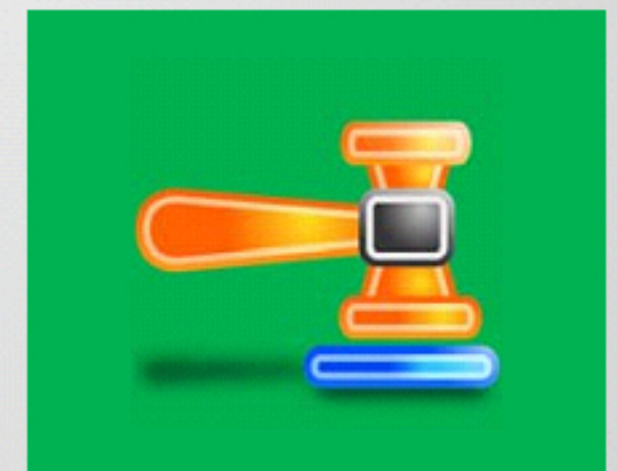
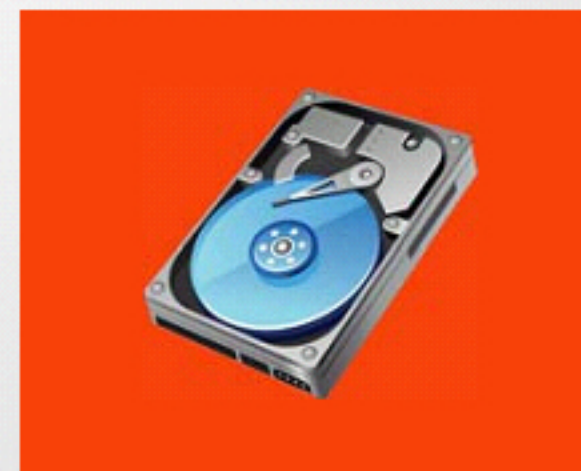


Malware Forensics

Module 11

Designed by **Cyber Crime Investigators**. Presented by Professionals.



Module Objectives



After successfully completing this module, you will be able to:

- 1 Define a malware and list the different ways a malware can get into a system
- 2 Discuss techniques attackers use to spread malware, and list the basic malware components
- 3 Apply malware forensics concepts, identify and extract malware from live and dead systems
- 4 Understand the prominence of setting up a controlled malware analysis lab
- 5 Prepare Testbed for malware analysis
- 6 Identify the general rules to perform malware analysis
- 7 Perform Static and Dynamic malware analysis and analyze malicious documents
- 8 Understand the challenges faced while performing malware analysis

Introduction to **Malware**

Malware is a malicious software that **damages or disables computer systems** and **gives limited or full control** of the systems to the malware creator for the purpose of theft or fraud.

Types of Malware

Backdoor

Rootkit

Botnet

Scareware

Downloader

Spam-sending malware

Launcher

Worm or virus

Credential-stealing program

Different Ways a Malware can Get into a System

1 Instant Messenger applications

2 Internet Relay Chat (IRC)

3 Removable devices

4 Links and Attachments in e-mails

5 Legitimate "shrink-wrapped" software packaged by a disgruntled employee

6 Browser and e-mail software bugs

7 NetBIOS (File Sharing)

8 Fake programs

9 Untrusted sites and freeware software

10 Downloading files, games, and screensavers from Internet sites

Common Techniques Attackers Use to Distribute Malware across Web

Blackhat Search Engine Optimization (SEO)

Ranking **malware-attacked** pages in search engine page result

Social Engineered Clickjacking

Tricking users into clicking **on innocent-looking** webpages

Malvertising

Embedding malware in **ad-networks** that display across hundreds of legitimate, high-traffic sites

Spear Phishing Sites

Mimicking legitimate institutions in an attempt to steal **login credentials**

Compromised Legitimate Websites

Hosting **embedded malware** sites that spreads to unsuspecting visitors

Drive-by Downloads

Viruses exploiting **flaws in browser** software to install malware just by visiting a web page

Source: Security Threat Report (<http://www.sophos.com>)

Components of Malware

Components of a malware software relies on the requirements of the **malware author** who designs it for a specific target to perform the intended tasks

Basic components of a malware:

Malware Component	Description
Crypter	Software that protects malware from undergoing reverse engineering or analysis, thus hardening the task of security mechanism its detection
Downloader	A type of Trojan that downloads other malware from the Internet on to the PC. Usually, attackers install downloader software when they first gain access to a system
Dropper	A type of Trojan that installs other malware files on to the system either from malware package or internet
Exploit	A malicious code that breaches the system security via software vulnerabilities to access information or install malware
Injector	A program that injects its code into other vulnerable running processes and changes the way of execution in order to hide or prevent its removal
Obfuscator	A program via various techniques that conceals its code and intended purpose, and thus, makes it hard for security mechanisms to detect or remove it
Packer	A program that allows to bundle all files together into a single executable file via compression in order to bypass security software detection
Payload	A piece of software that allows to control a computer system after it has been exploited
Malicious Code	A command that defines malware's basic functionalities such as stealing data and creating backdoor

Introduction to Malware Forensics

Often, attackers use malware such as **virus**, **worm**, **trojan**, **spyware**, and **ransomware**, etc., to commit a crime on the intended target system

Malware forensics deals with **identifying** and **capturing** malicious code and evidence of its effect on the **infected system**

Performing **malware analysis** enables one to know the type of malware, how it works, its behavior, and impact on the target system

You can use a set of tools and techniques to conduct **static analysis** and **dynamic (run-time) analysis** of the malicious code

Why Analyzed Malware?

To determine what happened exactly

To identify the exploited vulnerability

To determine the malicious intent of malware software

To identify the extent of damage caused from intrusion

To find out indicators of compromise

To catch the perpetrator accountable for installing the malware

To determine the complexity level of an intruder

To find signatures for host and network-based intrusion detection systems

Identifying and Extracting Malware

- If a user has **reported about suspicious activity** on his/her system, you have to examine the following areas of the compromised system to find the traces of malware installation

- Installed programs
- Suspicious executables
- Auto-starting locations
- Scheduled jobs
- Services
- Modules

- Logs
- User accounts and logon activities
- File system
- Registry entries
- Application traces
- Restore points, etc.

- You can use tools such as balbuzard, Cryptam Malware Document Detection Suite, etc. to extract patterns from malicious files for investigative purpose
- You can perform static and dynamic analysis together in order to identify the intent and capabilities of the malware software

Note: You can recognize malware by searching for the already known malware characteristics, rootkit detectors, anti-virus, etc.

Prominence of Setting up a Controlled Malware Analysis Lab



- Usually, malware analysis is carried out by infecting a system with the **malicious code** and then evaluating its behavior using a set of monitoring tools
- Thus, a **dedicated laboratory system** is required that can be infected keeping the production environment safe
- Best way to set up such lab system involves:
 - Using a physical system isolated from the production network to prevent the spread of the malware
 - Using **virtualization software** such as Virtualbox, VMware, Parallels, etc. (to set up single physical system with multiple VMS installed in it, each running different OSs)

Importance of virtual environment for malware analysis:

Protects real systems and network from being infected by the malware under analysis

Easy to analyze malware interaction with other systems

Allows capturing of screen during analysis

Ability to take snapshots of the laboratory system, which can be used to easily revert to a previous system state

Preparing Testbed for Malware Analysis

Allocate a **physical system** for the analysis lab

Install **Virtual machine** (VMware, Hyper-V, etc.) on the system

Install **guest OSs** in the Virtual machine(s)

Isolate the system from the network by ensuring that the **NIC card** is in “**host only**” mode

Simulate internet services using tools such as **iNetSim**

Disable the ‘**shared folders**’ and the ‘**guest isolation**’

Install **malware analysis** tools

Generate **hash value** of each OS and tool

Copy the **malware** over to the guest OS

Supporting Tools for Malware Analysis

Virtual Machines Tools

- Virtual Box (<https://www.virtualbox.org>)
- Parallels Desktop 11 (<http://www.parallels.com>)
- Boot Camp (<https://www.apple.com>)
- VMware vSphere Hypervisor (<http://www.vmware.com>)

Screen Capture and Recording Tools

- Snagit (<https://www.techsmith.com>)
- Jing (<https://www.techsmith.com>)
- Camtasia (<https://www.techsmith.com>)
- Ezvid (<http://www.ezvid.com>)

Network and Internet Simulation Tools

- NetSim (http://tetcos.com/netsim_gen.html)
- ns-3 (<https://www.nsnam.org>)
- Riverbed Modeler (<http://www.riverbed.com>)
- QualNet (<http://web.scalable-networks.com>)

OS Backup and Imaging Tools

- Genie Backup Manager Pro (<http://www.genie9.com>)
- Macrium Reflect Server (<http://www.macrium.com>)
- R-Drive Image (<http://www.drive-image.com>)
- O&O DiskImage 10 (<https://www.oo-software.com>)

General Rules for Malware Analysis

During malware analysis, pay attention to the key features instead of understanding each and every detail

Try different tools and approaches to analyze the malware, as single approach may not be helpful

Identify, understand, and defeat new malware analysis prevention techniques

Documentation **Before Analysis**

The following are some of the documentations that an investigator should prepare before performing an executable file analysis:

- 1** Full path and location of the file
- 2** MAC-timestamp
- 3** The system information where file was stored, e.g. OS and version, file system, user accounts, IP address
- 4** References to that file within the file system or registry
- 5** Who found the file and when
- 6** Details of forensics investigation tools

Types of Malware Analysis

■ Static Malware Analysis:

- Also known as **code analysis**, involves going through the executable binary code without actually **executing** it to have a better understanding about the malware and its purpose
- **Disassemblers** such as IDA Pro, can be used to disassemble the **binary file**

■ Dynamic Malware Analysis:

- Also known as **behavioral analysis**, involves executing the malware code to know how it interacts with the host system and its impact on it
- This type of analysis requires **virtual machines** and **sandboxes** to deter the spreading of malware
- **Debuggers** such as GDB, OllyDbg, WinDbg, etc., are used to debug malware at the time of execution to study its behavior

- Both techniques are intended to understand how the **malware works**, but differ in the tools used, and time and skills required for performing **analysis**
- It is recommended to perform both static and dynamic analysis to understand the functionality of malware to a large extent

Malware Analysis: **Static**

- In **static analysis**, we are not running the malware code so there is no need of creating a safe environment
- Analyzing the **binary code** provides information such as data structures, function calls, call graphs, etc.
- Load the binary code on to the **test system** (preferably the OS on which the malware is not designed to run) to analyze its static properties - strings embedded into the file, header details, hashes, embedded resources, packer signatures, metadata, etc.

