

The background features an abstract geometric design. It includes three concentric circles in shades of blue, positioned in the upper right and lower right areas. Two thin, light blue lines intersect to form a large 'V' shape that points towards the center of the cover. The overall aesthetic is clean and modern.

# **Malware Analysis & Tools**

By Jeffrey Farnan



# Contents

<b>1. Malware Analysis.....</b>	<b>3</b>
▪ <b>Static Analysis.....</b>	<b>3</b>
▪ <b>Dynamic Analysis.....</b>	<b>3</b>
<b>2. Malware Analysis Tools.....</b>	<b>4</b>
▪ <b>Static Analysis Tools.....</b>	<b>4</b>
▪ <b>Dynamic Analysis Tools.....</b>	<b>7</b>
<b>3. Malware Detection Tools.....</b>	<b>10</b>
▪ <b>VirusTotal.....</b>	<b>10</b>
▪ <b>Sysinternals Suite .....</b>	<b>11</b>
▪ <b>Hex Editor.....</b>	<b>12</b>
▪ <b>Windbg.....</b>	<b>13</b>

# Malware Analysis

Malware Analysis is the study of programs behaviour; there are many ways and tools which allow you to gain as much information from a suspicious program.

There are two approaches to analysing malware: static and dynamic analysis. Static analysis is analysing the malware without executing it. This involves using various tools to glean as much information from the source code, about what it does. Dynamic Analysis is executing the program in a controlled environment and analysing its behaviour and what's it's doing.

## Static Analysis

Static Analysis is a way to study the programs behaviour, without actually executing it, there are tools such as decompilers, disassemblers, and source code analysers all which help to determine what its intentions are. An advantage of static analysis is that it gives an indication of what to look out for in the dynamic analysis, an example would be if a IP address, was viewed in the code, during the dynamic analysis it might try to contact this address over the internet.

## Dynamic Analysis

In dynamic analysis the executable is run in a controlled environment or a "Sandbox" as it's known. This controlled environment is usually set up in a virtual machine and is usually a basic OS with nothing of importance stored on it. Dynamic analysis uses tools such as debuggers and packet sniffers. Dynamic analysis is about monitoring the system as the program is running and studying what changes its making to the system, what files it accesses, what changes to files it makes like adding or deleting files, remote logging: what external URLs or IP addresses does it connect to.

# Malware Analysis Tools

This section will take you through the different technology used for analysis. Books have been written about some of these applications, they have complex functionality, here will be a brief overview of each application and the functionality which was helpful.

## Static Analysis Tools

### IDA PRO

The Interactive Disassembler, or simply known as IDA is a disassembler and debugger. It's an application which has many features such as programmable, extendible and a multi-processor disassembler which can be run on the leading operating systems. IDA both supports the x86 and x64 architectures. IDA supports many file formats such as Portable Executable (PE), Executable and Linking Format (ELF), Common Object (COFF). IDA PRO can disassemble a program and let you perform tasks such as function discovery, local variable identification and stack analysis, plus much more. Using IDA Pro lets you dig deeper into a program, allowing you to dig deeper into what it's doing and its intentions.

### Using IDA PRO

You load an executable into IDA Pro by either dragging it in or by opening up the application and selecting it. First IDA Pro will recognise the file's format and its processor architecture. IDA maps the PE file into memory as if loaded by the operating system loader. Different options are available to disassemble the file either by PE format, MS-DOS executable or binary format.

- PE Format:
- MS-DOS executable :
- Binary File: which disassembles the file as raw data, allowing extracting more information than the PE format.

