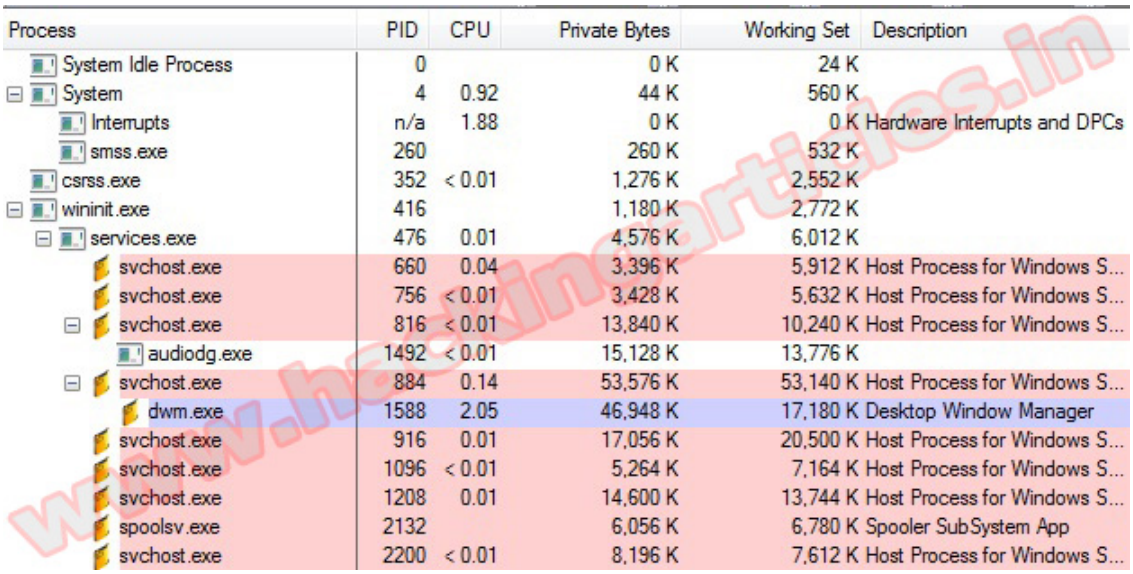
List of Computer Forensics Tools (Part 1)

