Protect code execution

Once the operating system is configured to reduce the ability to execute malware or unauthorized access activity, it is necessary to review the characteristics and execution capabilities of the different applications and programs.

> How do we know if a program we download from the Internet contains malware?
>
> What tools are available in the operating system itself to prevent malware from running or minimize the impact if a malicious application is run?

Publishing a Hash associated with a file or program available for download makes it more difficult to modify the program with malware.

Windows PowerShell uses **get-filehash** to verify the signature of a file.

Cryptographic software signature

One of the best guarantees for running legitimate software is through the cryptographic signature of the program manufacturer. Digital certificate legitimizes the authorship of a product, and makes it very difficult to modify software to add malware.

There are some tools that allow you to verify the digital certificate associated with a certain manufacturer. From the properties of the executable image itself you can see the digital certificate. In addition, sysinternals tools offers us to verify that digital certificate.

Sigcheck

Sysinternals Suite tools are available for free download on the page https://learn.microsoft.com/en-us/sysinternals/ there is a specific one to perform file signature checks: **Sigcheck**

usage: sigcheck [-a][-h][-i][-e][-l][-n][[-s]|[-c|-ct]][-m]][-q] [-r][-u][-vt][-v[r][s]][-f catalog file] <file or directory>

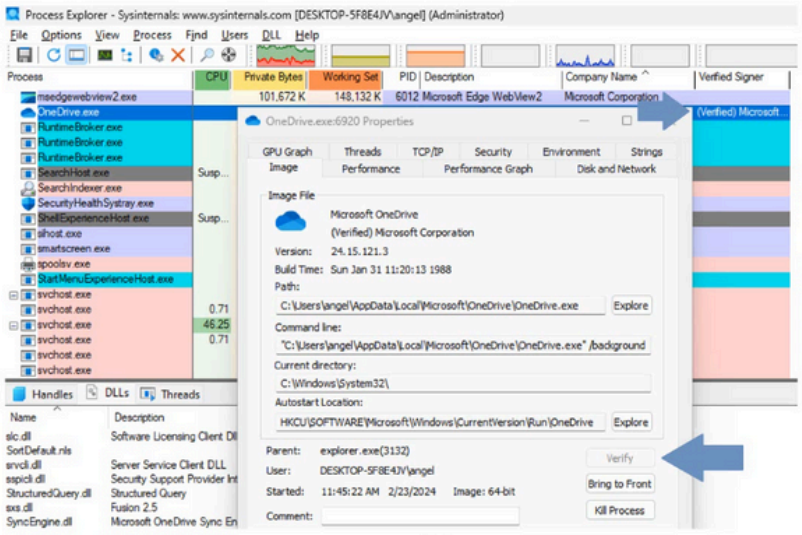
usage: sigcheck -d [-c|-ct] <file or directory>

usage: sigcheck -o [-vt][-v[r]] <sigcheck csv file>

usage: sigcheck -t[u][v] [-i] [-c|-ct] <certificate store name|*>

Sysinternals Suite: Process Explorer

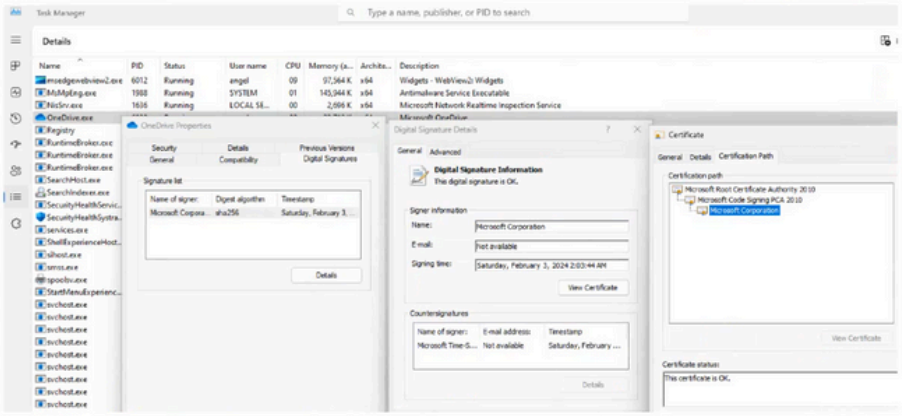
Process Explorer also allows you to verify the signature of an executable, even from the running process itself. In addition to being able to send or verify that process with Virus Total.



