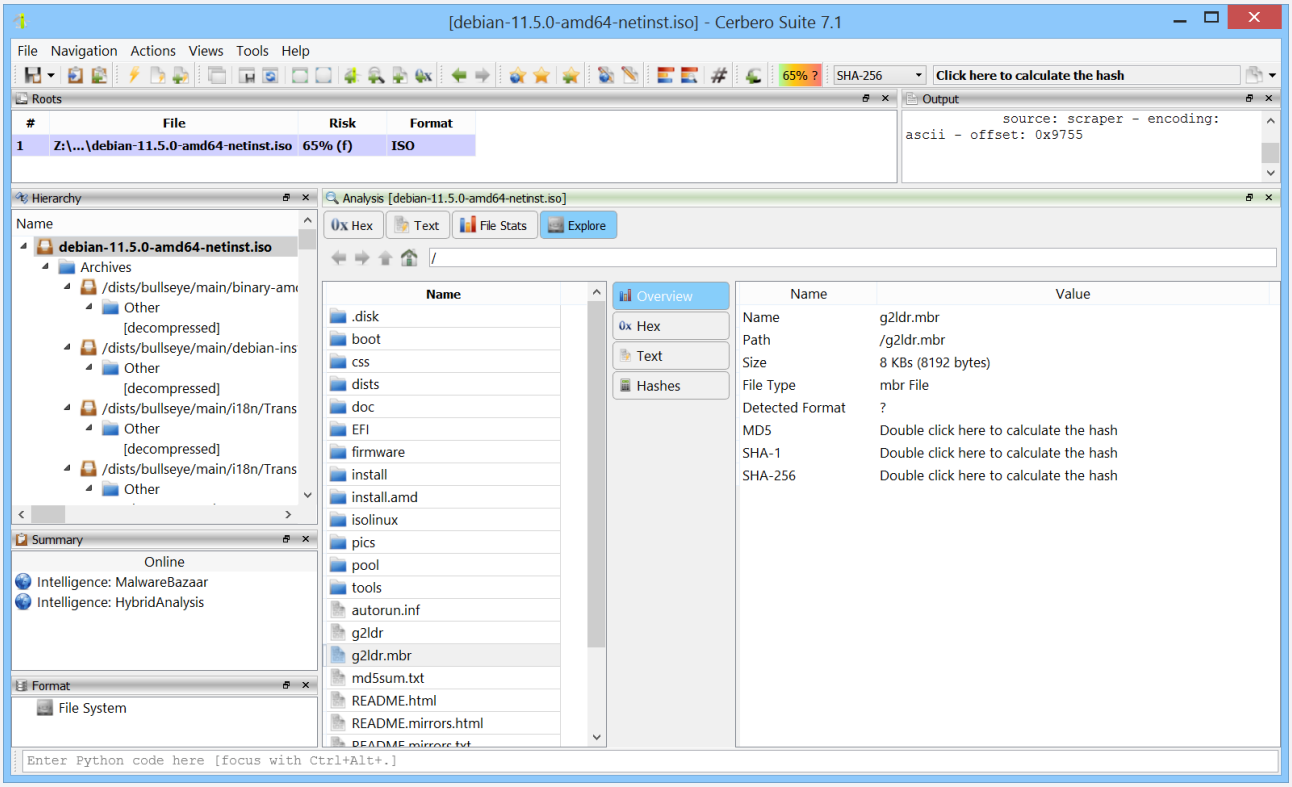
Recognizing that new threats may not conform to specific file formats or might target formats not yet fully supported, ThreatPulse offers a versatile and timely solution. It serves as a dynamic resource for detecting emerging threats, sometimes providing temporary detection capabilities that can be crucial until the main binaries of Cerbero Suite are updated.

Available to all Cerbero Suite license holders through Cerbero Store, ThreatPulse ensures that users are equipped with the most current tools and strategies, enabling them to address a broad spectrum of threats effectively and promptly, even those that challenge existing detection paradigms.



FILE SYSTEM VIEW

We have created a new interface specifically to showcase file system structures.



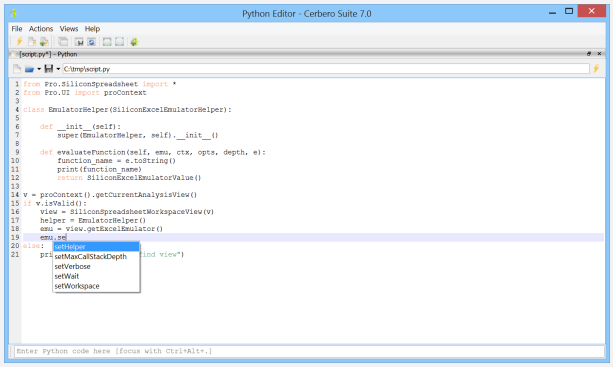
The new file system view.

The file system view provides a multifaceted display and embeds the previously presented file info view. Coupled with familiar navigation tools and shortcuts, it ensures a smooth and intuitive journey through any file system.

The SDK provides access to the file system interface and its view, saving plugin developers the hassle of crafting their own.

PYTHON WORKSPACE

Our Python editor and workspace have undergone significant enhancements. Now, they not only support the editing of files on disk, but also come equipped with auto-completion.