- **Manual Mode**

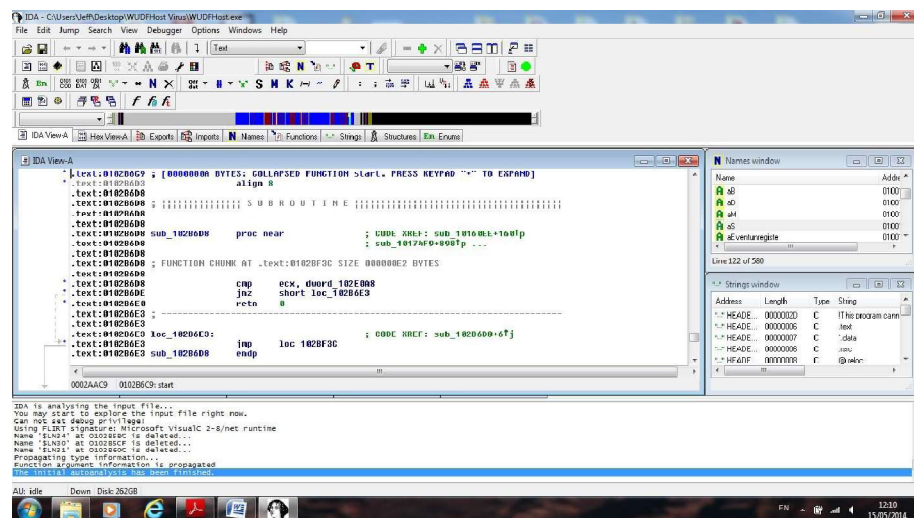
IDA Pro does not load the PE header and the resources sections by default, by clicking Manual mode loads each section manually, so no section would escape analysis.

- **The Interface**

After loading has complete, the disassembly window is opened. This is where the assembly code resides and where you can view the Functions, Imports and Exports and Strings windows, etc. IDA comes with different modes to view the binaries, Graph mode and Text mode, to simply change between modes press the space bar.

- **Text mode**

The text mode displays a traditional view of the binary data regions, allowing you to view the memory addresses, the section name (.text) and opcodes (83EC18).



- **Graph mode**

Graph mode displays operation codes and line numbers, plus allowing you to view the programs flow. Arrows indicate the paths the program flows in based on particular decisions having been made. The green arrow displays if a conditional jump is taken, red if it is not taken, and blue displays an unconditional jump. Upward arrows indicate loop situations.

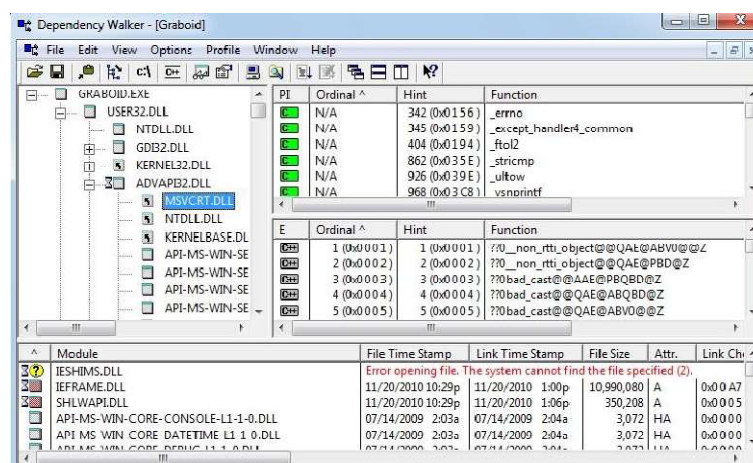
## IDA windows

- **Functions window:** Displays all functions listed in the executable showing the length of each.
- **Names window:** displays address, functions, code, data and strings which has a name attached to it.
- **Imports window:** All imported DLL's the executable uses are listed.
- **Exports window:** All exported functions are listed for a file.
- **Structures window:** Lists all active data structures.
- **Strings window:** Shows all strings of text.

When analysing code these windows are particularly important, allowing you to cross-reference functions, by double clicking on an item of interest, it jumps directory to the main body of the code where that item is located.