Pictures own elaboration

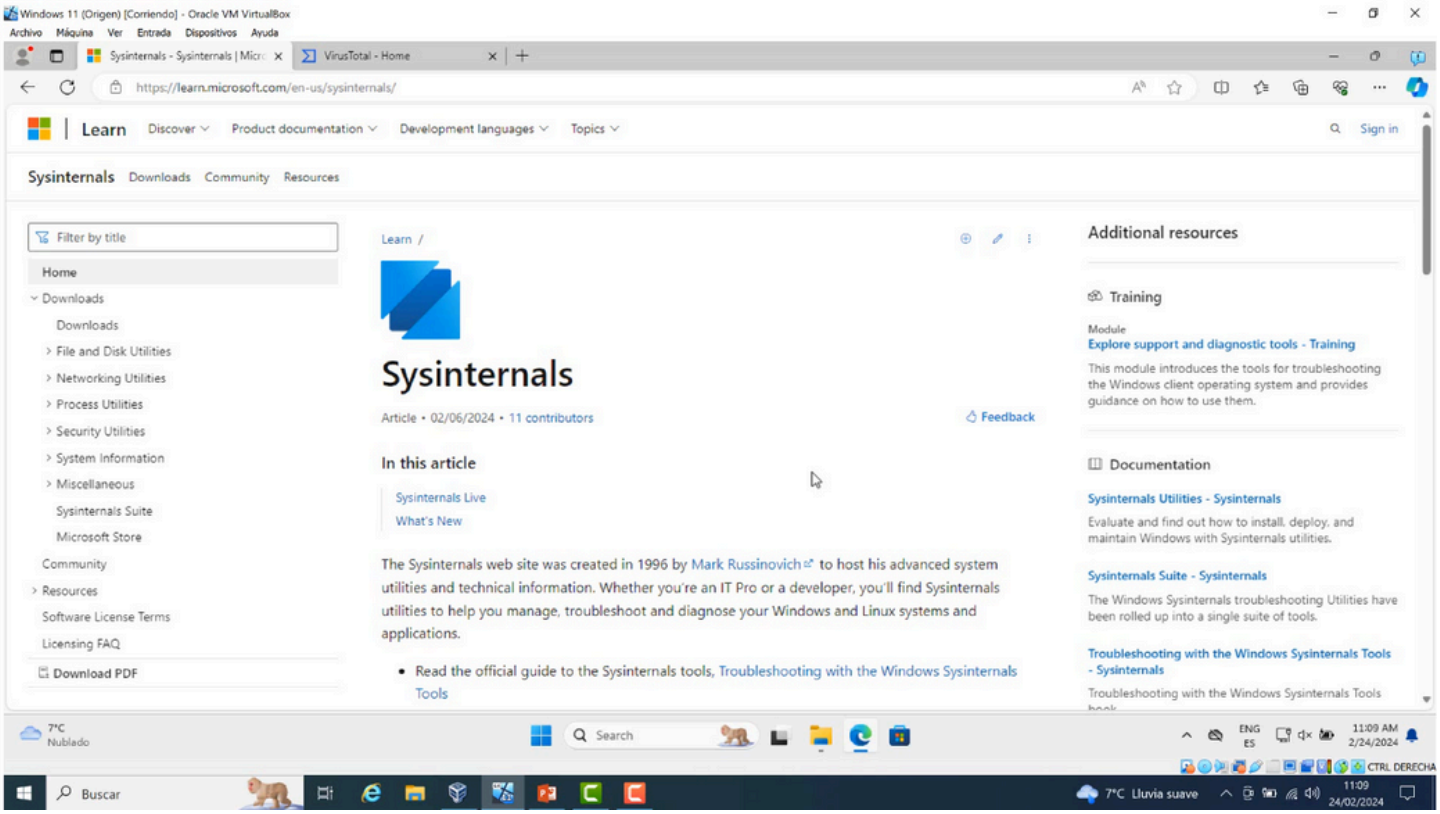
Demo

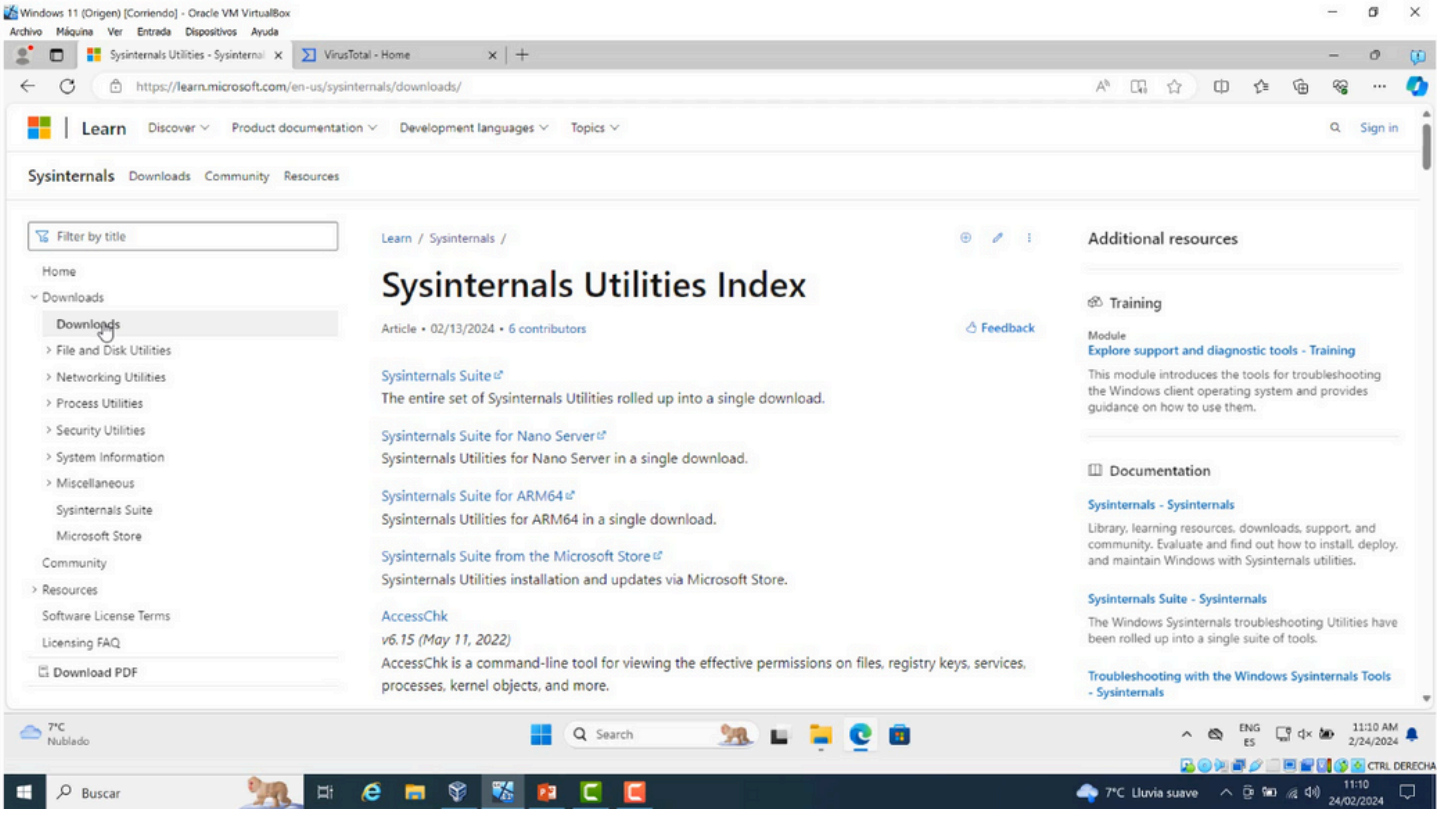
- Verify the digital certificate of a process from the Task manager.
- Verify that certificate from Process Explorer.