In addition to the auto-completion feature the editor now displays tool-tips that appear while inputting function arguments.

Auto-completion currently encompasses all built-in Python libraries and those modules in our SDK that have already been documented. As we continually update and expand the documentation, the scope of auto-completion also grows. Since all core modules are thoroughly documented, auto-completion is an invaluable tool for plugin developers.

ENGINE INTERMEZZO

In case you're not yet familiar with Cerbero Engine, here is a quick introduction. You can read more on our web page.

WHAT IS CERBERO ENGINE?

Cerbero Engine is our solution for enterprise projects such as cloud or in-house services. It offers the same SDK as Cerbero Suite and has already been used to analyze billions of files.

WHAT CAN IT DO?

The SDK is extensive and features support for dozens of file formats, scanning, disassembly, decompiling, emulation, signature matching, file carving, decompression, decryption and much more.

We make sure Cerbero Engine keeps up with the latest threats and challenges presented by file formats which are difficult to analyze. We offer state-of-the-art support for various file types such as Adobe PDF and Microsoft Office.

HOW SECURE IS IT?

Cerbero Engine has been designed taking into account all types of security issues when analyzing malicious files: buffer overflows, integer overflows, infinite loops, infinite recursion, decompression bombs, denial-of-service etc.

WHAT PLATFORMS DOES IT SUPPORT?

Just like Cerbero Suite, Cerbero Engine is cross-platform. Currently we offer it for both Windows (x86, x64) and Linux (x64). It is also compatible with older versions of Windows and Linux.

CAN IT BE EMBEDDED?

Cerbero Engine is deployed as an embeddable module: a Dynamic-Link Library (DLL) on Windows and a Shared Library on Linux. The engine can be loaded from both C/C++ and Python 3.

Loading the engine from Python is extremely simple.

```
from ProEngine import *

# initialize the engine
proEngineInit()

# from here on the SDK can be accessed
from Pro.Core import *
# ...

# finalize the engine before exiting
proEngineFinal()
```

Loading the engine from C/C++ is also very simple: it only requires including the 'ProEngine' header and specifying the location of the engine on disk.

```
#define PRO_ENGINE_INIT
#include "ProEngine.h"

int main()
{
    // initialize the engine
    if (!proEngineInit("/path/to/the/
        ↪ engine", ProEngine_InitPython))
        return -1;

    // from here on the SDK can be
        ↪ accessed

    // finalize the engine before exiting
    proEngineFinal();
    return 0;
}
```

IS IT FAST?

While the SDK is in Python, our engine is written in C++ and is both multi-thread and multi-process. This design decision guarantees maximum speed, while also giving you the capability to write cross-platform code that is compatible across both Cerbero Engine and Cerbero Suite.

Since the SDK is in Python, you don't need to worry about rebuilding your project when the engine is updated. Moreover, we take great care not to introduce breaking changes to the SDK: we don't want you to worry that an update could cause your code to stop working!

HOW DO YOU LICENSE IT?

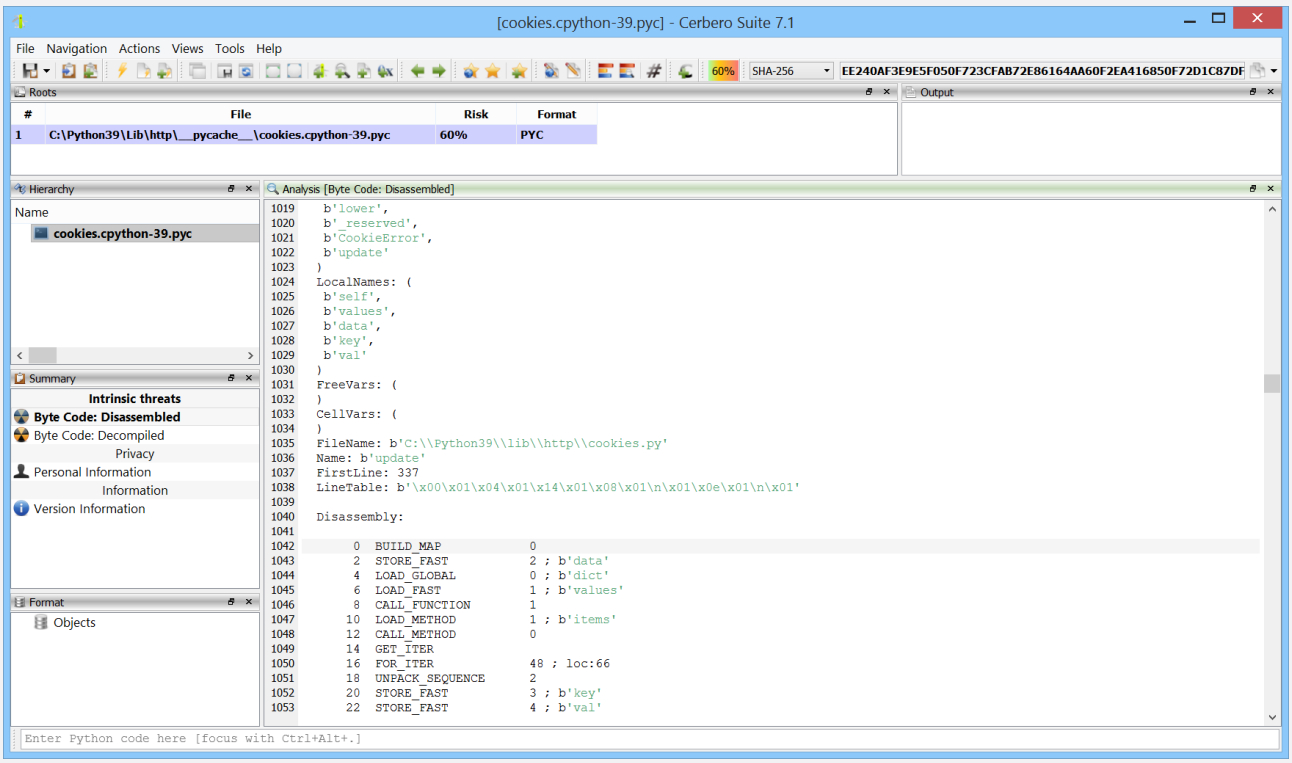
We license Cerbero Engine on a per-case basis. Licensing depends on the project's scope. If you are interested in a quotation, please contact us.