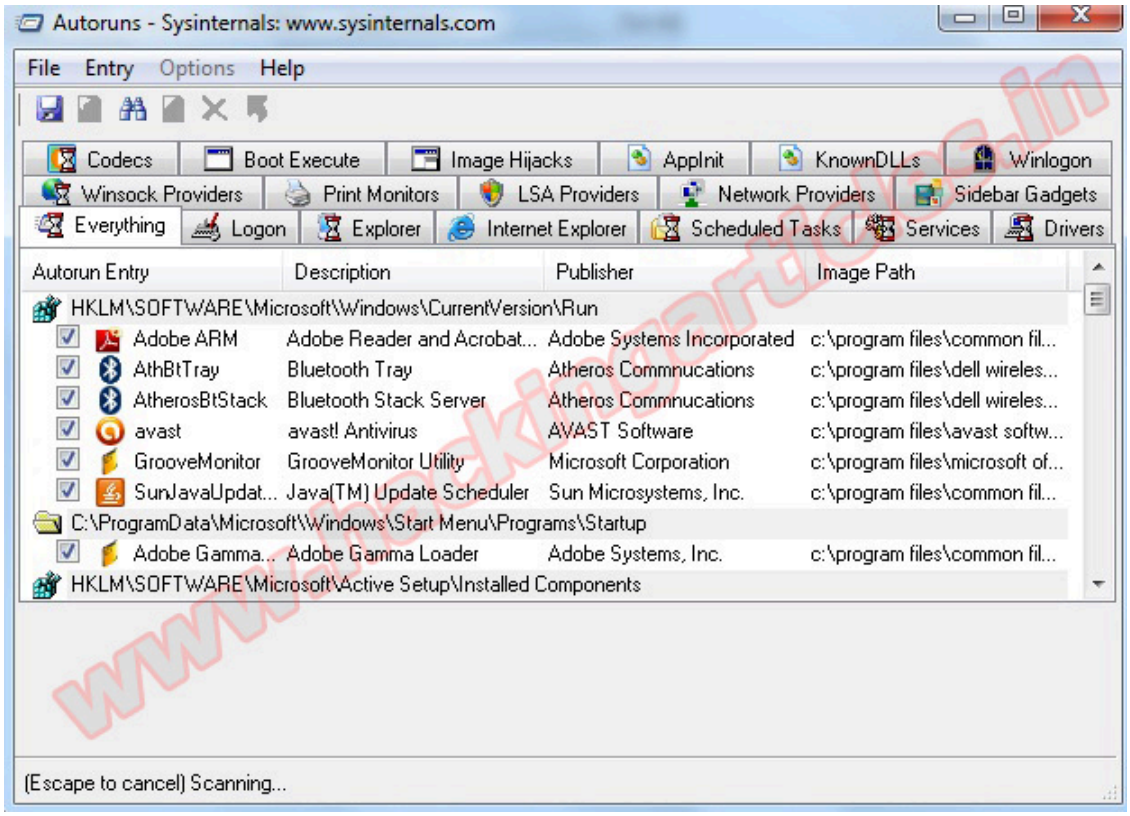
September 6, 2011 By Raj Chandel

Process Explorer: The Process Explorer display consists of two sub-windows. The top window always shows a list of the currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode that Process Explorer is in: if it is in handle mode you'll see the handles that the process selected in the top window has opened; if Process Explorer is in DLL mode you'll see the DLLs and memory-mapped files that the process has loaded. Process Explorer also has a powerful search capability that will quickly show you which processes have particular handles opened or DLLs loaded.