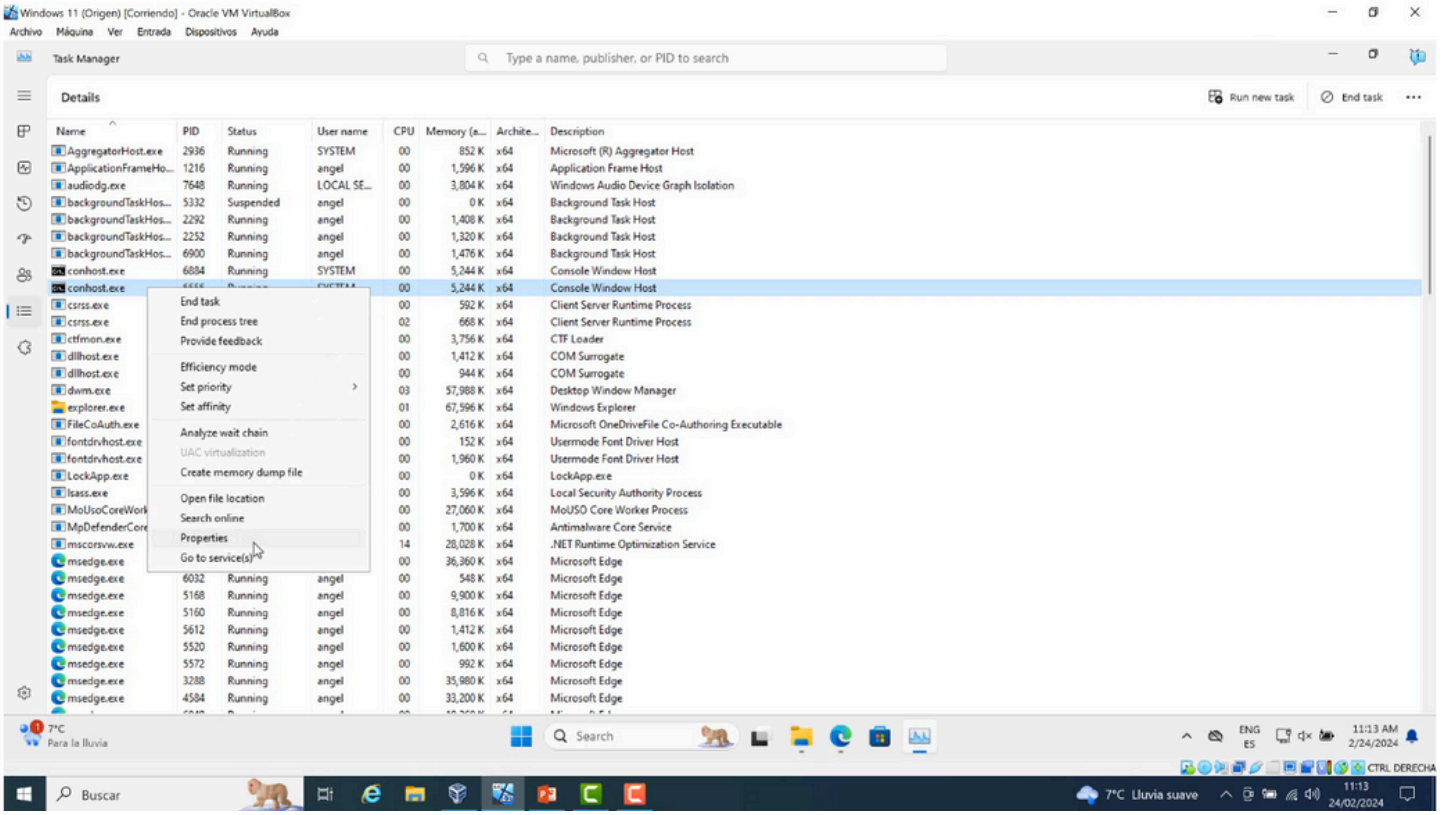
Pictures own elaboration