Purchasing a license of Cerbero Engine comes with discounted lab licenses for Cerbero Suite. By using Cerbero Suite, your engineers can interactively debug parsing issues, analyze edge cases, use the Python editor for development and create graphical applications that work in conjunction with Cerbero Engine.

ALL THINGS PYTHON

We have released three packages designed to assist reverse engineers in unraveling the complexities of Python PYC bytecode files and how they are deployed. These packages are available to all licenses of Cerbero Suite.

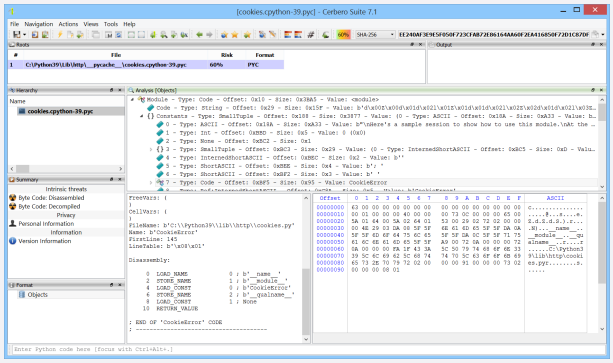
The first package adds support for the PYC format.



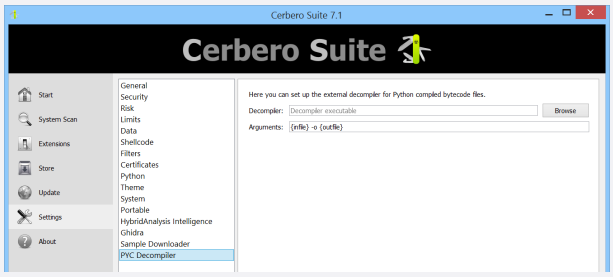
The disassembled bytecode of a Python PYC file.

PYC files are compiled bytecode versions of Python source code. These compiled files can be deployed in place of the original source code, serving as a bytecode format for execution by the Python interpreter. PYC files are tied to the specific version of Python they were compiled with, necessitating recompilation when different Python versions are used.

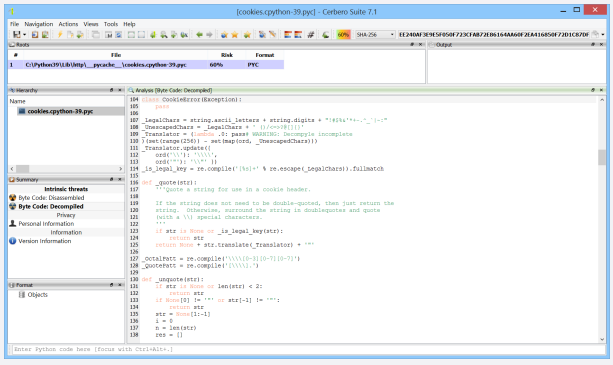
The support is designed to be fully compatible with all Python versions, enabling users to delve into the intricacies of the complete PYC file format and its instructions.