Some of the static malware analysis techniques:

- File **fingerprinting**
- Local and Online **malware scanning**
- Performing **strings search**
- Identifying **packing/obfuscation** methods
- Finding the **portable executables (PE)** information
- Identifying **file dependencies**
- Malware **disassembly**

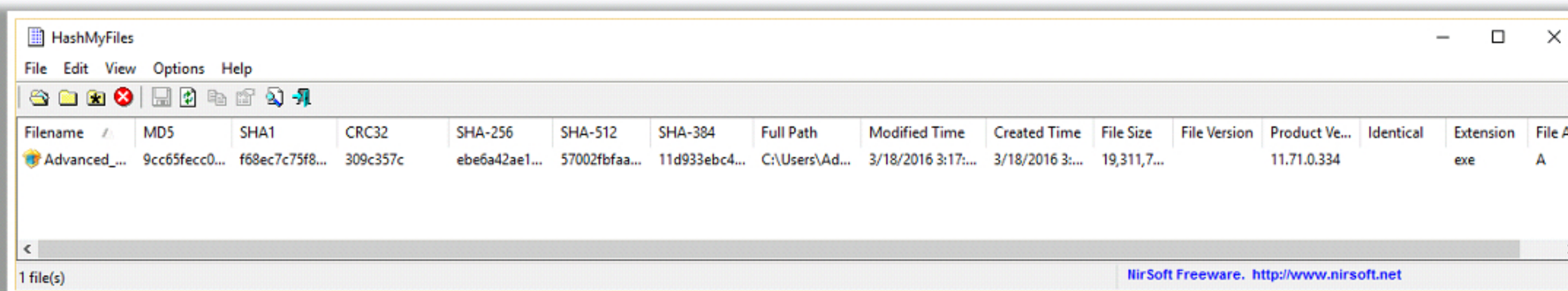
Static Malware Analysis: File Fingerprinting

It is recommended to compute hash value for a given **binary code** before carrying out the investigation

Common **hash calculators** include HashTab, HashMyFiles, HashCalc, md5sum, md5deep, etc.

You can use the computed hash value to periodically verify if any change is made to the **binary code** during analysis

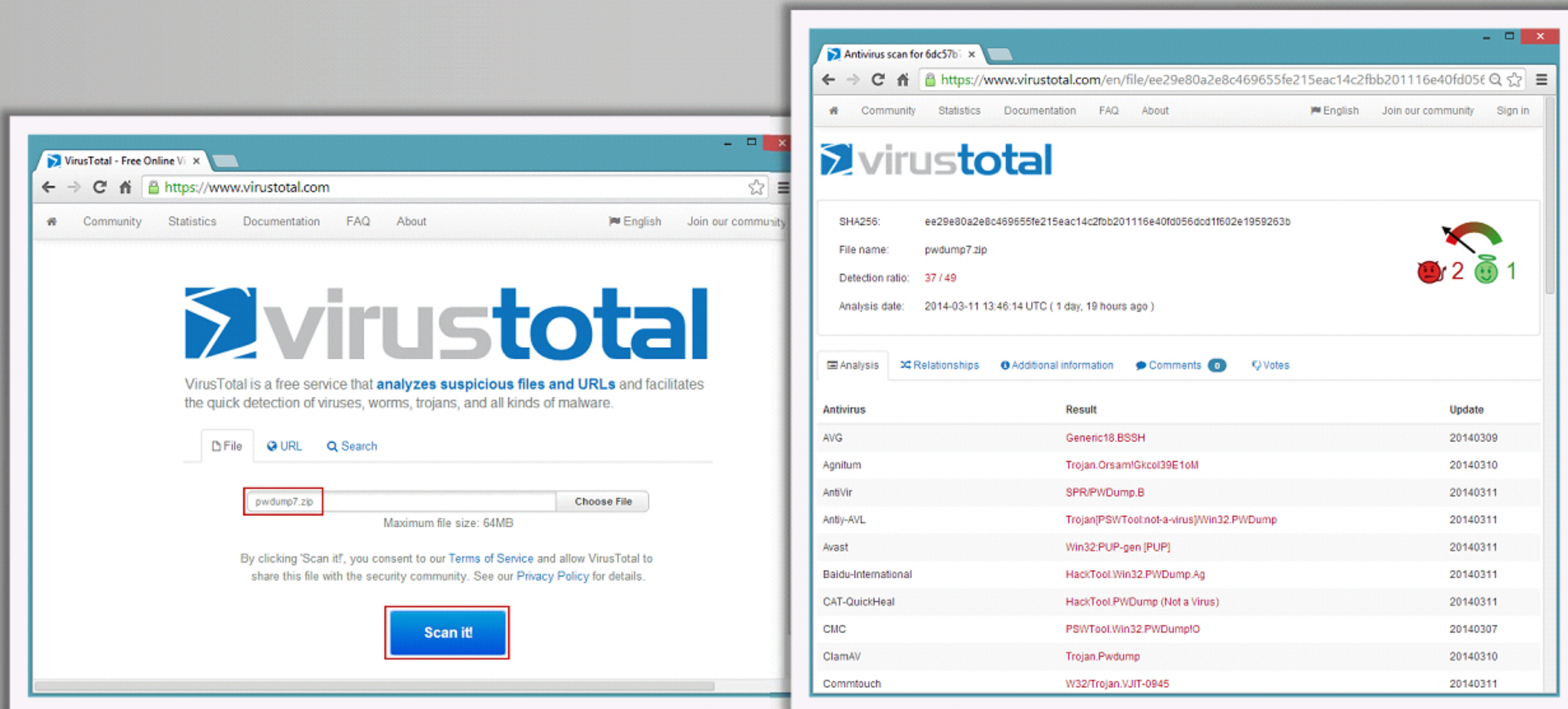
You can also compare the computed hash value with that of the identified malware stored in **databases**. Ex: VirusTotal - an online database



<http://www.nirsoft.net>

Online Malware Testing: VirusTotal

- VirusTotal is a free service that **analyzes suspicious files and URLs**, and facilitates the detection of viruses, worms, Trojans, etc.



The left screenshot shows the VirusTotal homepage with the file 'pwdump7.zip' entered in the file input field. The right screenshot shows the analysis results for the same file, displaying a detection ratio of 37/49 and a list of antivirus engines and their results.

Analysis Results:

Antivirus	Result	Update
AVG	Generic18.BSSH	20140309
Agnitum	Trojan.OrsamIGkcol39E1oM	20140310
AntiVir	SPR/PWDump.B	20140311
Antiy-AVL	Trojan[PSWTool.not-a-virus]Win32.PWDump	20140311
Avast	Win32:PUP-gen [PUP]	20140311
Baidu-International	HackTool.Win32.PWDump.Ag	20140311
CAT-QuickHeal	HackTool.PWDump (Not a Virus)	20140311
CMC	PSWTool.Win32.PWDump!O	20140307
ClamAV	Trojan.Pwdump	20140310
CommTouch	W32/Trojan.VJIT-0945	20140311

<http://www.virustotal.com>

Online Malware Analysis Services



Anubis: Analyzing Unknown Binaries

<http://anubis.iseclab.org>



Payload Security

<https://www.hybrid-analysis.com>



Malware Protection Center

<https://www.microsoft.com>



Malwr

<https://malwr.com>



Dr. Web Online Scanners

<http://vms.drweb.com>



Metascan Online

<http://www.metascan-online.com>



Bitdefender QuickScan

<http://quickscan.bitdefender.com>



IObit Cloud

<http://cloud.iobit.com>



Valkyrie

<https://valkyrie.comodo.com>



ThreatAnalyzer

<http://www.threattracksecurity.com>

Static Malware Analysis: Local and Online Malware Scanning

- Scan the **binary code** using renowned and up-to-date **anti-virus software**
- If the code under analysis is a component of a **well-known malware**, it may have been already discovered and documented by many anti-virus vendors
- Go through their documentation to recognize the code **capabilities, signatures**, etc.
- You can also upload the code to **websites** such as VirusTotal (<https://www.virustotal.com>) and Jotti (<https://virusscan.jotti.org>) to get it scanned by a wide-variety of different scan engines

The screenshot shows the Jotti malware scan interface. At the top is the Jotti logo. Below it is a navigation bar with links: Jotti's malware scan, Scan file, Search hash, Language, FAQ, Privacy, and Contact. The main content area shows the scan results for a file named '11.exe'. A message states: 'This file was scanned a while ago. Below are the results of that scan.' There is a button 'Scan this file again'. The file details are as follows:

Field	Value	Status	Scan taken on:
Name:	Ac 11.exe	Scan finished. 1/21 scanners reported malware.	13 March 2016 09:10:07 CET
Size:	18.42MB (19,311,728 bytes)		
Type:	PE32 executable (GUI) Intel 80386, for MS Windows		
First seen:	13 March 2016 09:10:04 CET		
MD5:	9cc65fecc01b1028ceab2a77f39985f3		
SHA1:	f68ec7c75f8c3572526eba676f236d800b463039		

Below the file details is a table showing the results of 21 different antivirus scanners:

Scanner	Date	Result
Ad-Aware	13 Mar 2016	Found nothing
Avast	12 Mar 2016	Found nothing
Bitdefender	13 Mar 2016	Found nothing
eScan	13 Mar 2016	Found nothing
F-PROT	13 Mar 2016	Found nothing
IKARUS	13 Mar 2016	Found nothing
SOPHOS	13 Mar 2016	Found nothing
agnitum	11 Mar 2016	Found nothing
AVG	13 Mar 2016	Found nothing
ClamAV	11 Mar 2016	PUA.Spyware.XPCSpyPro
eSet	12 Mar 2016	Found nothing
F-Secure	13 Mar 2016	Found nothing
KASPERSKY	13 Mar 2016	Found nothing
TREND MICRO	12 Mar 2016	Found nothing
Arcabit	13 Mar 2016	Found nothing
AVIRA	12 Mar 2016	Found nothing
Dr.WEB	13 Mar 2016	Found nothing
FORTINET	12 Mar 2016	Found nothing
GDATA	13 Mar 2016	Found nothing
Quick Heal	12 Mar 2016	Found nothing
VBA32	12 Mar 2016	Found nothing

At the bottom of the page, there is a copyright notice: © 2004-2016 Jotti, and a URL: <https://virusscan.jotti.org>.