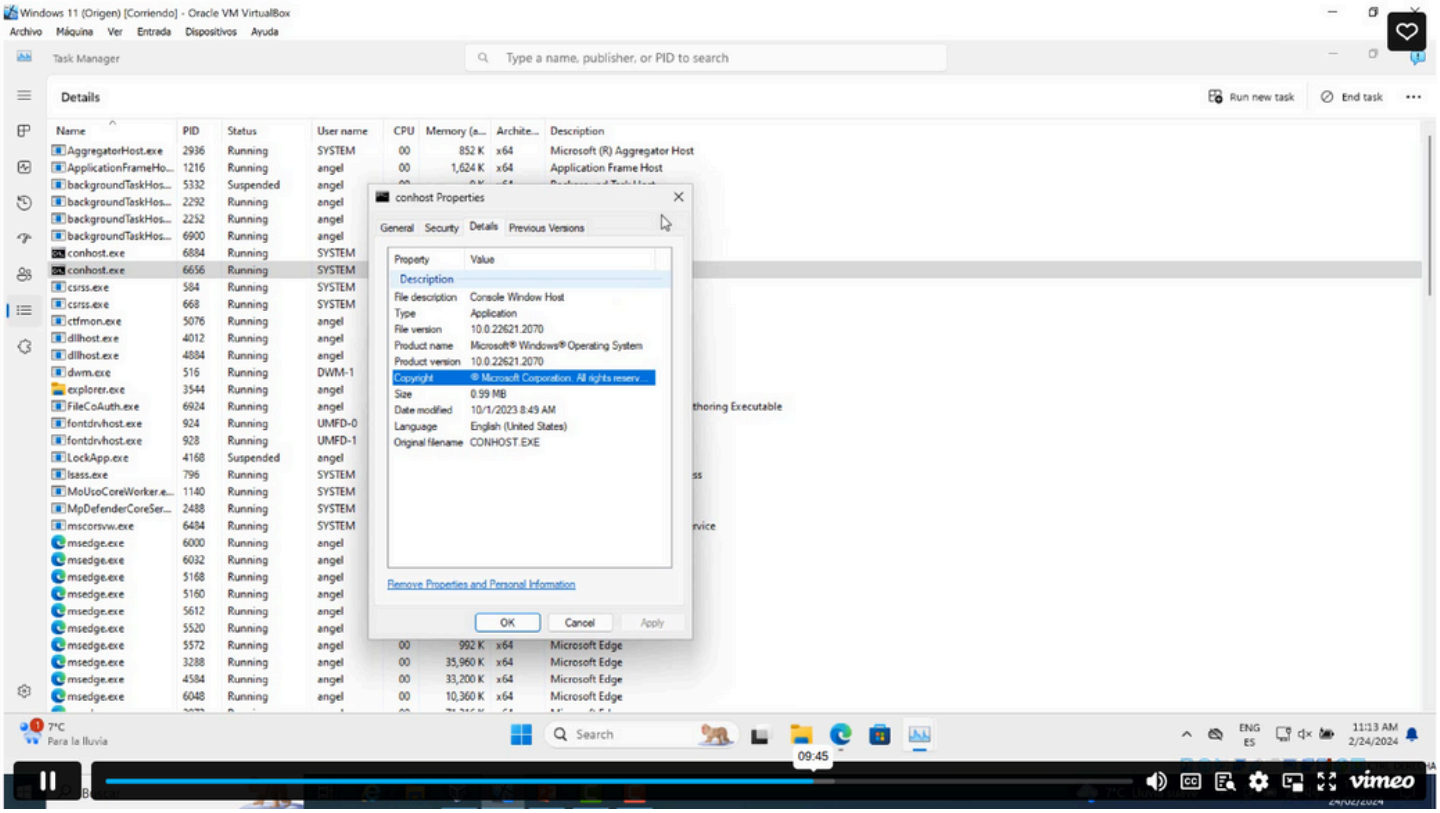
Sys internals, presentación:



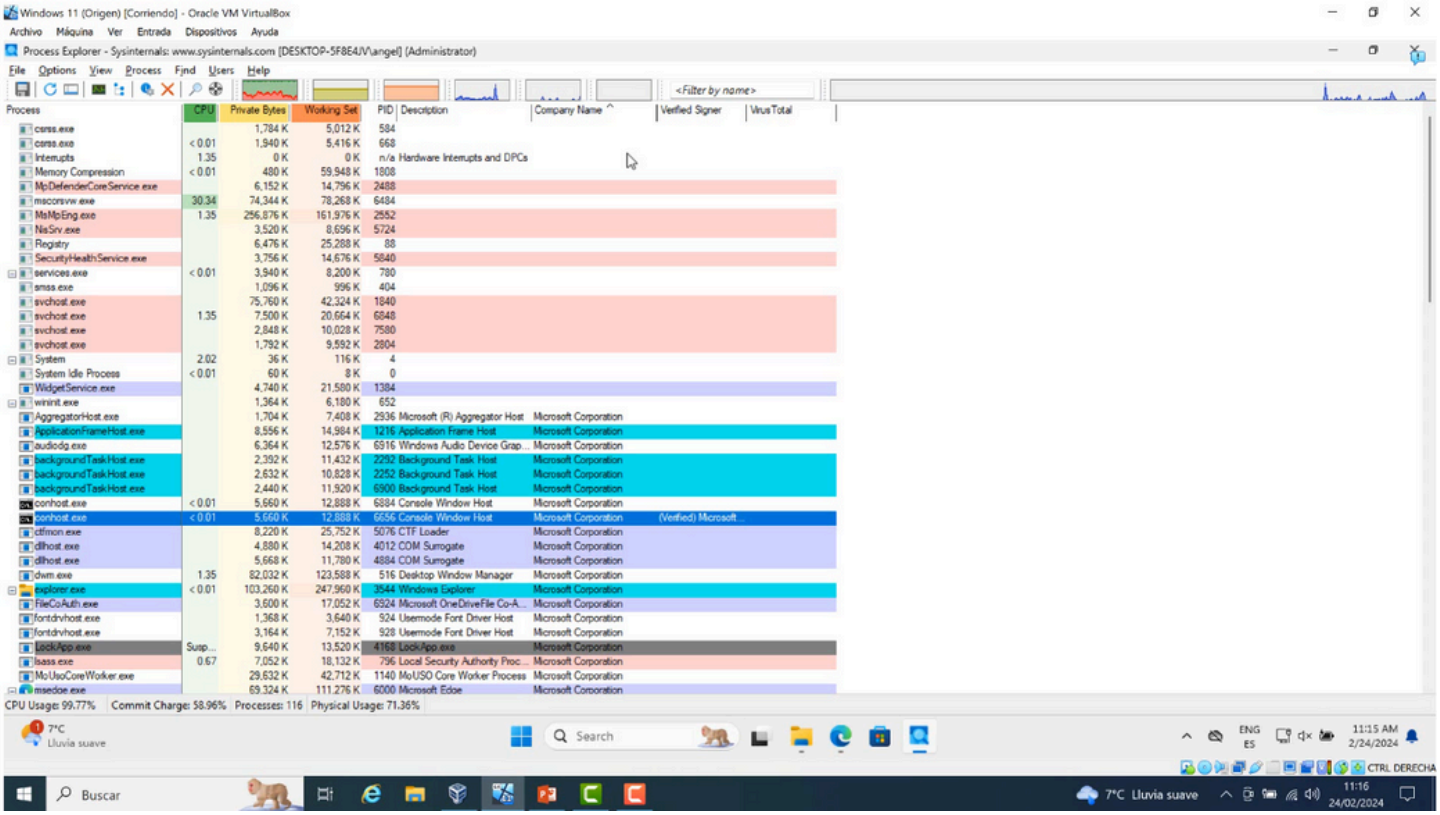


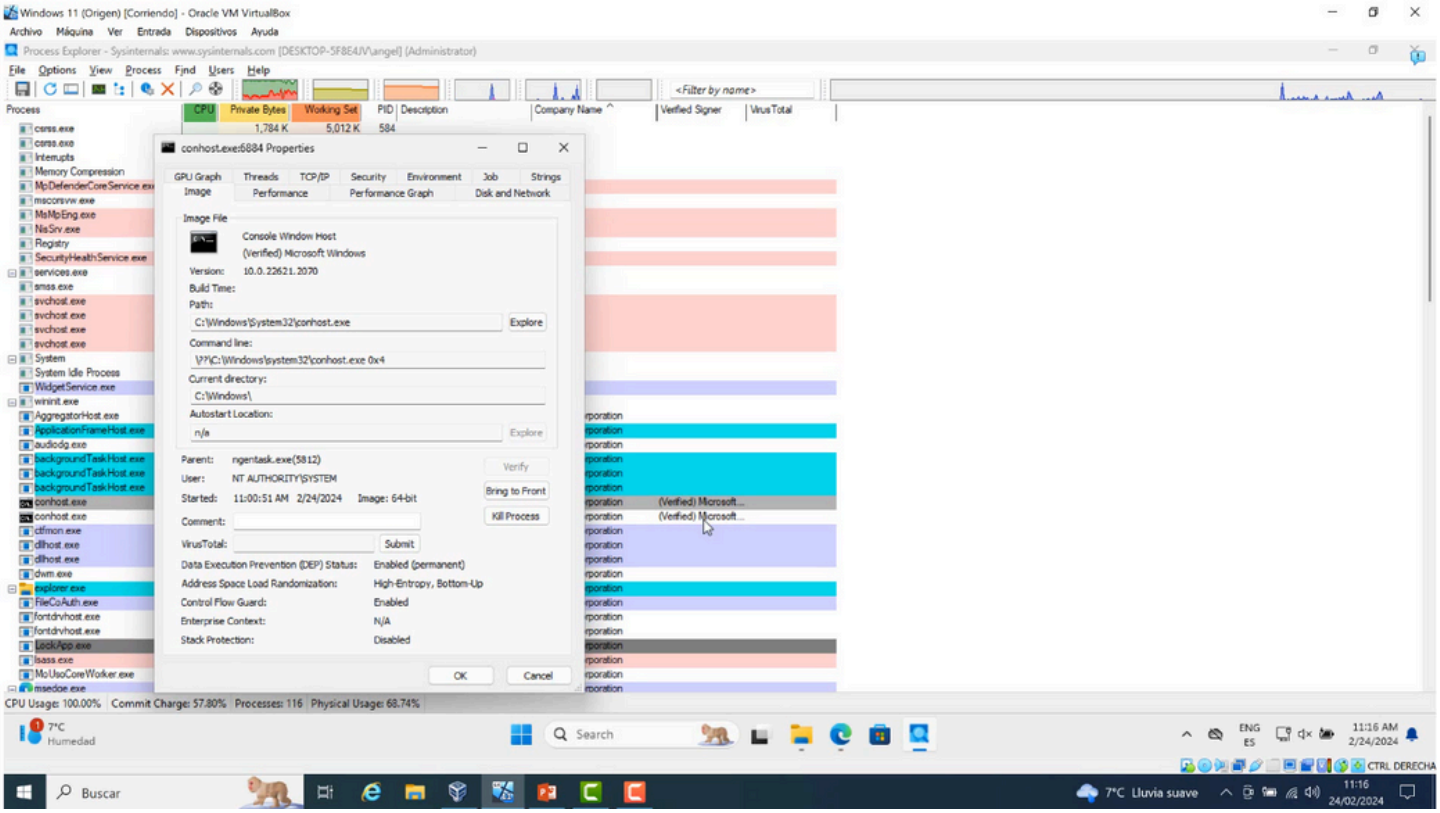
Con Task manager, verificar la firma digital y el copyright:



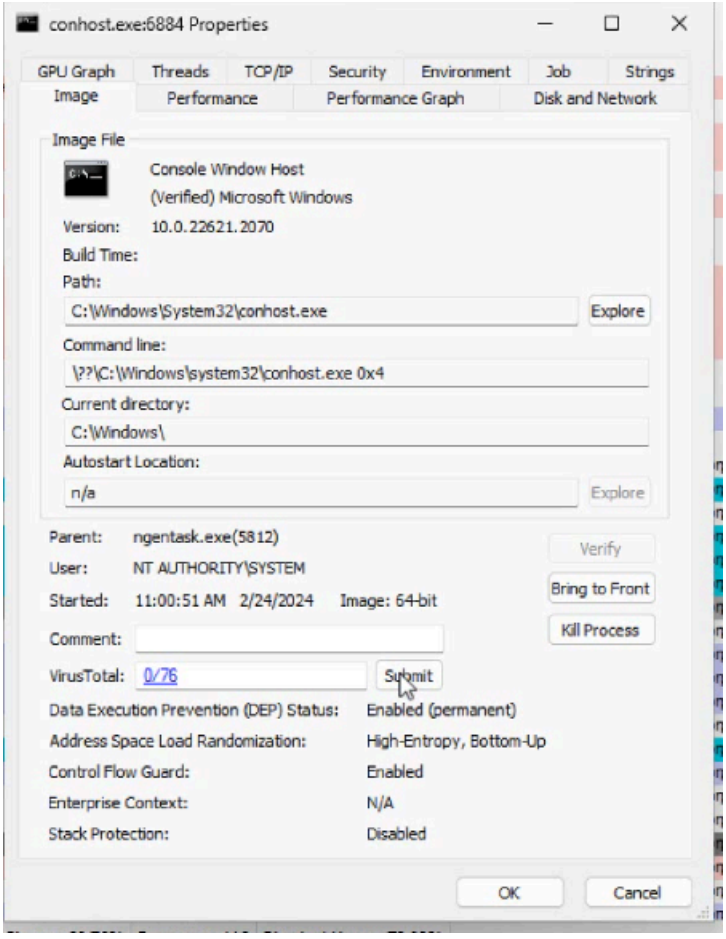


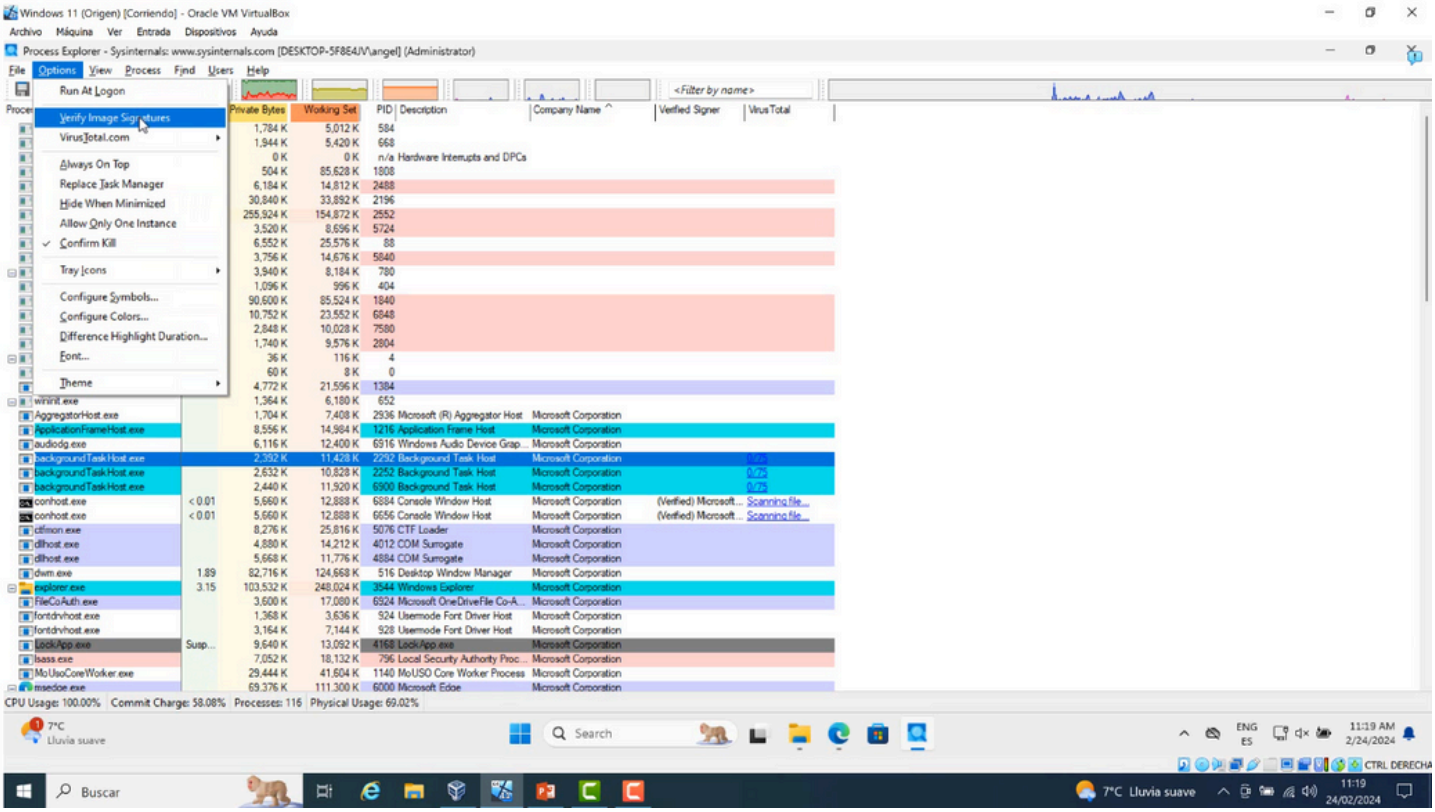
Vamos a verificar la firma digital usando Sysinternals ahora, mas preciso con process explorer:





Podemos enviarlo a Virus Total para mayor inspección, análisis con ese determinado hash del archivo en la base de datos de Virus Total:





Conclusions

- There are several tools that allow you to verify the origin of the software, in this way the execution of malicious software is prevented, or at least made more difficult.
- The sysinternals suite of tools offers us a wide number of utilities for different security purposes, such as the possibility of verifying digital certificates associated with the signing of programs and applications.

Singularity Hackers 0xWORD My Public Inbox