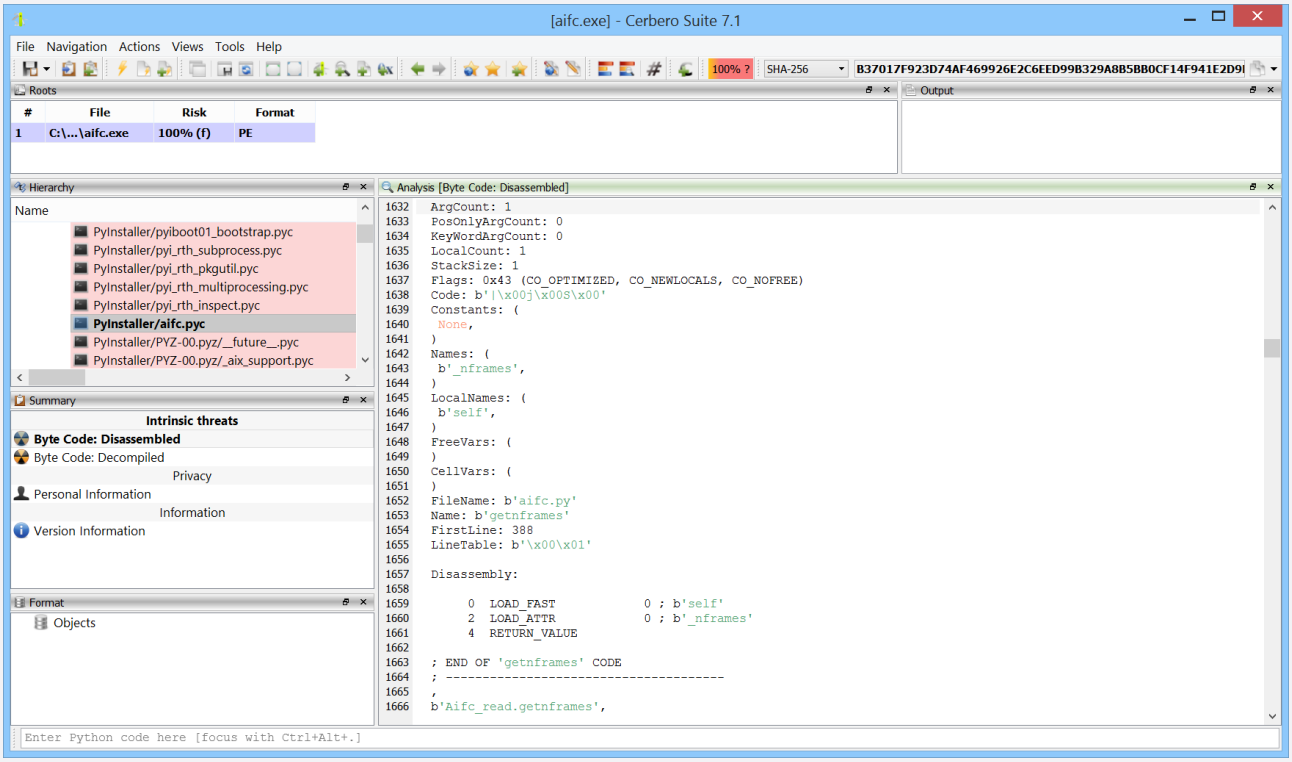
The package also allows the integration of an external decompiler such as Decompyle++ through the settings.



Once the external decompiler is set up, accessing the decompiled source code is achievable with just a single click.



. . . continued from page 9.



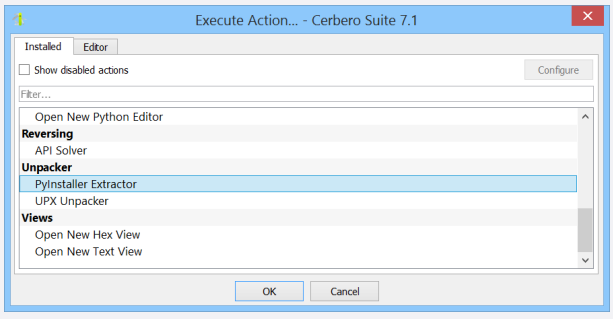
Files automatically extracted from a PyInstaller executable.

The second package is called PyInstaller Extractor.

PyInstaller is a tool that packages Python applications into standalone executables, compatible with Windows, Linux, and macOS. It works by analyzing Python scripts to discover every import statement and include the appropriate Python files, binaries, and libraries in the executable. Additionally, PyInstaller converts all Python code into bytecode before packaging, enhancing performance and security.

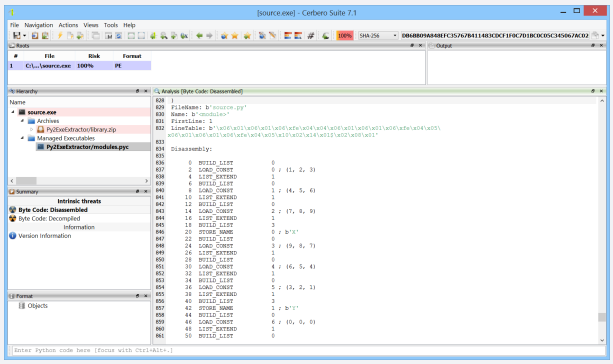
The extractor supports all versions of PyInstaller, all supported file types and automatically identifies PyInstaller generated binaries. It also supports PyInstaller bytecode decryption.

If a PyInstaller binary is not automatically detected, files can be extracted manually using the dedicated action.



Finally, the third package is called Py2Exe Extractor.

py2exe is a Python package that converts Python scripts into executable Windows programs. The tool packages Python bytecode and the necessary libraries into a single executable file, eliminating the need for a Python interpreter to be installed on the client machine. py2exe works by analyzing the imported modules in the Python script and includes them along with a Python interpreter as a part of the generated executable.



The extractor supports all versions of py2exe and automatically identifies py2exe generated executables.