Static Malware Analysis: Performing Strings Search

1

Strings communicate information from the program to its user

2

Analyze **embedded strings** of the readable text within the program's executable file.
Ex: Status update strings and error strings

3

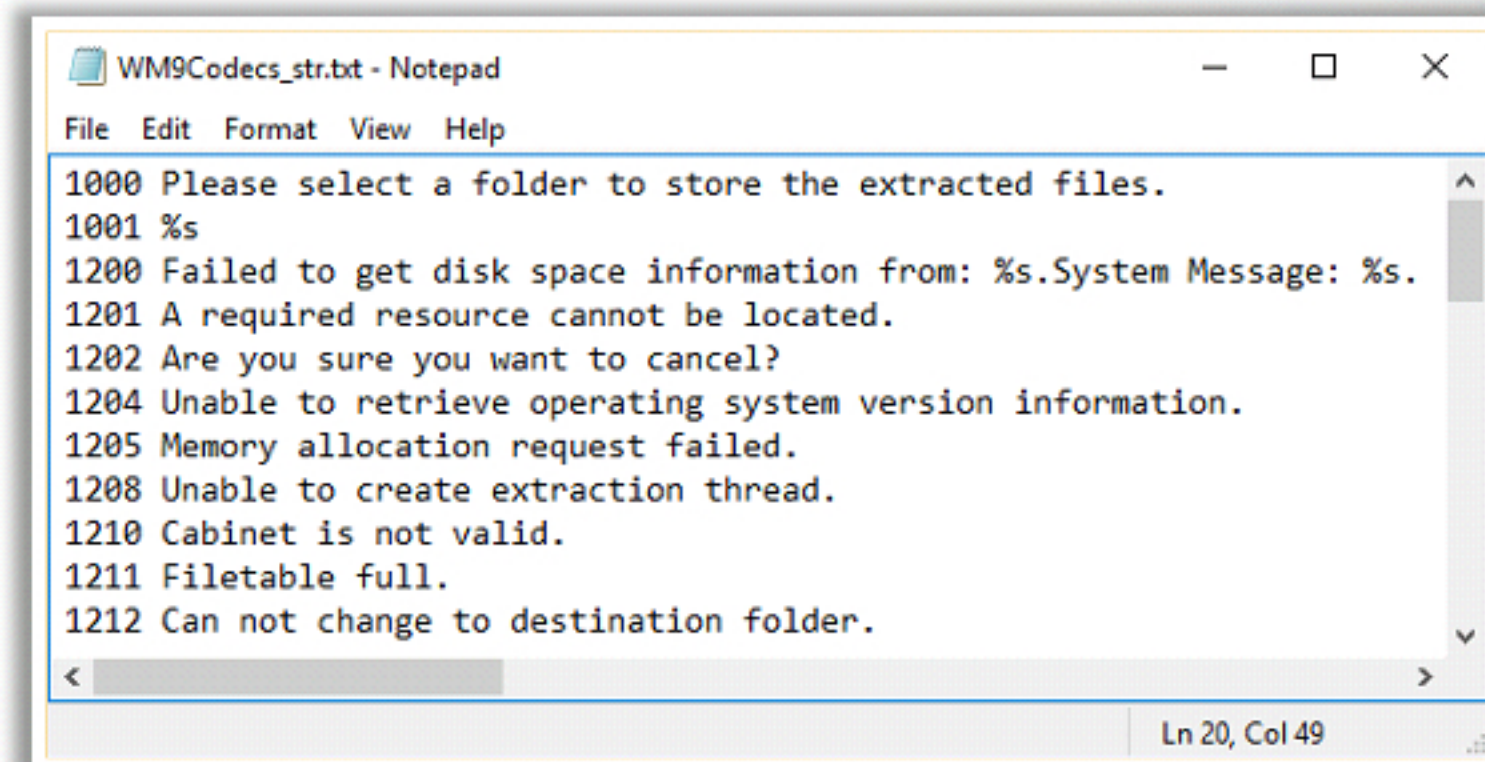
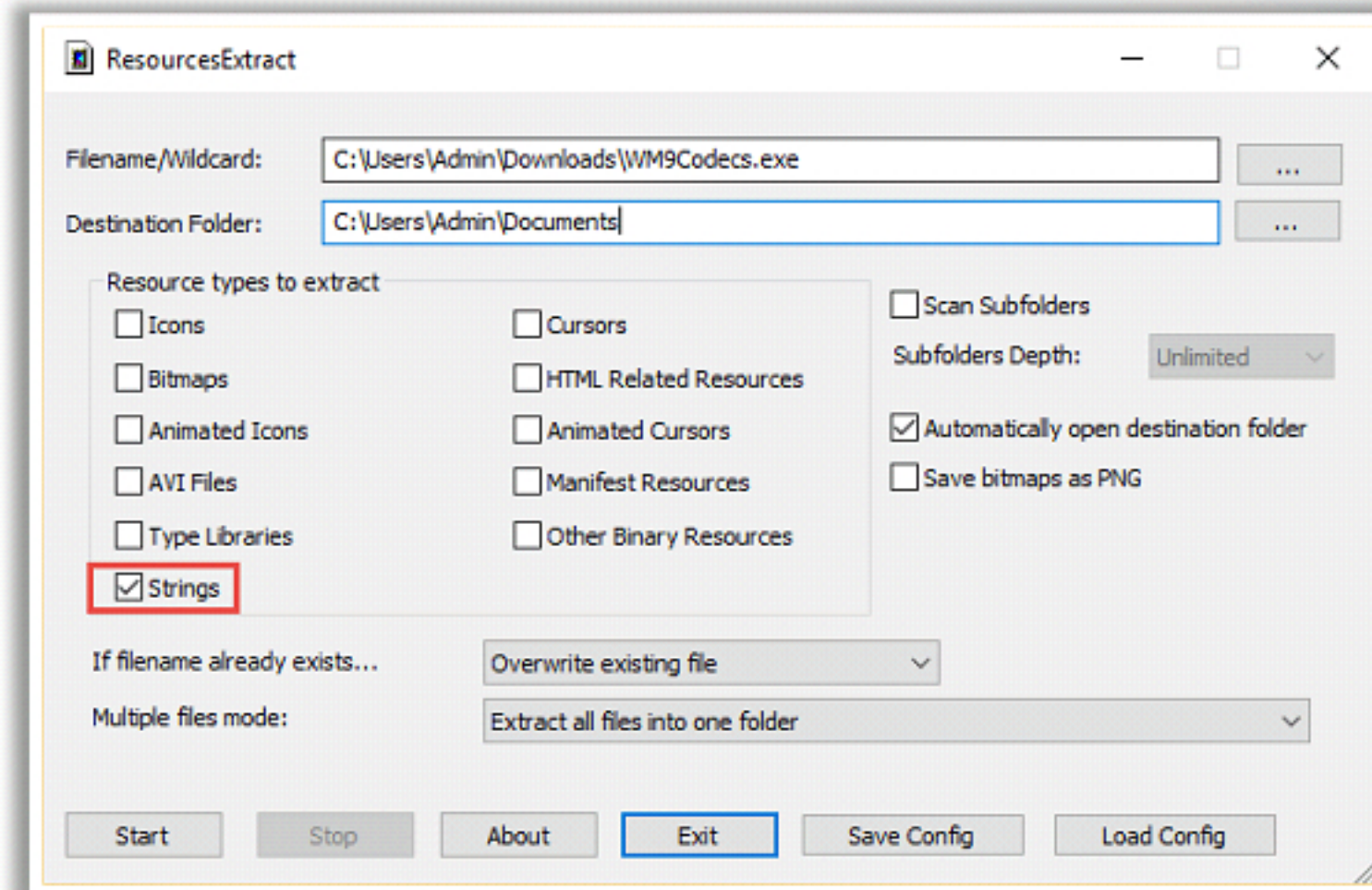
Use tools such as Strings, ResourcesExtract, Bintext, Hex Workshop, etc. to extract embedded strings from **executable files**

4

Ensure that the tool extract strings are represented in both **ASCII** and **Unicode** formats

5

On extracting, one can see the input of strings of interest in **search engine** for more information



Note: Strings may be often misleading or cause you to activate a sort of reverse-honeypot

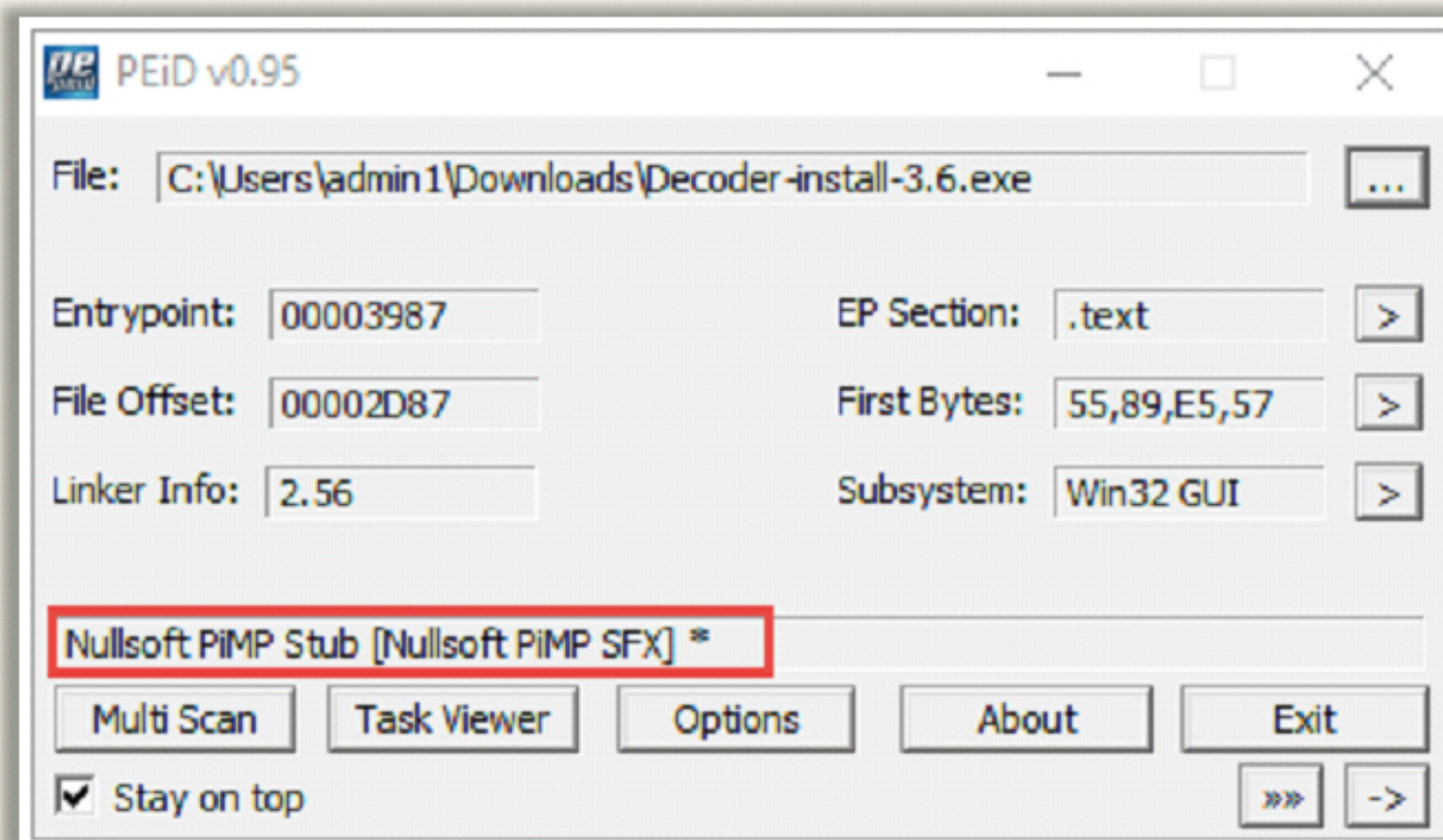
<https://www.microsoft.com>

Static Malware Analysis: Identifying Packing/Obfuscation Methods

Attackers often use packers to compress, encrypt, or modify a **malware executable file**