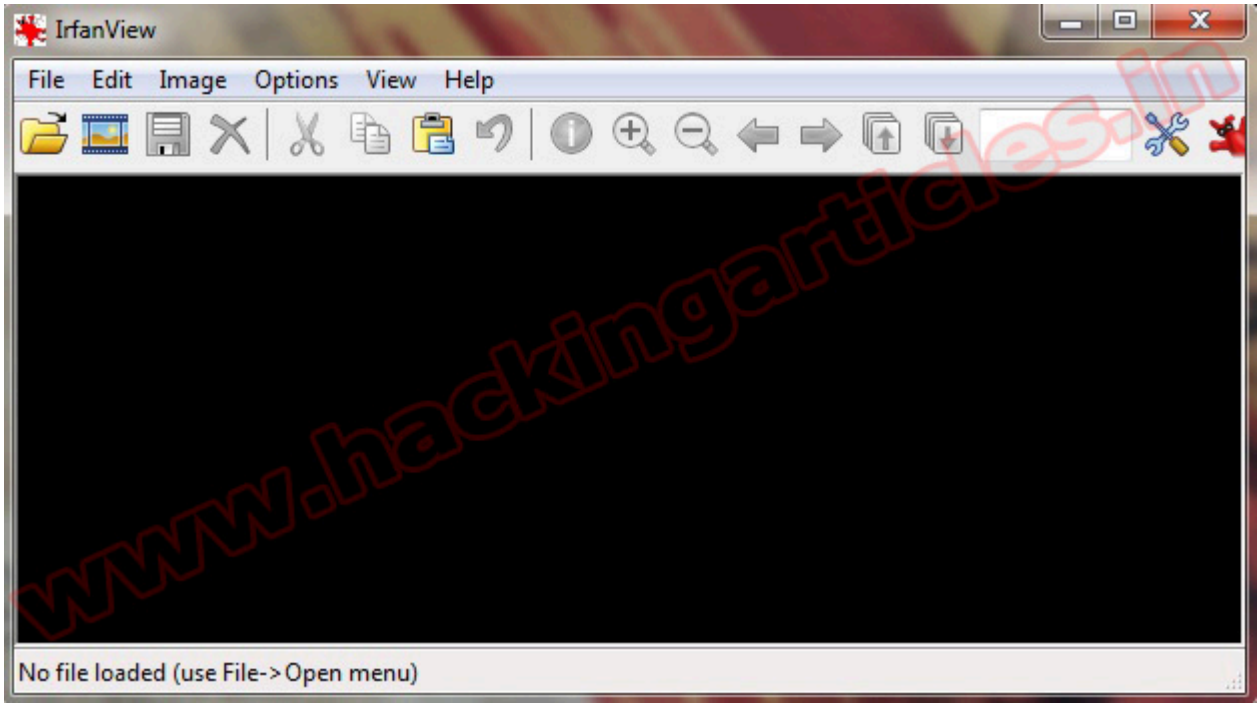


Process	PID	CPU	Private Bytes	Working Set	Description
System Idle Process	0		0 K	24 K	
System	4	0.92	44 K	560 K	
Interrupts	n/a	1.88	0 K	0 K	Hardware Interrupts and DPCs
smss.exe	260		260 K	532 K	
csrss.exe	352	< 0.01	1,276 K	2,552 K	
wininit.exe	416		1,180 K	2,772 K	
services.exe	476	0.01	4,576 K	6,012 K	
svchost.exe	660	0.04	3,396 K	5,912 K	Host Process for Windows S...
svchost.exe	756	< 0.01	3,428 K	5,632 K	Host Process for Windows S...
svchost.exe	816	< 0.01	13,840 K	10,240 K	Host Process for Windows S...
audiodg.exe	1492	< 0.01	15,128 K	13,776 K	
svchost.exe	884	0.14	53,576 K	53,140 K	Host Process for Windows S...
dwm.exe	1588	2.05	46,948 K	17,180 K	Desktop Window Manager
svchost.exe	916	0.01	17,056 K	20,500 K	Host Process for Windows S...
svchost.exe	1096	< 0.01	5,264 K	7,164 K	Host Process for Windows S...
svchost.exe	1208	0.01	14,600 K	13,744 K	Host Process for Windows S...
spoolsv.exe	2132		6,056 K	6,780 K	Spooler SubSystem App
svchost.exe	2200	< 0.01	8,196 K	7,612 K	Host Process for Windows S...

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.

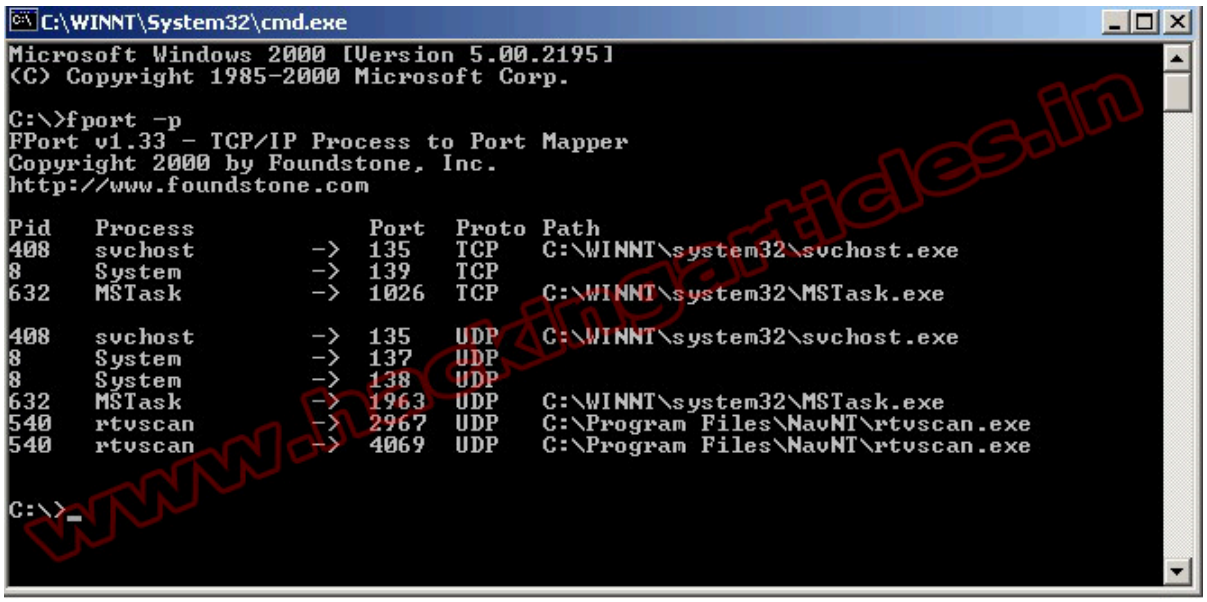


Irfan View : IrfanView is a very fast, small, compact and innovative Freeware (for non-commercial use) graphic viewer for Windows.