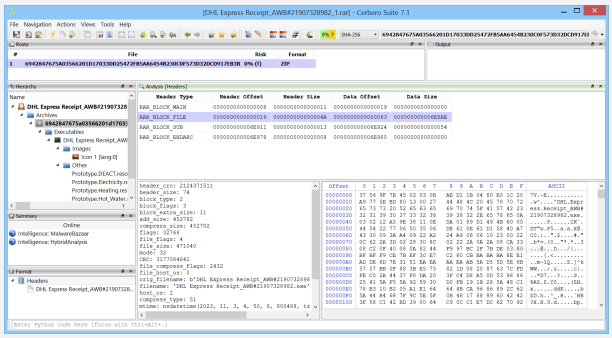
Collectively, these packages equip reverse engineers with a versatile and powerful toolkit for tackling the varied challenges posed by Python-based applications and executables, making Cerbero Suite an indispensable resource in the realm of Python reverse engineering.

MORE ARCHIVES

Since the launch of Cerbero Suite 7, we have significantly expanded our archive support, adding to the already extensive range of formats that were previously available. These packages are available to all licenses of Cerbero Suite.

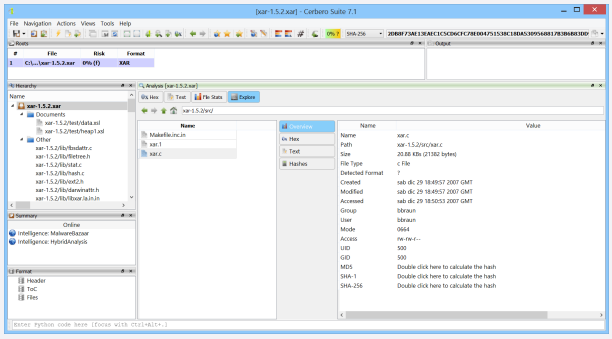
We have released the RAR Format package.

Supporting the RAR format is crucial in the security field due to its frequent use in deploying malicious files. RAR, known for its efficient compression and encryption capabilities, is a popular choice among cyber attackers for distributing malware. Its ability to compress files significantly and password-protect them makes it a preferred method for concealing harmful payloads.

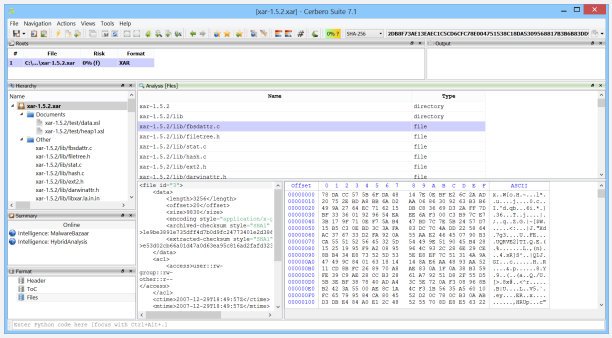


The support includes encrypted archives and the inspection of the format structures.

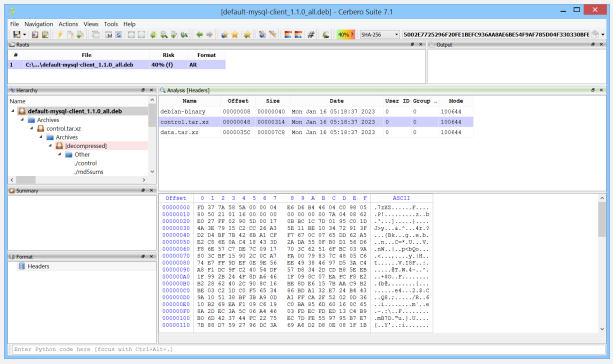
The XAR Format package: XAR (eXtensible ARchive format) is an archive file format which is used for software installation routines in macOS as well as browser extensions in Safari.



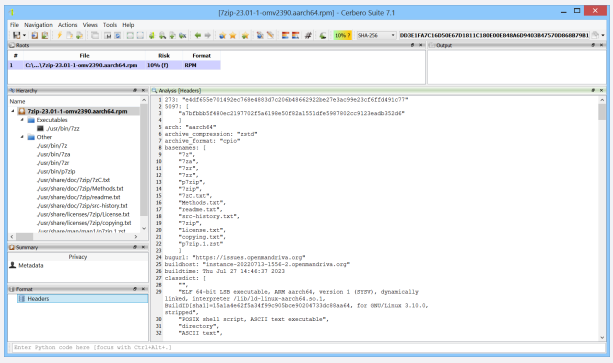
The support includes inspecting the format's structures.



The AR Format package: The AR archive format, originally devised for Unix systems, serves as a straightforward file archiving tool, combining multiple files into a single archive without inherent compression. It's primarily used in Unix-like environments for storing static libraries ('.a' files), and is also a key component in the structure of DEB packages for Debian-based Linux distributions. Furthermore, the AR format finds its application in the Windows operating system as well, where it is used for '.lib' files.