It toughens the task of the **reverse engineers** in finding out the actual program logic and other metadata via static analysis

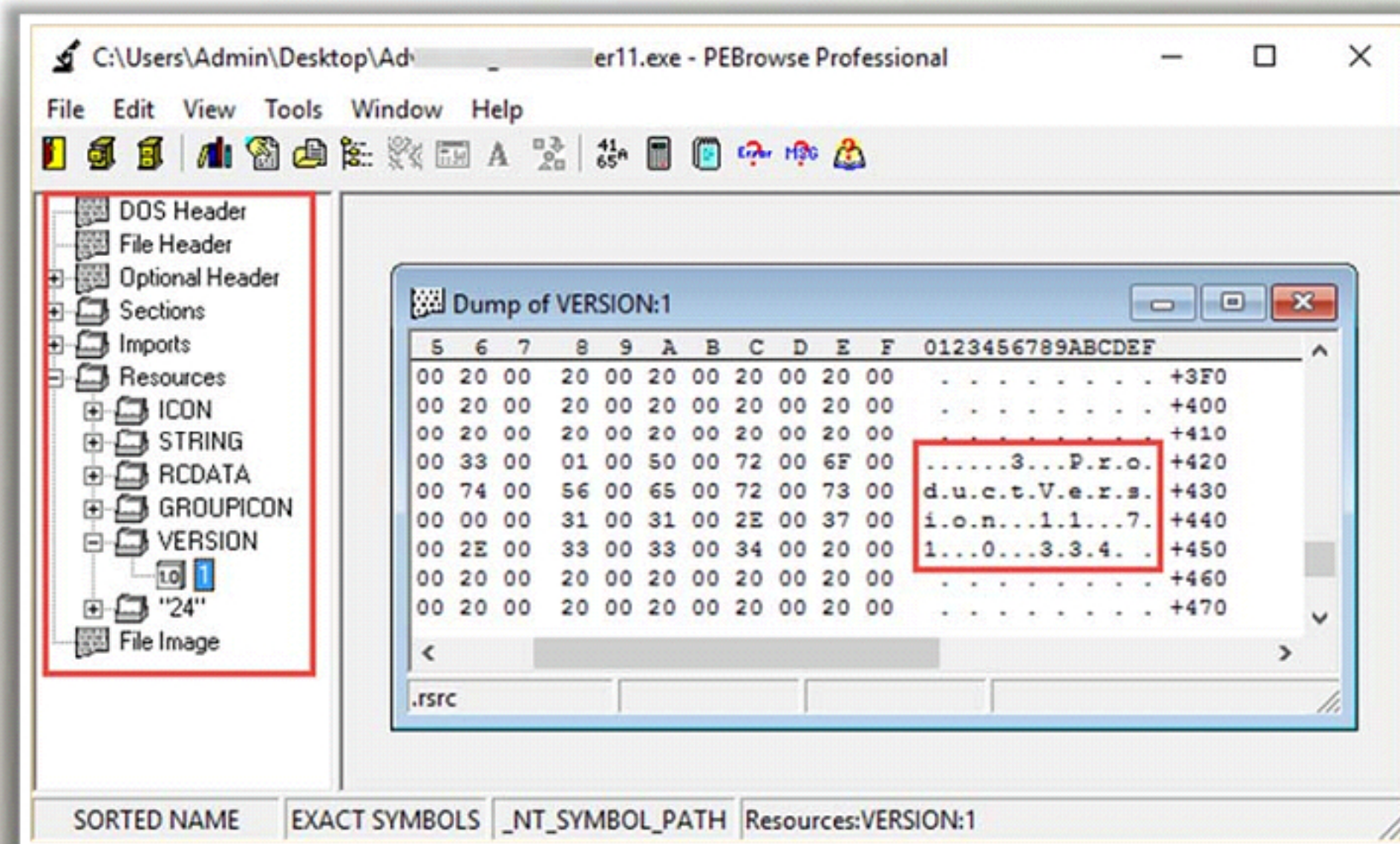
Use tools such as **PEiD**, which detects most common packers, cryptors and compilers for PE executable files



<http://www.softpedia.com>

Static Malware Analysis: Finding the Portable Executables (PE) Information

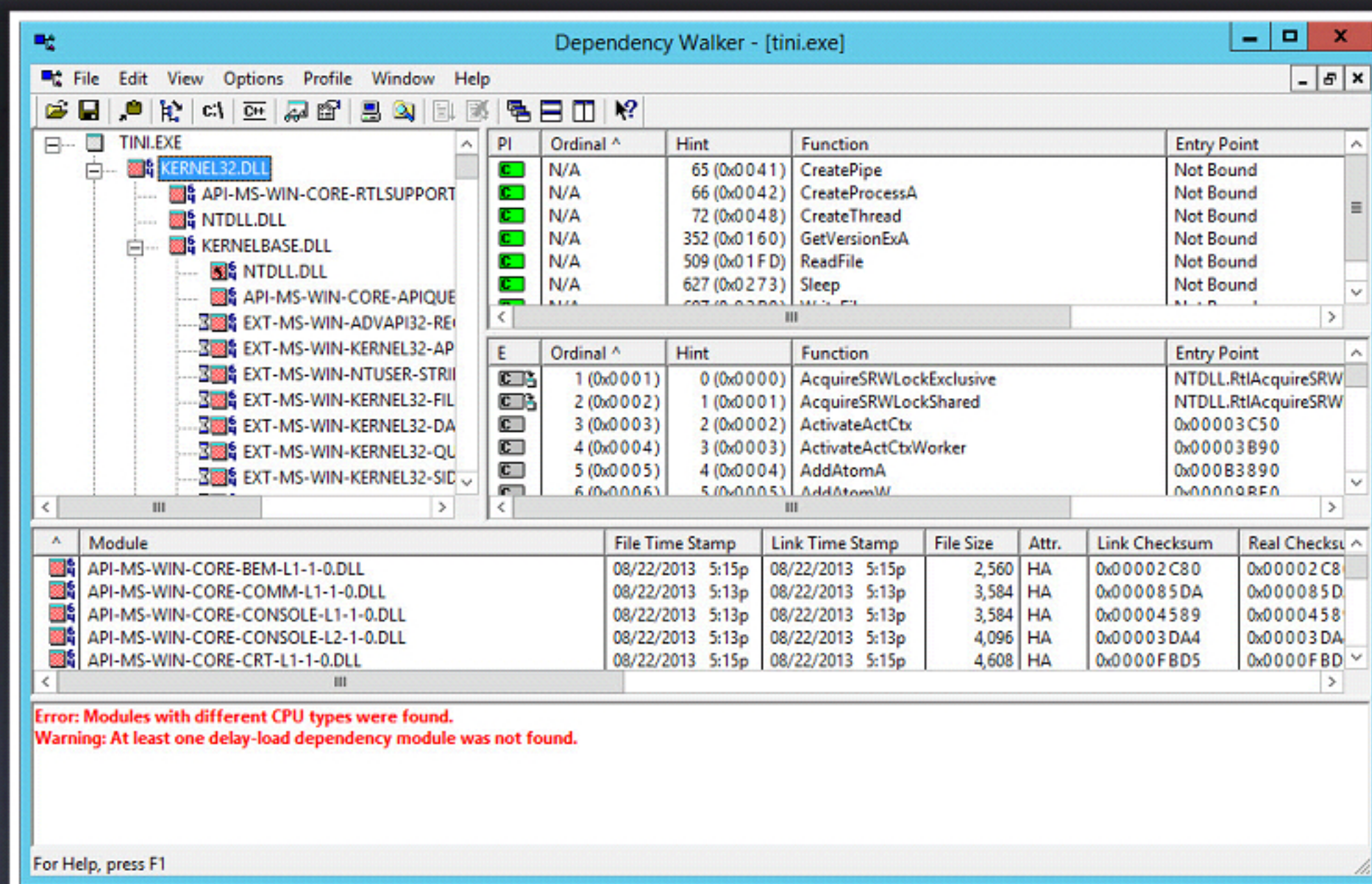
- PE format is the **executable file** format used on Windows operating systems
- Information available for examining the **metadata** of a PE file:
 - Time and date of compilation
 - Functions imported and exported by the program
 - Linked libraries
 - Icons, menus, version info, strings, etc. embedded in resources
- You can use tools such as PView, PE Explorer, Portable Executable Scanner (PEscan), PEBrowse Professional, Resource Hacker, Dependency Walker, etc. to extract the above mentioned information