## Dependency Walker

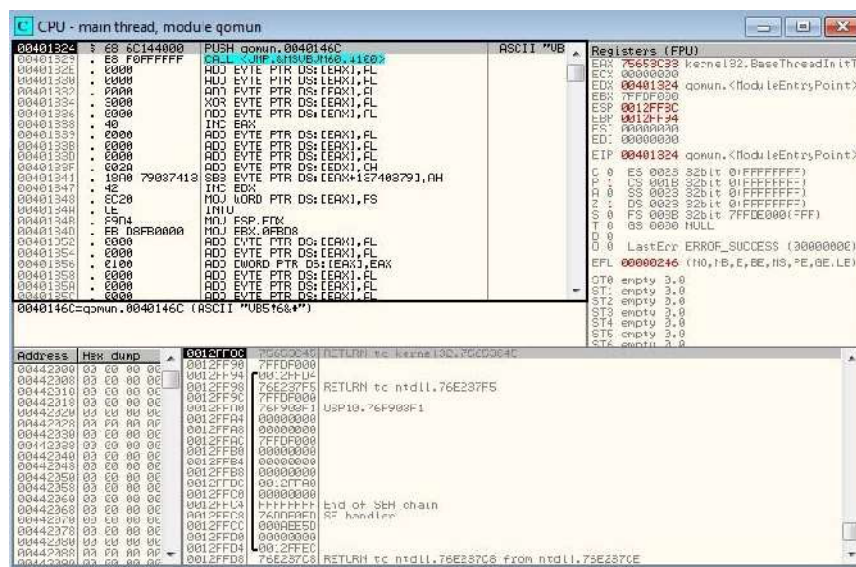
The Dependency Walker tool can scan for all dependent DLL's used by a program, including missing DLLs and DLLs which are not valid. Dependency walker checks for import and export function match. Dependency Walker can help correct and prevent problems, with the use of DLLs.



## Dynamic Analysis Tools

### OllyDbg

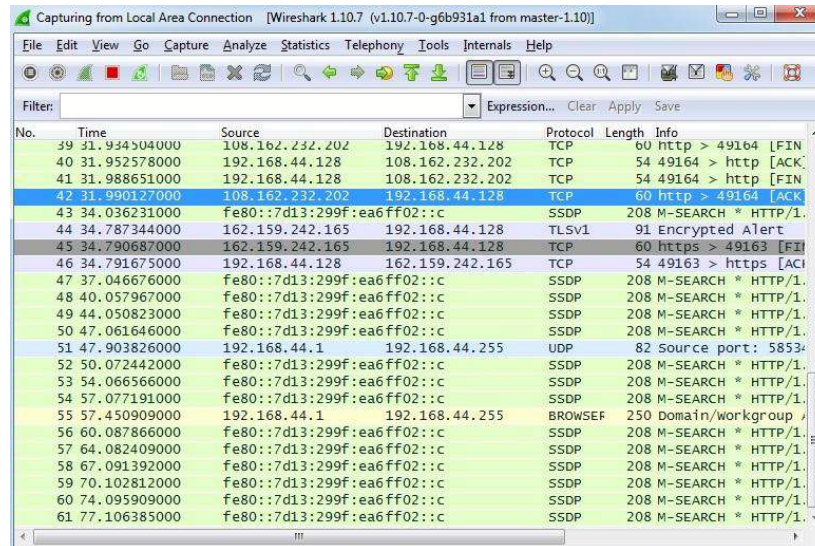
OllyDbg is an assembler level debugger for windows 32-bit executables. It analyses binary code, can be used to correct programs or go in dept in analysing assembly level code when no source code is available. You can view the assemble as its runs and see what changes its making to memory, what procedures and API calls its making, what DLLs are been used.