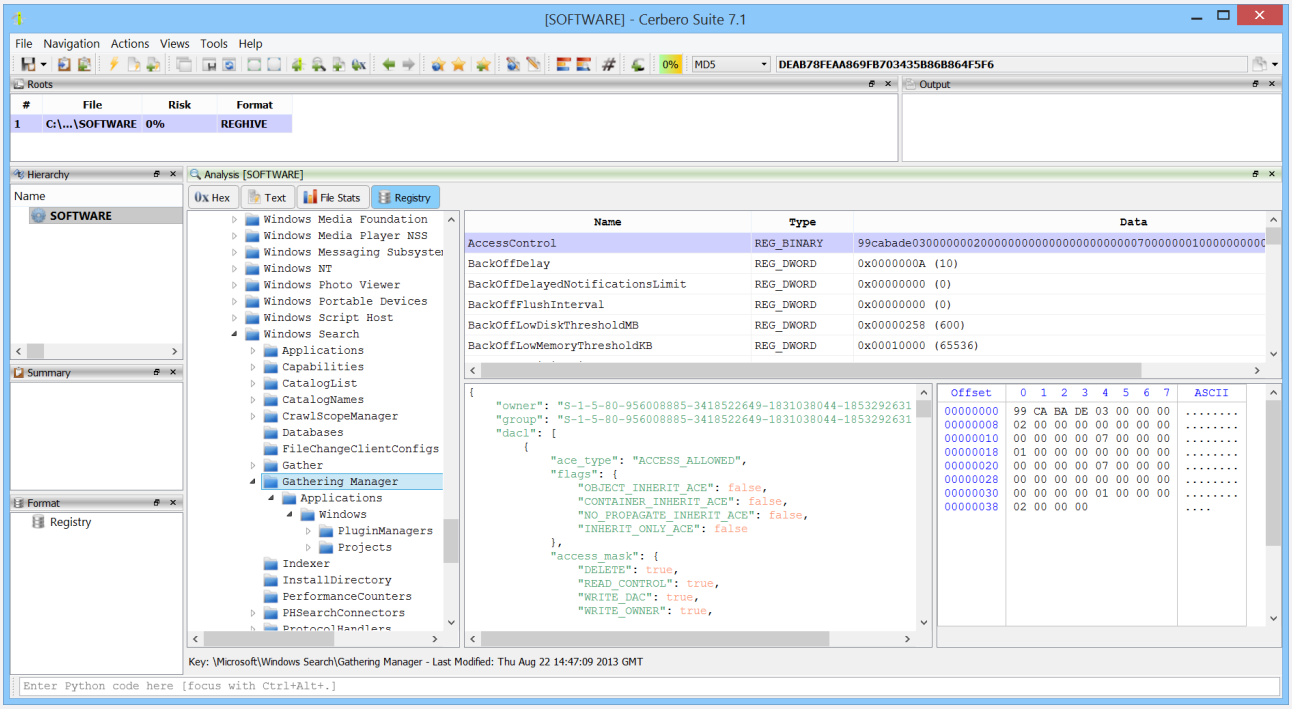
The RPM Format package: The RPM Package Manager (RPM) format is a package management system used primarily in Red Hat-based Linux distributions, including Fedora and CentOS. It is utilized for managing the installation, update, and removal of software on Linux systems. An RPM file contains the software itself, along with metadata about the software such as its version, dependencies, and instructions for installation. This format streamlines the process of software management, providing a standardized approach to handling packages on Linux platforms.



All these packages are seamlessly integrated into the Python SDK, enabling programmatic file extraction without the need to open the user interface. This allows for streamlined and automated processing, enhancing the versatility and efficiency of your workflow.

WINDOWS REGISTRY HIVES

We have released the RegHive Format package for all licenses of Cerbero Suite.

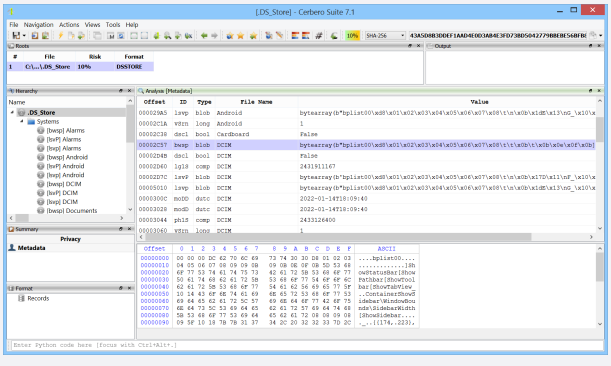


The keys and values of a Windows Registry hive.

This package offers enhanced functionality for exploring Windows Registry hives. It enables detailed inspection of keys and values, and importantly, provides additional insights by displaying the last modification date and time for each key. Moreover, it includes the ability to view security access details for each key, offering a comprehensive overview of the Registry's structure and access controls.

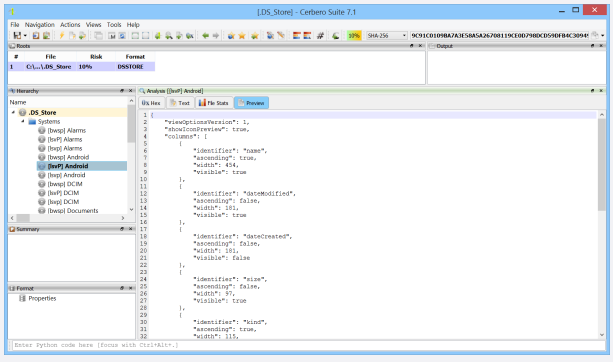
MACOS .DS_STORE

We have released the DSStore Format package for all licenses of Cerbero Suite.