<http://www.smidgeonsoft.prohosting.com>

Static Malware Analysis: Identifying File Dependencies

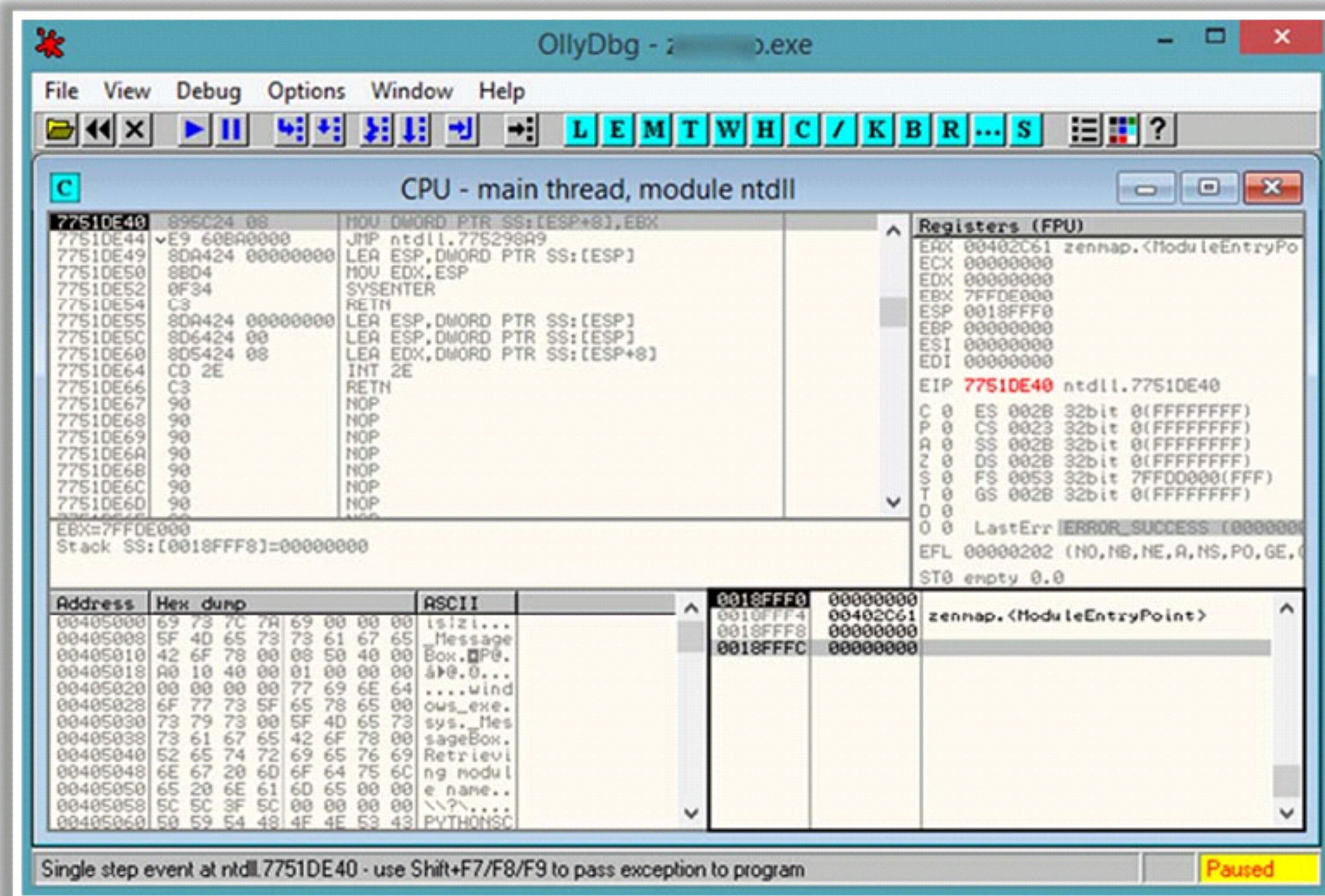
- Programs need to work with **internal system files** to function properly
- Programs store the **import** and **export functions** in kernel32.dll file
- Check the **dynamically linked list** in the malware executable file
- Finding out all the **library functions** may allow you to guess about what the malware program can do
- You can use tools such as **Dependency Walker**, which lists all dependent modules within the executable file



<http://www.dependencywalker.com>

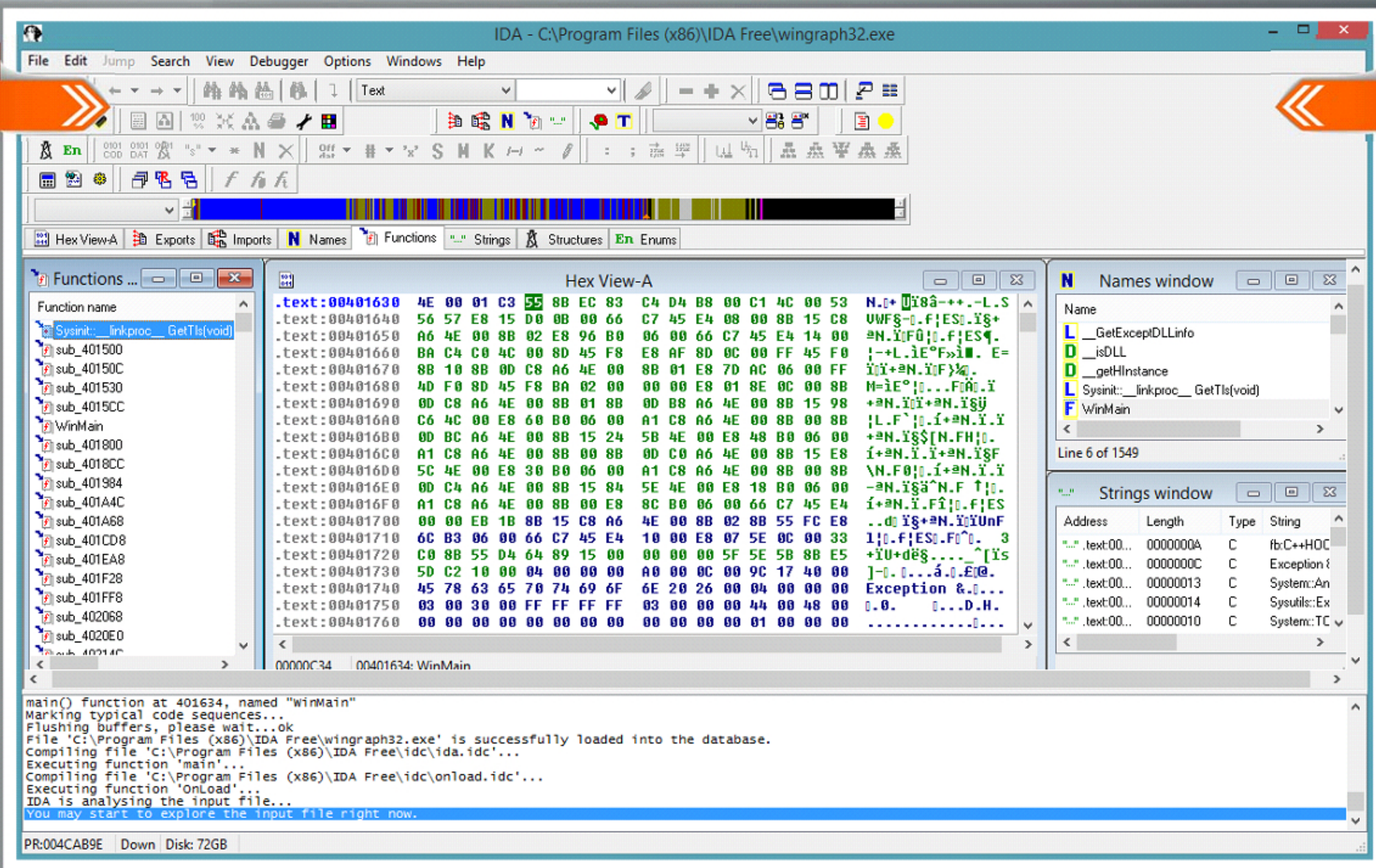
Static Malware Analysis: Malware Disassembly

- Disassemble the **binary code** and analyze the assembly code instructions
- You can use tools such as **IDA Pro** that can reverse machine code to **assembly language**
- Based on the reconstructed assembly code, you can inspect the **program logic** and recognize its threat potential. This process is carried out by using debugging tools such as **OllyDbg**, **WinDbg**, etc.



<http://www.ollydbg.de>

Malware Analysis Tool: IDA Pro



Malware Analysis: **Dynamic**

System Baseline:

- Refers to taking **snapshot** of the system at the time the malware analysis begins
- Main purpose of system baselining is to identify significant changes from the **baseline state**
- System baseline includes details of file **system**, **registry**, **open ports**, **network activity**, etc.

Host Integrity Monitor:

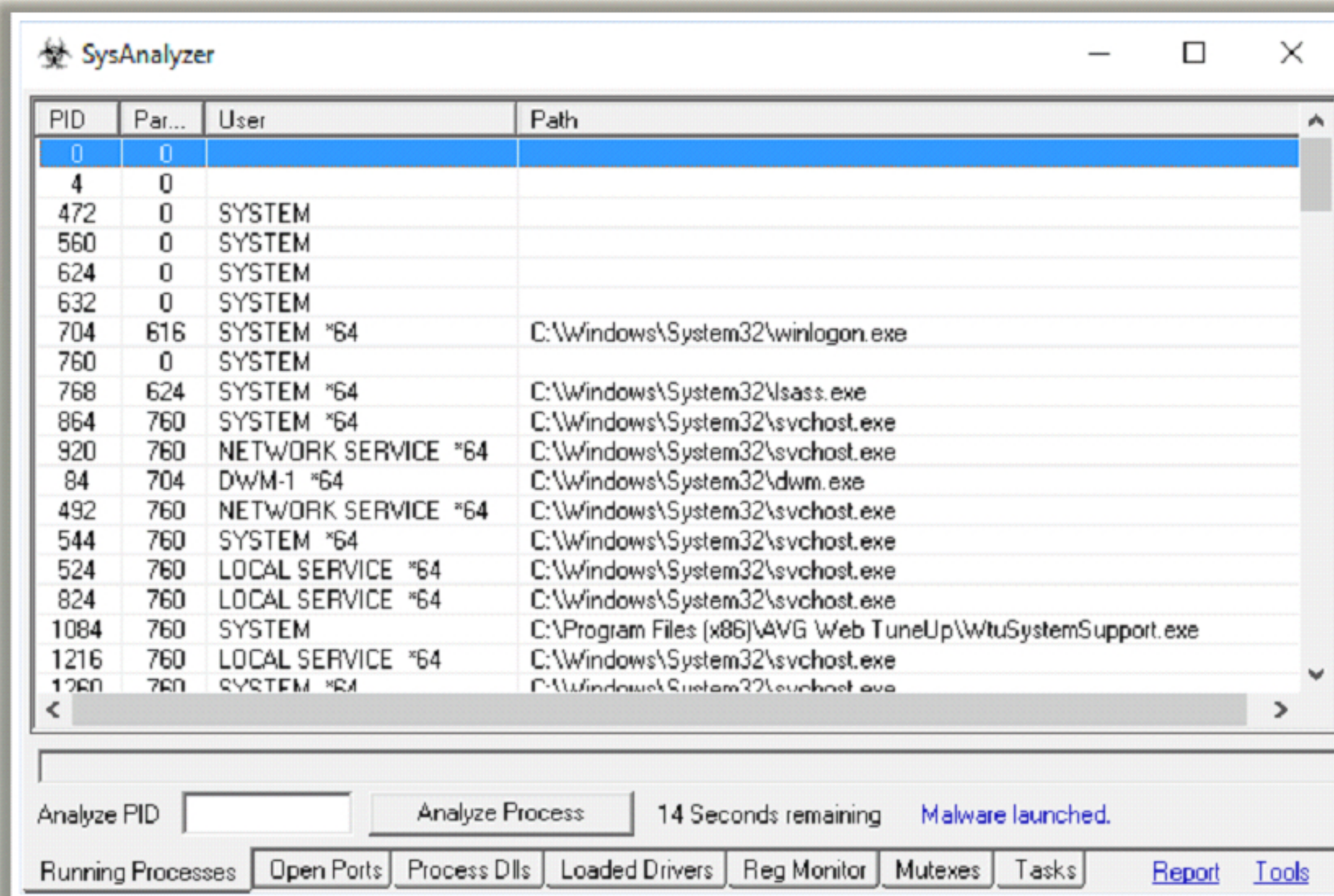
- Host integrity monitoring involves taking a snapshot of the **system state** using the same tools before and after the analysis to detect **changes** made to the entities residing on the system.
- Host integrity monitoring includes:

- 🕒 Installation Monitor
- 🕒 Process Monitor
- 🕒 Files and Folder Monitor
- 🕒 Registry Analysis/Monitoring
- 🕒 Network Traffic Monitoring/Analysis
- 🕒 Port Monitor

- 🕒 DNS Monitoring/Resolution
- 🕒 API Calls Monitor
- 🕒 Device Drivers Monitor
- 🕒 Startup Programs Monitor
- 🕒 Windows Services Monitor

Dynamic Malware Analysis: Installation Monitor

- You can use tools such as Mirekrosoft Install Monitor, Advanced Uninstaller PRO, Epsilon Squared's InstallWatch, Revo Uninstaller Pro, Comodo Programs Manager, **SysAnalyzer**, etc. to detect changes made to a system on execution of an **unknown binary specimen**



<http://www.sysanalyser.com>

CHFI
Computer Hacking Forensic
INVESTIGATOR

- Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

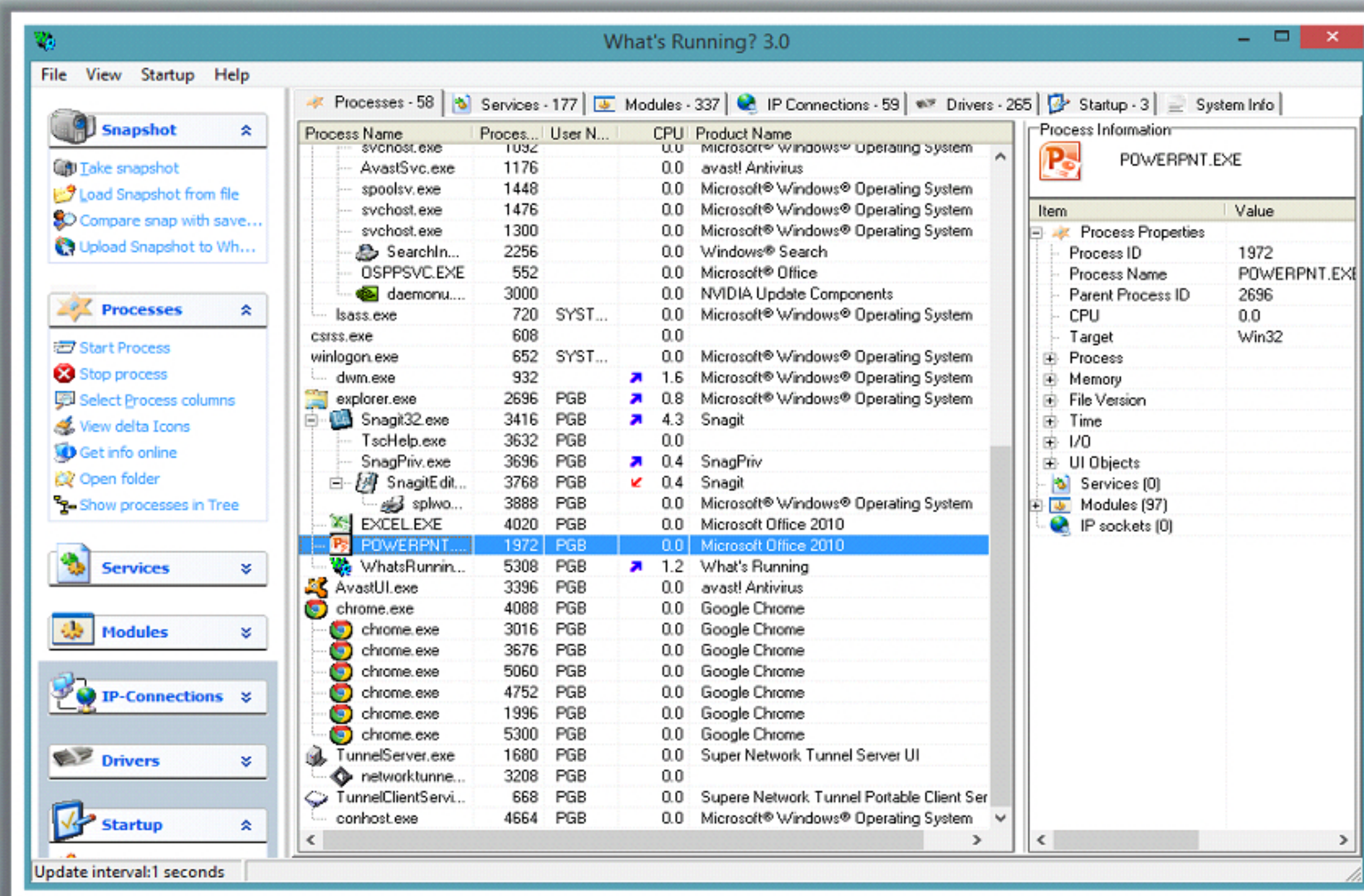
Process Monitoring Tool: What's Running

Features

- Inspect the **processes** and get performance along with **resource usage data** such as memory usage, processor usage, and handles
- Gather information about **dlls** loaded, **services** running within the process, and **IP-connections** associated with processes



What's Running is a monitoring tool that gives an **inside look** into your Windows operating systems



<http://www.whatsrunning.net>

Process Monitoring Tools



Process Explorer

<http://technet.microsoft.com>



Security Task Manager

<http://www.neuber.com>



System Explorer

<http://systemexplorer.net>



Proc Net Monitor

<http://securityxploded.com>



HijackThis

<http://sourceforge.net>



MONIT

<http://mmonit.com>



Autoruns for Windows

<http://technet.microsoft.com>



ESET SysInspector

<http://www.eset.com>



KillProcess

<http://orangelampsoftware.com>



OpManager

<http://www.manageengine.com>

Dynamic Malware Analysis: **File and Folder Monitor**

You can use files and folder integrity monitoring tools to examine real-time file system and folder activity on an infected system

SIGVERIF

- It **checks integrity of critical files** that have been digitally signed by Microsoft
- To launch SIGVERIF, go to **Start** → **Run**, type **sigverif** and press **Enter**

FCIV

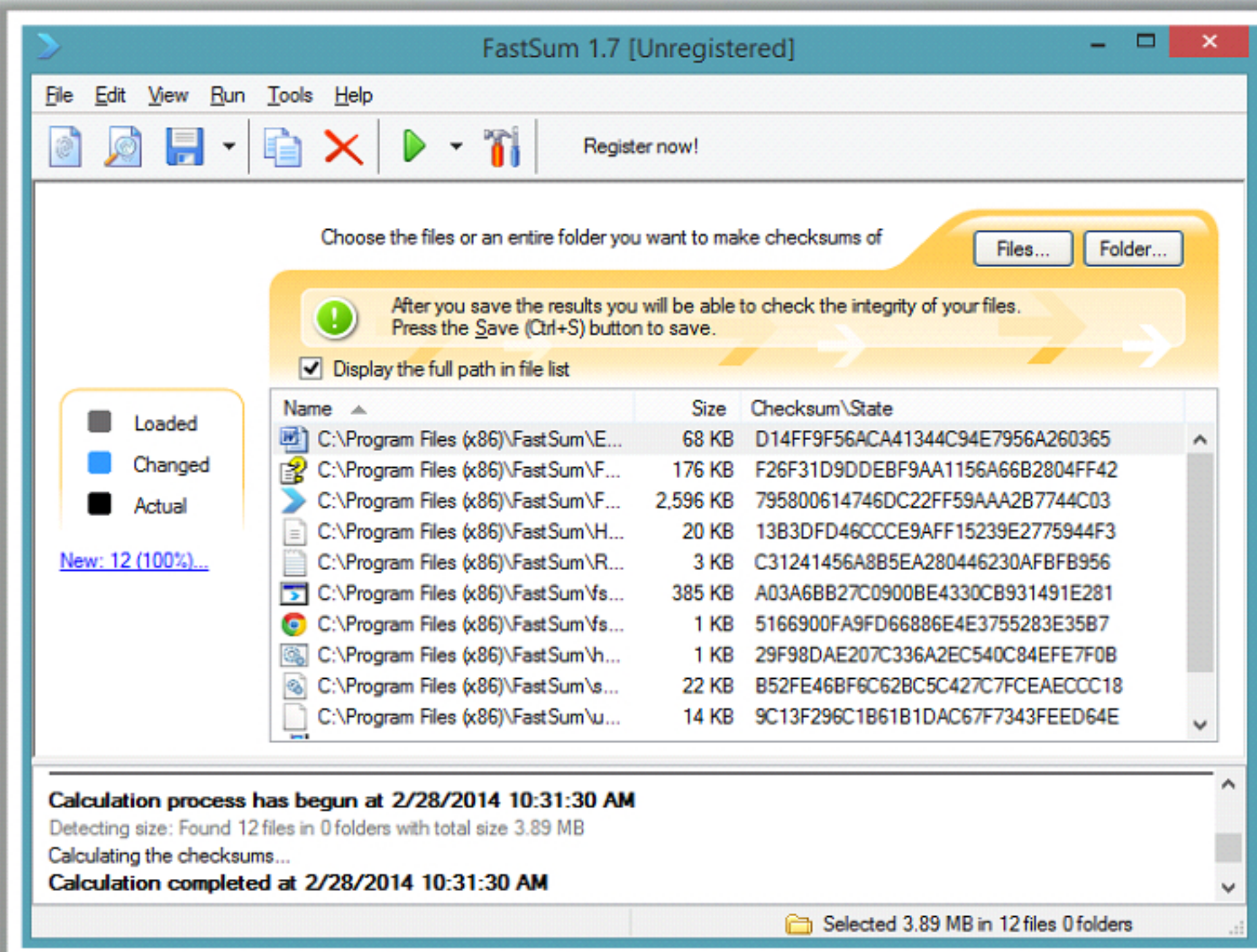
- It is a command line utility that computes **MD5** or **SHA1 cryptographic hashes** for files
- You can download FCIV at <http://download.microsoft.com>