- **CPU/Coding Panel:** This is the largest panel, and displays all assemble code produced. If stepping through it line-by-line, the code is highlighted showing the assemble code as its executing.
- **Registers Panel:** The registers panel is at the right hand side, and is used for holding information on the flags, standard and section registers plus extra information
- **Stack Panel :** The stack panel holds addresses which are used in the disassembles such as CPU section or memory dump section.
- **Memory Dump:** This is a dump for the memory addresses. Any raw data displayed alongside these addresses can be displayed in different formats such an ASCII, UNICODE, etc.

## Wireshark

Wireshark is a network protocol analyser and the standard application used by network analysts. Wireshark is a network packet analyser which is used to capture network traffic and analyse the different protocols.



Some of Wireshark's feature set include:

- Deep inspection of all standard and new protocols
- Live packet capture plus offline analysis
- Network data can be viewed via a GUI or browsed via the TShare utility or TTY-mode.
- Can read and write different data capture formats from other sniffer and network monitor applications.
- Live data can be read from other channels such as 802.11, Ethernet, PPP/HDLC Bluetooth, etc.

Some of Wireshark's feature set include:

- Deep inspection of all standard and new protocols
- Live packet capture plus offline analysis
- Network data can be viewed via a GUI or browsed via the TShare utility or TTY-mode.
- Can read and write different data capture formats from other sniffer and network monitor applications.



## **Sandboxes**

Virtualisation Software provides a save and time saving environment to test malware. Easy to set up and configure a lab environment can be set up in minutes. A virtual machine allows you to investigate the behavioural analysis of the malware sample, by how the specimen interacts with the file system, registry and the network.

- With a virtual machine, it's possible to take a snapshot of the systems state before, during and after and infection takes place. This allows identification of what changes to the system were made.
- The host-only option allows you to interconnect virtual systems.
- Update the security patches regularly.
- Don't enable networking on the virtual machine
- Do not connect the virtual machine to the host machine
- Monitor the host for any signs of infection from the virtual machine.

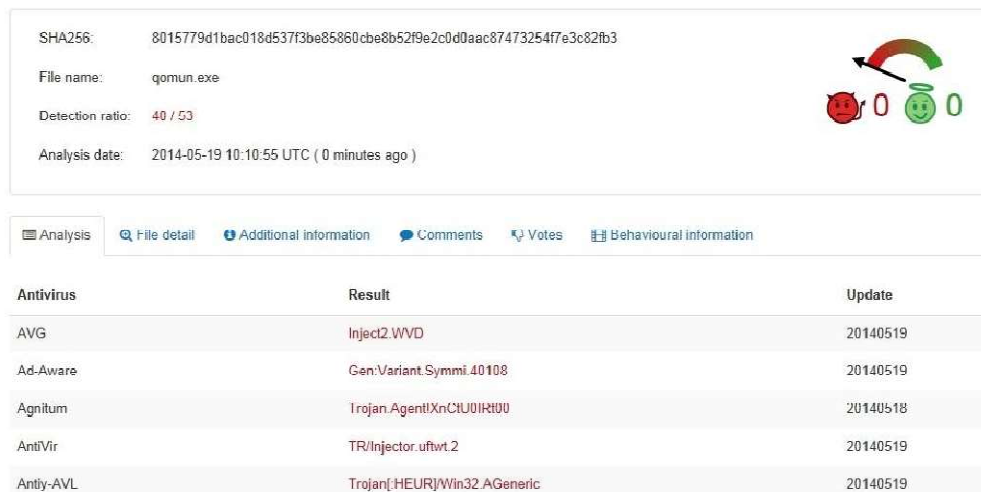
## Malware Detection Tools

There are a number of tools used for spotting malware.

### VirusTotal

VirusTotal is an online service which analyses suspicious executables files which are uploaded by the users. It quickly detects the different malware types such as Trojans, viruses and worms. It gives an indication if the file is harmful or not, with a 0/50 rating.

When a file is uploaded and the content of the file is scanned by 40 different Antivirus engines all at the same time. The information gathered by these antivirus engines is outputted and a rating is given as to how harmful the file is.