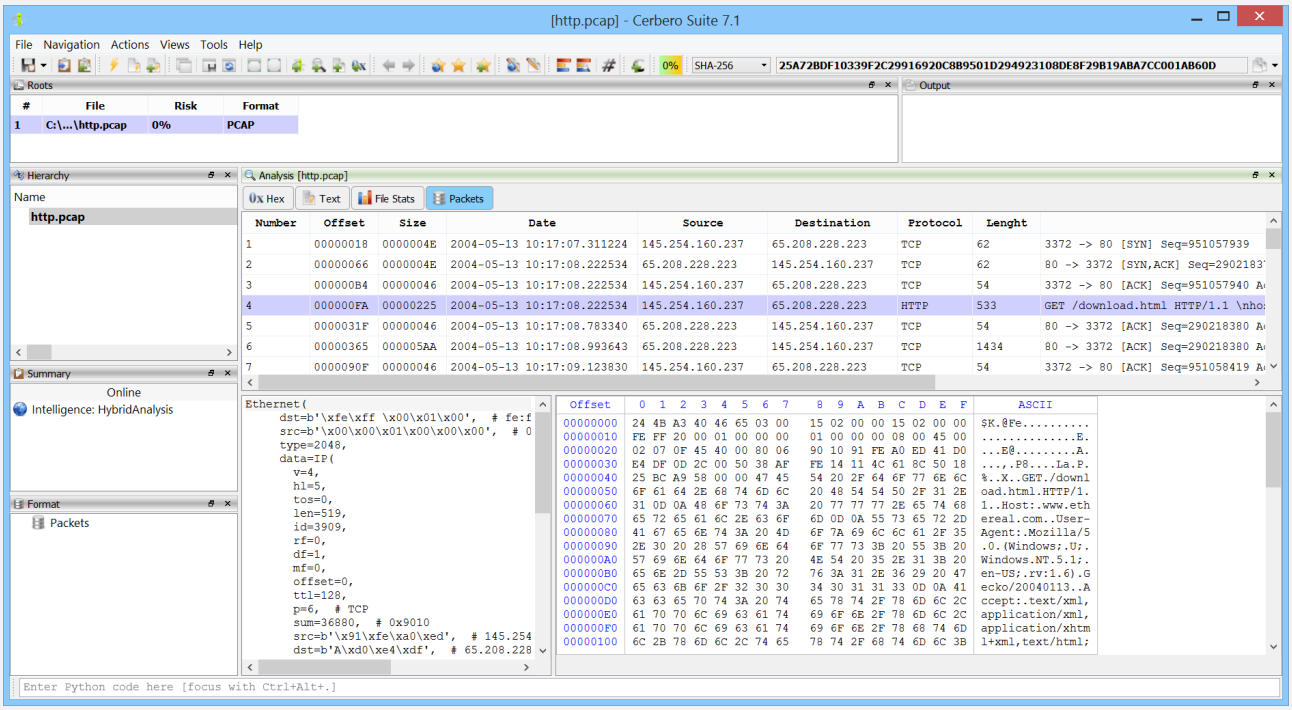
In Apple macOS, .DS_Store is a file that stores custom attributes of its containing folder, such as folder view options, icon positions, and other visual information. It is created and maintained by the Finder application in every folder and contains information that can be valuable for forensics purposes, such as file names and timestamps. This makes these files a rich source for reconstructing user activities, understanding file access patterns, and providing chronological context in digital forensic cases. Their analysis can reveal subtle but critical details about how a macOS system was used, contributing significantly to the overall forensic investigation process.

When the PList Format package is installed, embedded binary PList objects are automatically extracted.



PCAP & PCAPNG

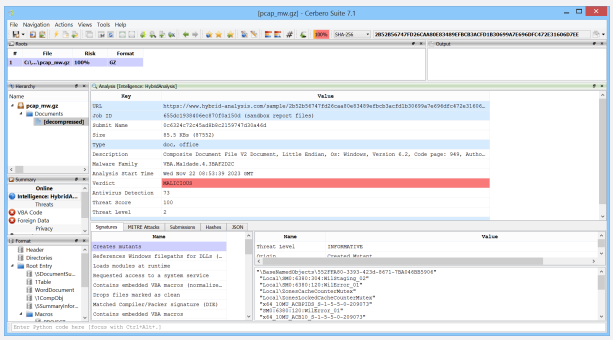
We have released the PCAP Format package for all licenses of Cerbero Suite.



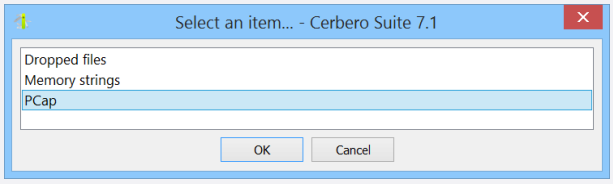
The packets captured in a PCAP file.