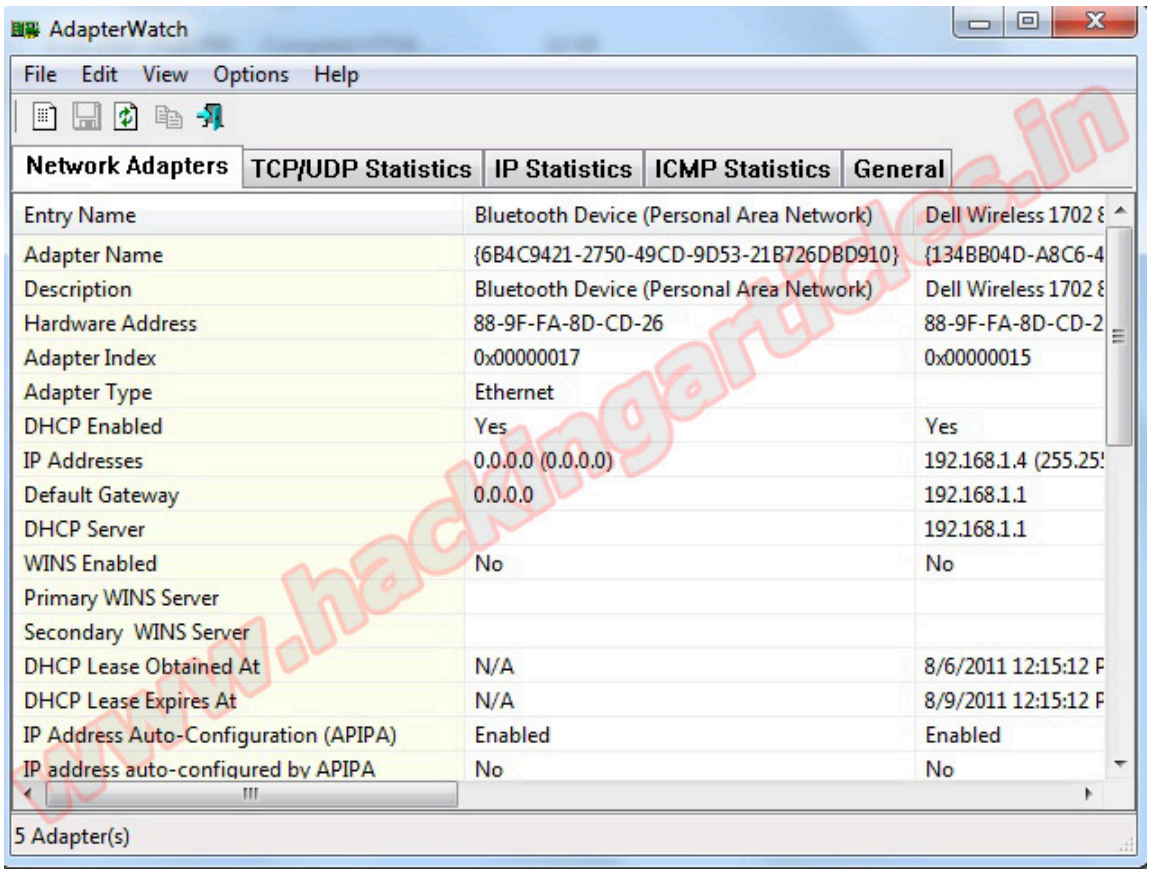


Fport :fport reports all open TCP/IP and UDP ports and maps them to the owning application. This is the same information you would see using the 'netstat -an' command, but it also maps those ports to running processes

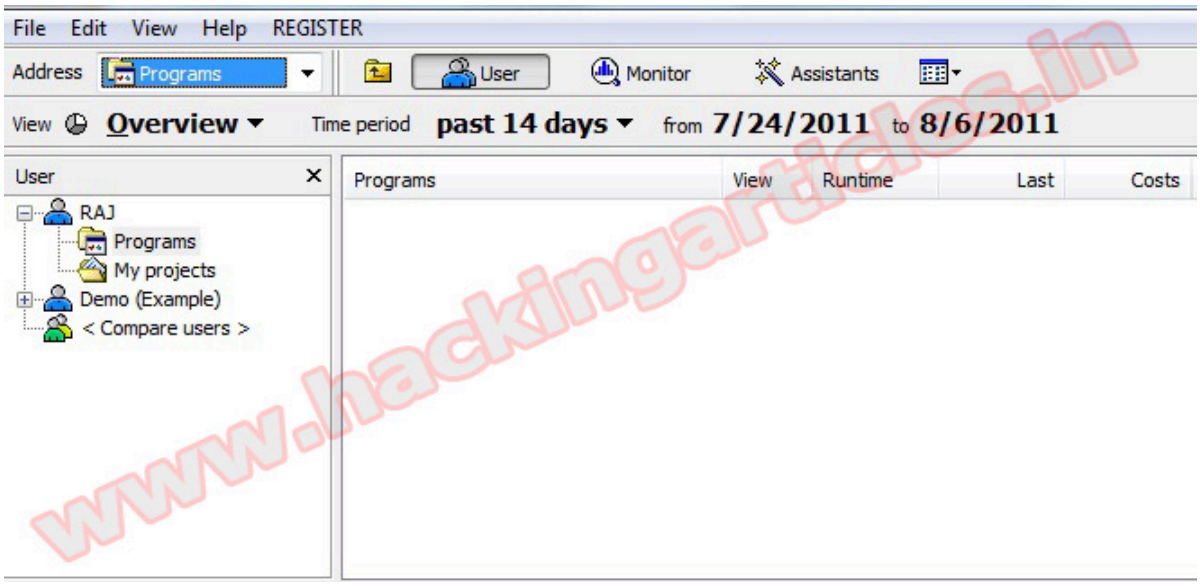
with the PID, process name and path. Fport can be used to quickly identify unknown open ports and their associated applications.



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.



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



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.