The screenshot shows the VirusTotal analysis interface. At the top, it displays the SHA256 hash, file name (qomun.exe), detection ratio (40 / 53), and analysis date (2014-05-19 10:10:55 UTC). A progress bar and a rating of 0/50 are also visible. Below this, there are tabs for Analysis, File detail, Additional information, Comments, Votes, and Behavioural information. The main section is a table with three columns: Antivirus, Result, and Update.

Antivirus	Result	Update
AVG	Inject2.WVD	20140519
Ad-Aware	Gen:Variant.Symmi.40108	20140519
Agnitum	Trojan.Agent!XnCtU0IRt00	20140518
AntiVir	TR/Injector.ufwt.2	20140519
Antiy-AVL	Trojan[HEUR]Win32.AGeneric	20140519

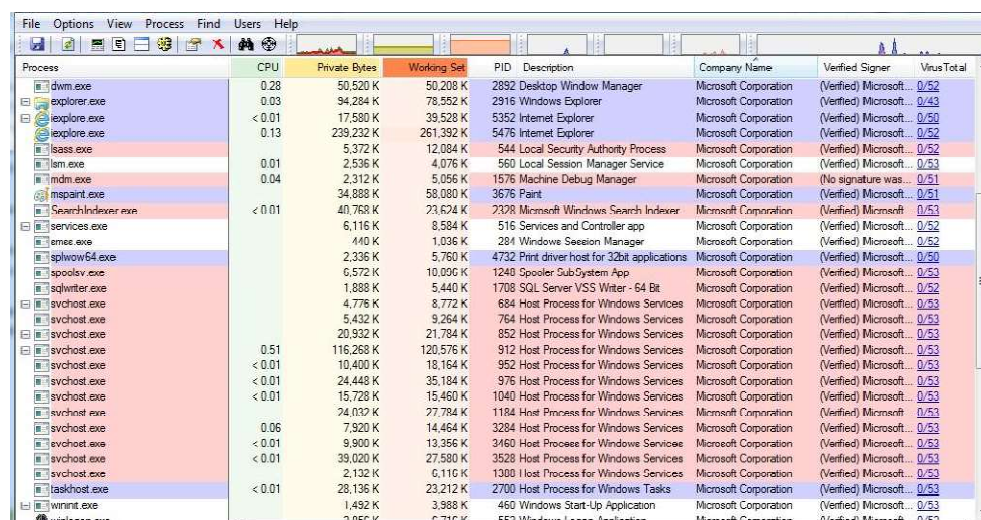
It acts as an information aggregator, gathering data about the different types of malware, and storing this information, for security professionals. VirusTotal gives you a date first seen (or date it first uploaded to its database), this indicates its new malware, and a detection ratio of 1/50 means an Antivirus has also detected it. By submitting a file to the website you're allowing VirusTotal to copy the file to its own database, and at the same time it produces its own MD5 Signature.

## Sysinternals Suite

Sysinternals (Suite) is a collection of Microsoft utilities which allow you to diagnose, monitor and troubleshoot computer problems or hunt down Malware which may be on your system. To find Malware on a System these tools are ideal, but a lot of experience is needed to find the abnormal from the normal

### Process Explorer

Processor Explorer is a monitoring tool which allows you to view running processes or applications. It's a task manager but gives a lot more information about the state of your system, such as which exe and DLLs processing are currently running and what other resources are they using.