The PCAP format is the main capture file format used in TcpDump/WinDump, snort, and many other networking tools and is fully supported by Wireshark/TShark. Our support does not aim to compete against a specialized tool like Wireshark, but it gives the capability to inspect PCAP files without leaving the Cerbero Suite interface. This is especially useful when analyzing malware reports.

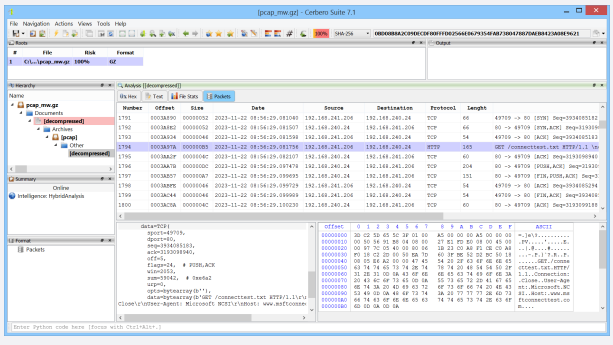
For example, the HybridAnalys Intelligence package allows to download sandbox artifacts by clicking on the 'Job ID' in the report.



By selecting 'PCap', the associated PCAP data is automatically downloaded and added to the project as a child object.



It is now possible to directly inspect the generated traffic without leaving Cerbero Suite.

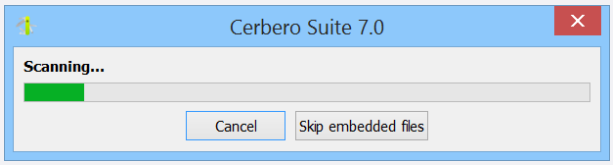


Additionally, the package adds support for the PCAPNG format. The PCAP Next Generation (PCAPNG) format is an enhanced version of the traditional PCAP format, offering features like capturing traffic from multiple interfaces, higher timestamp resolution, support for additional metadata and customizable options, and enriched capture information about the network environment.

TIPS & TRICKS

SINGLE FILE SCAN

To open the main file more quickly when dealing with a file containing numerous embedded files, you can use the ”Skip embedded files” option. This allows you to postpone the scanning of the embedded files, speeding up the initial opening process. Although their scanning is delayed, you retain full access to these embedded files in the UI and can initiate their individual scans whenever you choose to explore them.



REGISTRY HIVES VIA PYTHON

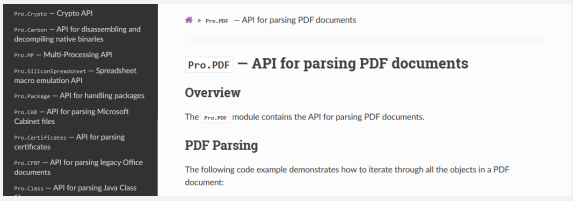
Windows Registry hives are fully integrated into Cerbero Suite, offering support both through the user interface and the Python SDK. The latter approach is particularly beneficial for creating versatile plugins for malware scanning and artifact detection. To illustrate, here’s a concise example demonstrating how to access keys and values using Python:

```
from Pro.Core import *
from Pkg.RegHive import *

def parseRegHive(fname):
  c = createContainerFromFile(fname)
  if c.isNull():
    return
obj = RegHiveObject()
if not obj.Load(c) or not obj.Parse():
  return
# retrieve the root key
key = obj.GetRegKey()
print(key.Name())
# enumerate sub-keys
for subkey in key.IterateSubKeys():
  print(" ", subkey.Name())
  # enumerate values for each sub-key
  for v in subkey.IterateValues():
    print("    ", v.name, v.value_type,
        ↪ v.value)
```

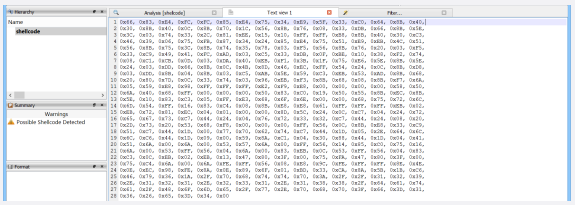
PDF SDK DOCUMENTATION

Navigating the intricacies of PDF manipulation is now easier, thanks to the comprehensive documentation of our PDF module. This provides invaluable help to developers that want to parse PDF documents using either Cerbero Suite or Cerbero Engine.

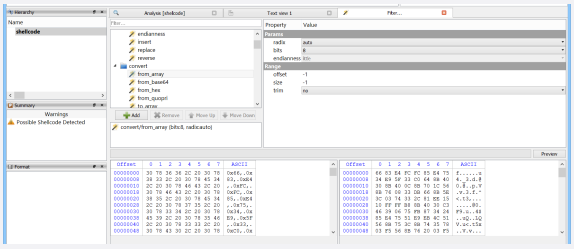


ARRAY VALUES EXTRACTION

It is often necessary the raw values from a numerical text array, such as: 0x01, 0x02, 0x03, etc.



The ”convert/from_array” filter is an incredily useful tool that performs this task for us. It automatically detects separators and the radix of the values. Additionally, the radix, the size, and the endianness of the values can all be configured.



Knowing how to use this tool can save you a considerable amount of time!

CERBERO LABS

If you have any questions, feel free to contact us at: info@cerbero.io

You can follow us on X to be notified about the latest updates!