

Forum:[Hack Forums](#)

Thread: [Computer Forensics Tools \(7\) Explained for beginners](#)

B3A - April 22, 2023, 6:33 am

Process Explorer : Process Explorer keep an eye on the processes running on your computer. The display is split into two parts. The top part lists all the processes currently active on your computer and tells you who owns each one. The bottom part changes depending on what mode you're in. If you're in handle mode, you'll see all the handles that the selected process in the top window has opened. If you're in DLL mode, you'll see all the DLLs and memory-mapped files that the process has loaded. Additionally, Process Explorer has a search function that allows you to quickly find out which processes have particular handles or DLLs loaded.

Link : https://filehippo.com/download_process-explorer/

Autoruns: Autoruns shows you what programs are configured to run during system bootup or login, and shows you the entries in the order Windows processes them. These programs include ones in your startup folder, Run, RunOnce, and other Registry keys.

Link : https://filehippo.com/download_autoruns/

Irfan View : IrfanView is a very fast and small Freeware (for non-commercial use) graphic viewer for Windows.

Link : <https://www.irfanview.com/>

Fport: Shows which applications are using which open ports for communication. It gives you the same information as the 'netstat -an' command, but with additional details like the process ID, name and path. It's helpful for figuring out which programs are using unknown open ports."

Adapterwatch : AdapterWatch displays useful information about your network adapters: IP addresses, Hardware address, WINS servers, DNS servers, MTU value, Number of bytes received or sent, The current transfer speed, and more. In addition, it displays general TCP/IP/UDP/ICMP statistics for your local computer.

Link : <http://www.nirsoft.net/utils/awatch.html>

Visual TimeAnalyzer: Visual TimeAnalyzer automatically tracks all computer usage and presents detailed, richly illustrated reports.

Link <https://www.neuber.com/timeanalyzer/download.html>

SIW: SIW is an advanced System Information for Windows tool that analyzes your computer and gathers detailed information about system properties and settings and displays it in an extremely comprehensible manner.

Link : <https://www.gtopala.com/siw/siw-trial.php>

Bonus :
[attachment=1326]

J4wKn33Bl4z3 - April 26, 2023, 4:53 pm

RE: Computer Forensics Tools (7) Explained for beginners

gg [warn]

B3A - May 1, 2023, 12:52 am

(Apr 26, 2023 04:53 PM)J4wKn33Bl4z3 Wrote: [\[CITE\]](#) RE: Computer Forensics Tools (7) Explained for beginners

gg [warn]

If that means you liked it im glad my friend

samasugeti - March 6, 2025, 10:53 pm

I would like to take a look, are these actual?

HerrWinston - May 28, 2025, 2:55 am

nice explanation, the website seem good, good tutorial

CosmicZexel - May 28, 2025, 1:03 pm

These tools seem to be pretty neat. Definitely have to check out Process Explorer when I get a chance to later. Great post OP!

xdc1-4 - June 1, 2025, 12:45 am

Thank you, my friend. Thank you