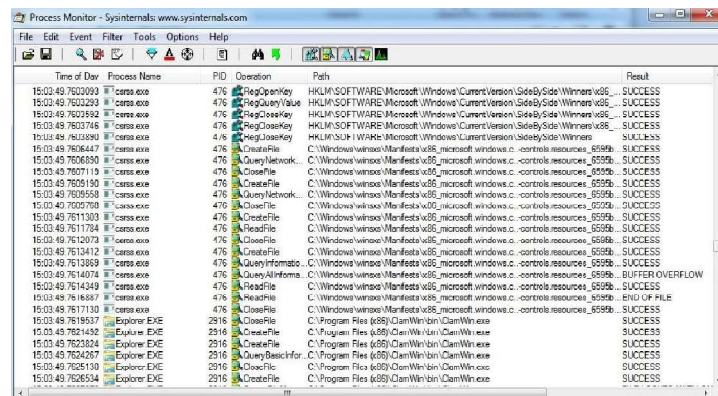
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer	VirusTotal
dwm.exe	0.28	50,520 K	50,208 K	2892	Desktop Window Manager	Microsoft Corporation	(Verified) Microsoft...	0/52
explorer.exe	0.03	94,284 K	78,552 K	2916	Windows Explorer	Microsoft Corporation	(Verified) Microsoft...	0/43
explorer.exe	< 0.01	17,580 K	39,528 K	5352	Internet Explorer	Microsoft Corporation	(Verified) Microsoft...	0/50
explorer.exe	0.13	239,232 K	261,392 K	5476	Internet Explorer	Microsoft Corporation	(Verified) Microsoft...	0/52
lsass.exe	0.01	5,372 K	12,084 K	544	Local Security Authority Process	Microsoft Corporation	(Verified) Microsoft...	0/52
lsmd.exe	0.04	2,536 K	4,076 K	560	Local Session Manager Service	Microsoft Corporation	(Verified) Microsoft...	0/53
mspaint.exe		2,312 K	5,056 K	1576	Machine Debug Manager	Microsoft Corporation	(No signature was...	0/51
SearchIndexer.exe	< 0.01	34,888 K	58,080 K	3676	Paint	Microsoft Corporation	(Verified) Microsoft...	0/51
services.exe		40,768 K	23,624 K	2328	Microsoft Windows Search Indexer	Microsoft Corporation	(Verified) Microsoft...	0/53
smss.exe		6,116 K	8,584 K	516	Services and Controller app	Microsoft Corporation	(Verified) Microsoft...	0/52
spoolsv.exe		440 K	1,036 K	284	Windows Session Manager	Microsoft Corporation	(Verified) Microsoft...	0/52
sqlwriter.exe		2,336 K	5,760 K	4732	Print driver host for 32bit applications	Microsoft Corporation	(Verified) Microsoft...	0/50
spoolsv.exe		6,572 K	10,096 K	1240	Spooler SubSystem App	Microsoft Corporation	(Verified) Microsoft...	0/53
sqlwriter.exe		1,888 K	5,440 K	1708	SQL Server VSS Writer - 64 Bit	Microsoft Corporation	(Verified) Microsoft...	0/52
svchost.exe		4,776 K	8,772 K	684	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft...	0/53
svchost.exe		5,432 K	9,264 K	764	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft...	0/53
svchost.exe		20,932 K	21,784 K	852	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft...	0/53
svchost.exe	0.51	116,268 K	120,576 K	912	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft...	0/53
svchost.exe	< 0.01	10,400 K	18,164 K	952	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft...	0/53
svchost.exe	< 0.01	24,448 K	35,184 K	976	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft...	0/53
svchost.exe	< 0.01	15,728 K	15,460 K	1040	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft...	0/53
svchost.exe		24,032 K	27,784 K	1184	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft...	0/53
svchost.exe	0.06	7,920 K	14,464 K	3284	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft...	0/53
svchost.exe	< 0.01	9,900 K	13,366 K	3460	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft...	0/53
svchost.exe	< 0.01	39,020 K	27,580 K	3528	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft...	0/53
svchost.exe		2,132 K	6,116 K	1300	Host Process for Windows Services	Microsoft Corporation	(Verified) Microsoft...	0/53
taskhost.exe	< 0.01	28,136 K	23,212 K	2700	Host Process for Windows Tasks	Microsoft Corporation	(Verified) Microsoft...	0/53
wininit.exe		1,492 K	3,988 K	460	Windows Start-Up Application	Microsoft Corporation	(Verified) Microsoft...	0/53
winlogon.exe		2,968 K	6,740 K	660	Windows Logon Application	Microsoft Corporation	(Verified) Microsoft...	0/53

The GUI when opened shows colour coded active processes, the pink processes are windows services, the blue Explorer services and white are start-up services.

It's a superb tool for malware hunting as it names the company which created the exe or DLL, provides a signature which can be verified and shows that it's a genuine product from that company, also allows you to run it against VirusTotal.com's database and 40 antivirus companies, to see if it is actually malware.

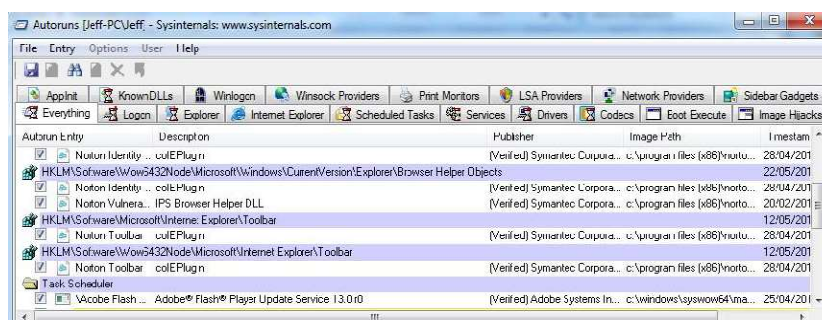
## Process Monitor

Processor Monitor displays different filters allowing you to display activity from the Registry, File System and the activity of the different process and threads. Only an advanced user could make sense of the extensive amount of information that is constantly streaming through its spreadsheet-like GUI. The user can choose the toolbar to filter information, from the Registry, File system, process and thread, the stack or networking activity.



## Autoruns

Autoruns shows the programs which are running at start-up or login. You can review the different start-up folder locations (start-up, RunOnce, Services).Autoruns allows you to look for malware in these locations, it will be highlighted.

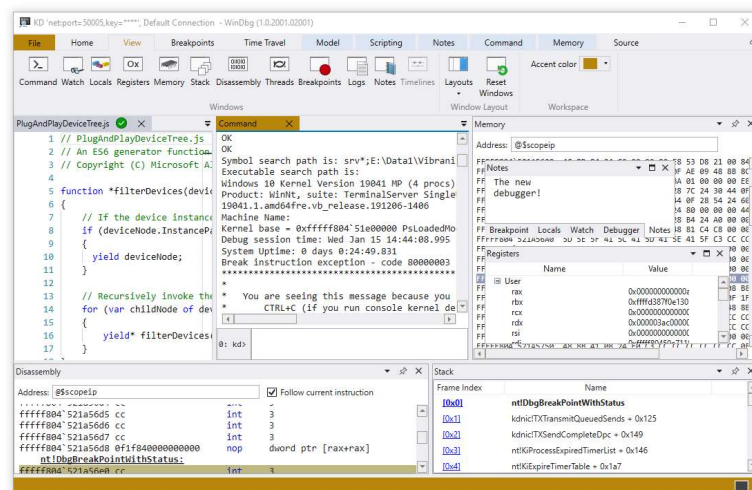


## Hex Editor

A hex editor is an application which allow the viewing and editing of binary files. The binary executables instructions and strings can be viewed giving the analyst an idea of what the program does and its intention.

## Windbg

Windbg is a free Window Debugger from Windows. Its original purpose was to help Window software developers debug code and fix software problems. It can debug user-mode and kernel-mode code, analyse crash dumps, and examine the CPU registers while the code executes.



To perform Windows kernel analysis, we need a specific setup of the Virtual Machine and Windbg in order to remotely debug the VM from the host. Rootkits leverage kernel level components to facilitate activities such as hiding processes, files, network connections and other common objects.