TRIPWIRE

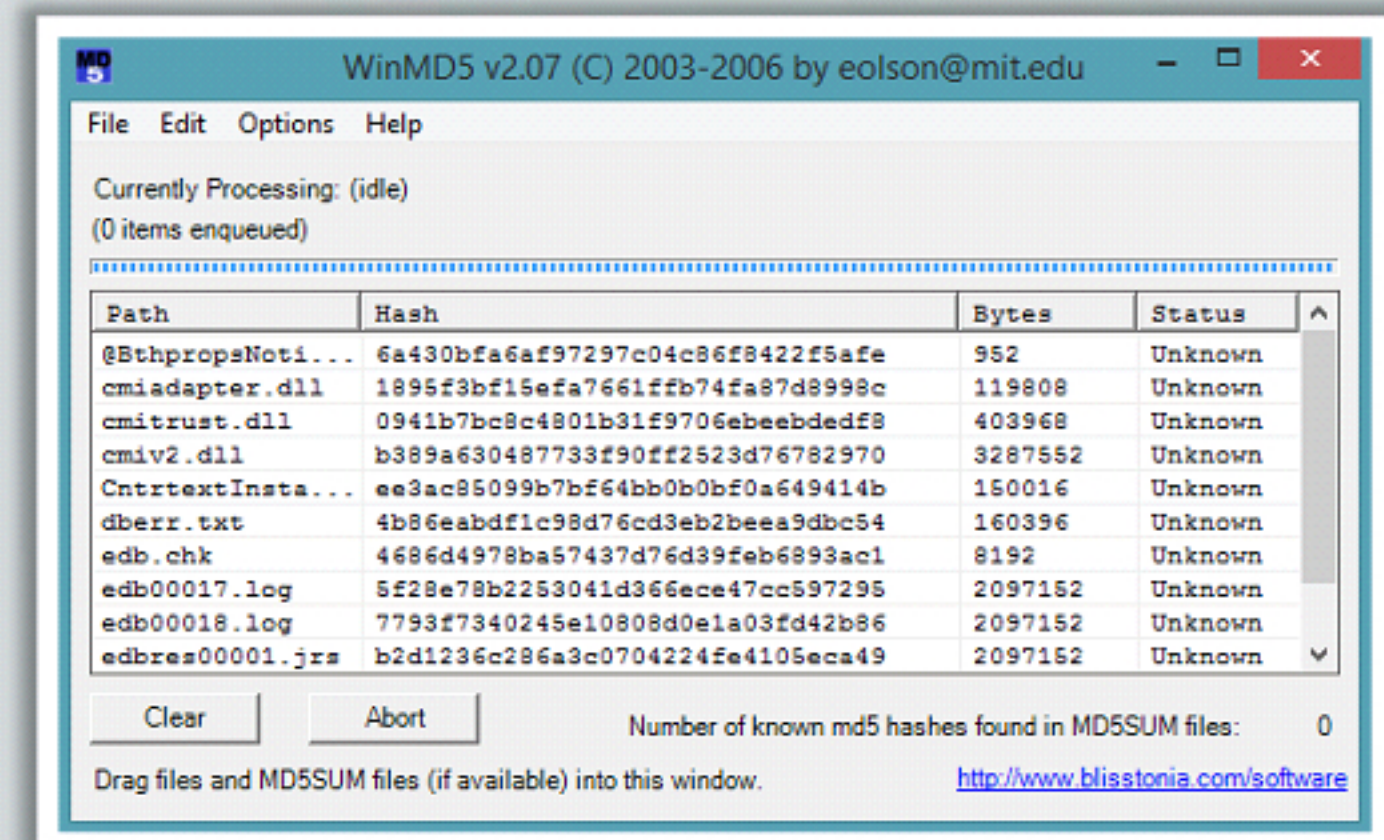
- It is an enterprise class system integrity verifier that **scans** and **reports critical system files for changes**



File and Folder Integrity Checkers: FastSum and WinMD5



<http://www.fastsum.com>



<http://www.winmd5.com>

- FastSum is used for **checking integrity** of the files
- It computes checksums according to the **MD5 checksum** algorithm



File and Folder Integrity Checkers



Directory Monitor

<https://directorymonitor.com>



PA File Sight

<http://www.poweradmin.com>



Fsum Frontend

<http://fsumfe.sourceforge.net>



CSP File Integrity Checker

<http://www.tandemsecurity.com>



Verisys

<http://www.ionx.co.uk>



ExactFile

<http://www.exactfile.com>



AFICK (Another File Integrity Checker)

<http://afick.sourceforge.net>



OSSEC

<http://www.ossec.net>



FileVerifier++

<http://www.programmingunlimited.net>



Change Tracker Enterprise

<https://www.newnettechnologies.com>

Dynamic Malware Analysis: Registry Monitor

You can use registry entry monitoring tools to examine the changes made to the system's registry by suspect program



Find registry errors, unneeded registry junk, and helps in detecting registry entries created by **malware**

Key: HKCU\Software\Initex\ProxyChecker\Settings\
Entry's name: Path
Value: c:\program files (x86)\proxifier\proxychecker.exe
Entry last modified: 27.02.2014, 04:30
Error severity: 99
Error description: File or directory "c:\Program Files\proxifier\proxychecker" does not exist
File reference: c:\Program Files\proxifier\proxychecker
Reason for detection: Invalid file reference
Tags:

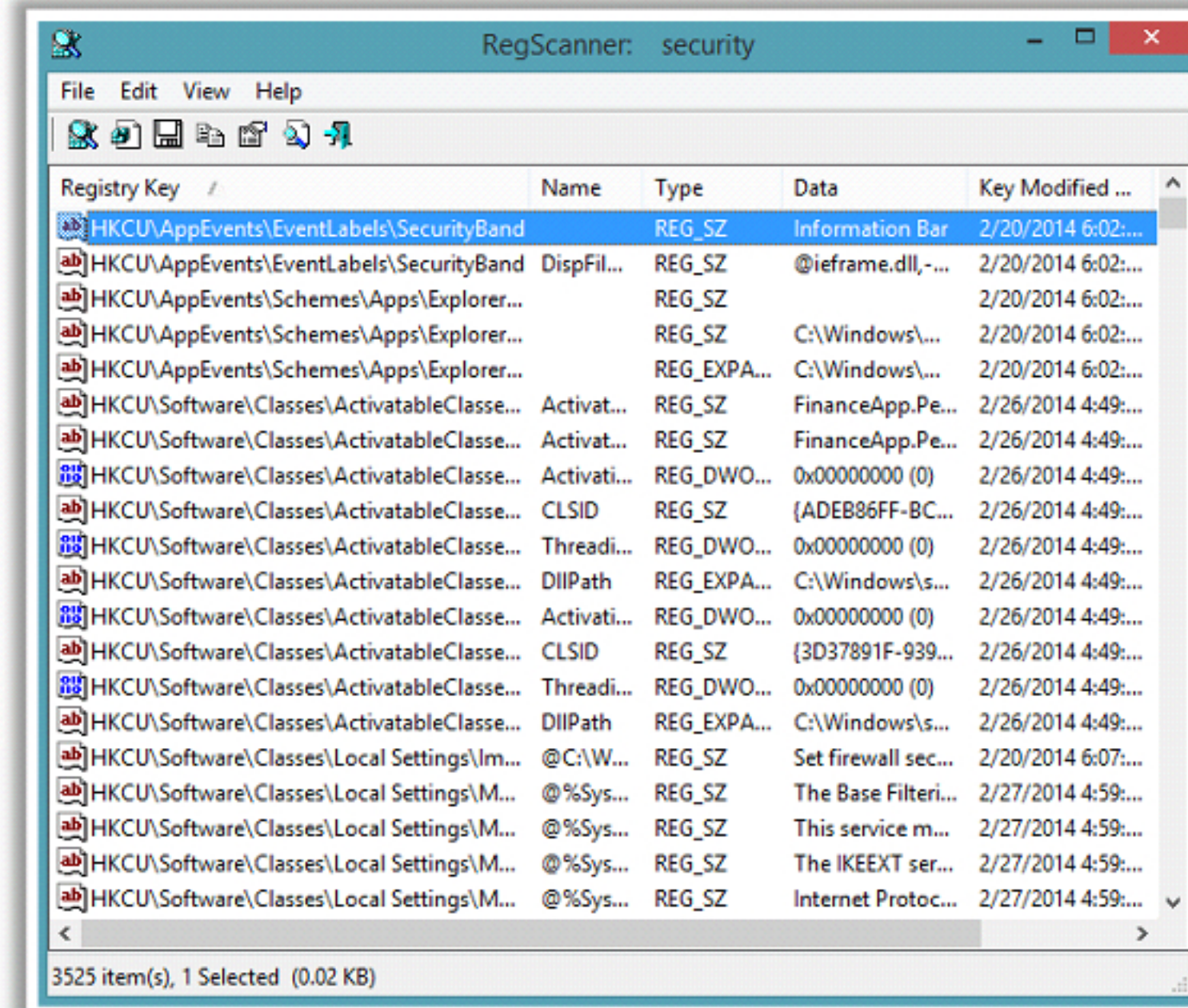
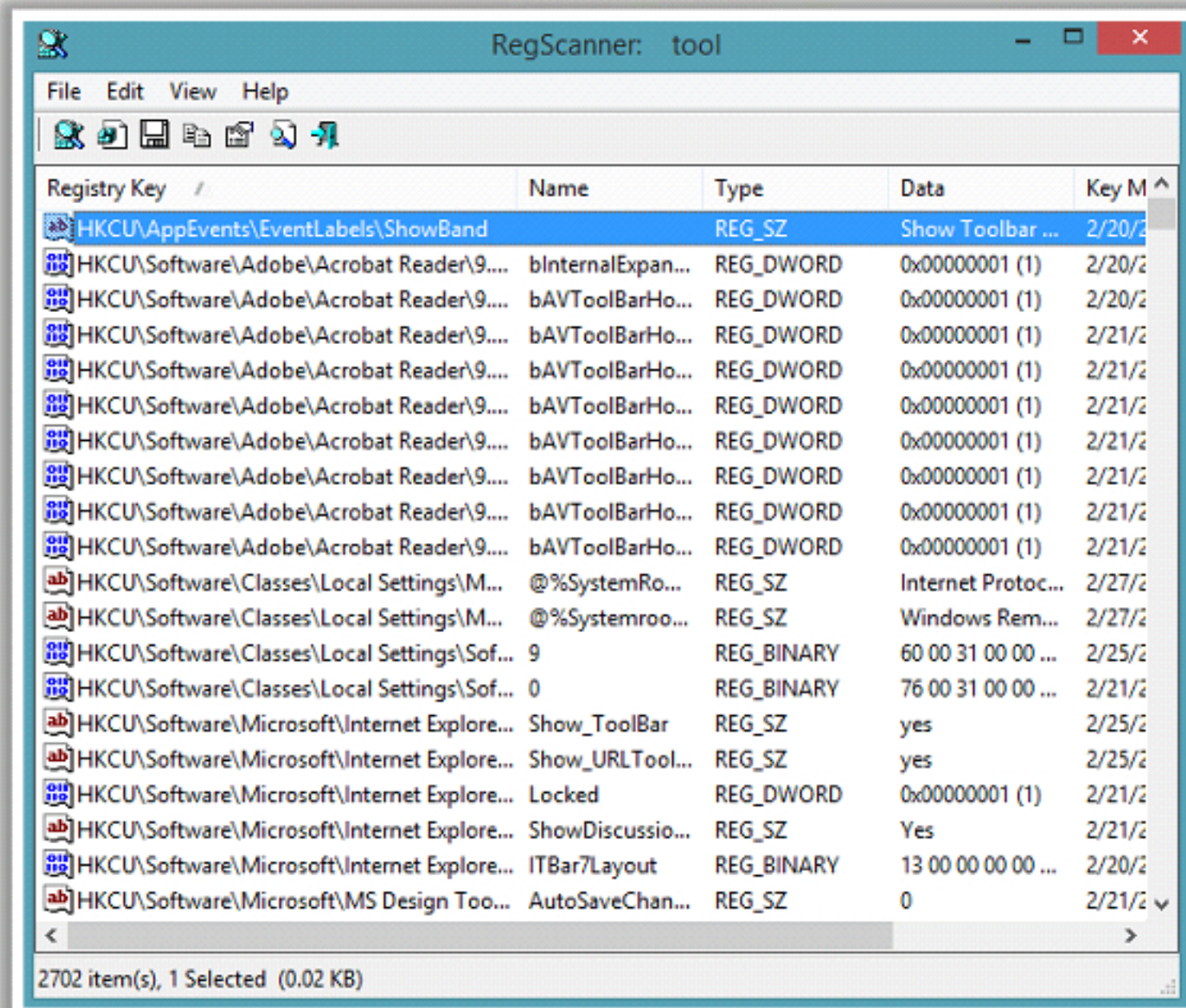
Key	Entry's name	Value	Entry last modified	Error severity	Error description	File reference	Reason
Invalid file or directory reference 1 / 62							
☐	HKCR\Local Settings\WrtCach	@{Microsoft.Reade	C:\Program File	20.02.2014, 13:06	20%	File or directory	C:\Program File Invalid file r
☐	HKCR\ProcMon.Logfile.1\Defa	@	"C:\Users\PGB\	27.02.2014, 11:22	25%	File or directory	C:\Users\PGB\ Invalid file r
☐	HKCR\ProcMon.Logfile.1\Defa	{KEY}	{KEY}	27.02.2014, 11:22	80%	File or directory	C:\Users\PGB\ Invalid file r
☐	HKCR\ProcMon.Logfile.1\shell	@	"C:\Users\PGB\	27.02.2014, 11:22	25%	File or directory	C:\Users\PGB\ Invalid file r
☐	HKCR\ProcMon.Logfile.1\shell	{KEY}	{KEY}	27.02.2014, 11:22	80%	File or directory	C:\Users\PGB\ Invalid file r
☐	HKCU\software\classes\Local	@{Microsoft.Reade	C:\Program File	N/A	20%	File or directory	C:\Program File Invalid file r
☐	HKCU\software\classes\Proch	@	"C:\Users\PGB\	N/A	25%	File or directory	C:\Users\PGB\ Invalid file r
☐	HKCU\software\classes\Proch	@	"C:\Users\PGB\	N/A	25%	File or directory	C:\Users\PGB\ Invalid file r
☒	HKCU\Software\Initex\Proxy	Path	c:\program files	27.02.2014, 04:30	99%	File or directory	c:\Program File Invalid file r
☐	HKCU\Software\Initex\Proxy	{KEY}	{KEY}	27.02.2014, 04:30	80%	File or directory	c:\Program File Invalid file r
☐	HKCU\Software\Microsoft\Win	C:\ManageEngine\	CN/A	27.02.2014, 11:42	99%	File or directory	C:\ManageEngi Invalid file r
☐	HKCU\Software\Microsoft\Win	C:\Program Files (x8	N/A	27.02.2014, 11:42	99%	File or directory	C:\Program File Invalid file r
☐	HKCU\Software\Microsoft\Win	C:\Program Files (x8	N/A	27.02.2014, 11:42	99%	File or directory	C:\Program File Invalid file r
☐	HKCU\Software\Microsoft\Win	C:\Program Files (x8	N/A	27.02.2014, 11:42	99%	File or directory	C:\Program File Invalid file r
☐	HKCU\Software\Microsoft\Win	C:\Program Files\Ne	N/A	27.02.2014, 11:42	99%	File or directory	C:\Program File Invalid file r

Selected: 1, highlighted: 1, total: 180

Custom fix... Fix Delete Close

Registry Entry Monitoring Tool: RegScanner

RegScanner allows you to scan the Registry, **find the desired Registry values** that match to the specified search criteria, and display them in one list



<http://www.nirsoft.net>

Registry Entry Monitoring Tools



Reg Organizer

<http://www.chemtable.com>



MJ Registry Watcher

<http://www.jacobsm.com>



Registry Viewer

<http://accessdata.com>



Comodo Cloud Scanner

<http://www.comodo.com>



Active Registry Monitor

<http://www.deviceclock.com>



Regshot

<http://regshot.sourceforge.net>



Buster Sandbox Analyzer

<http://bsa.isoftware.nl>



WhatChanged Portable

<http://portableapps.com>



SysTracer

<http://www.blueproject.ro>



Alien Registry Viewer

<http://lastbit.com>

Dynamic Malware Analysis: Network Activity Monitor

01

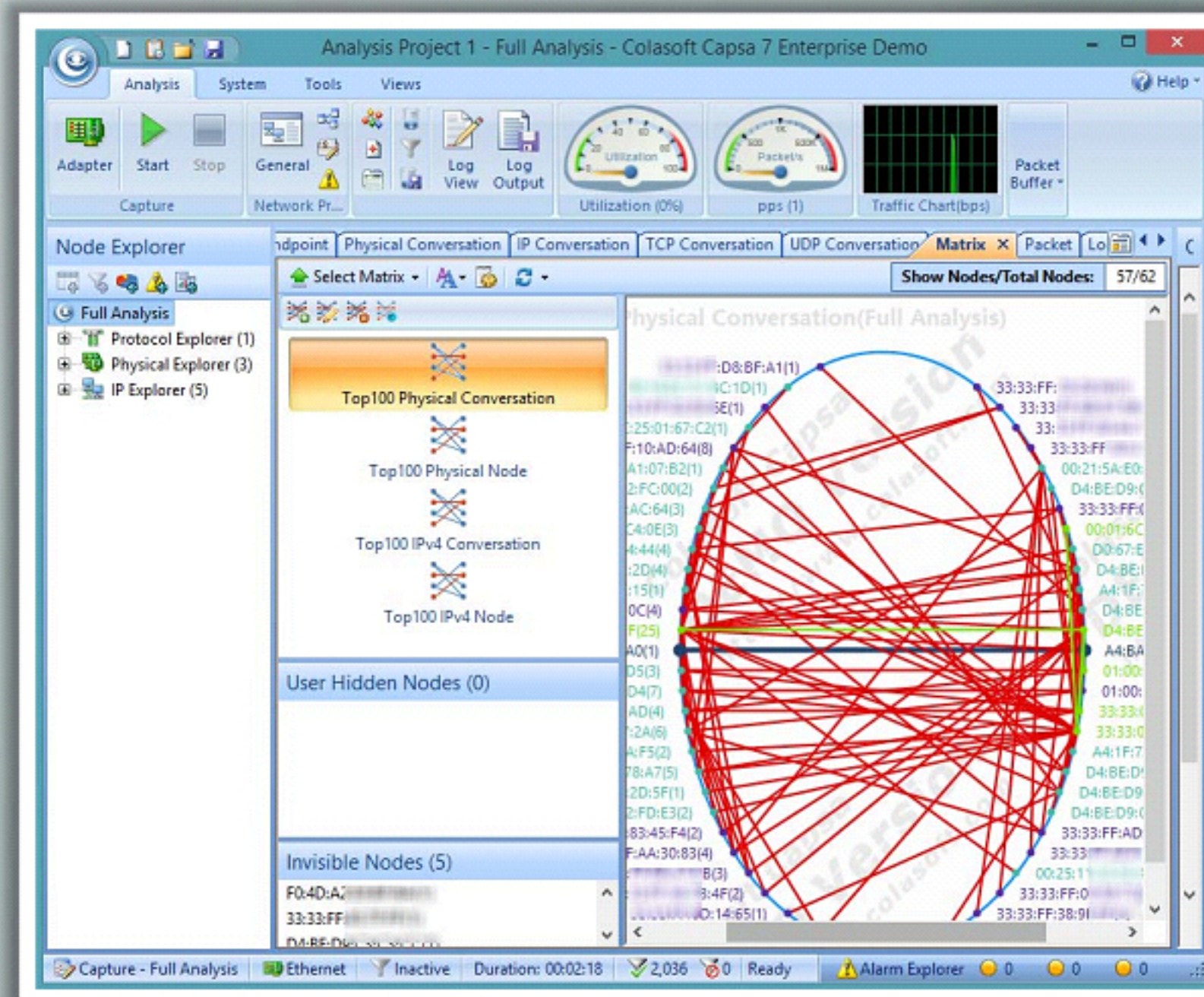
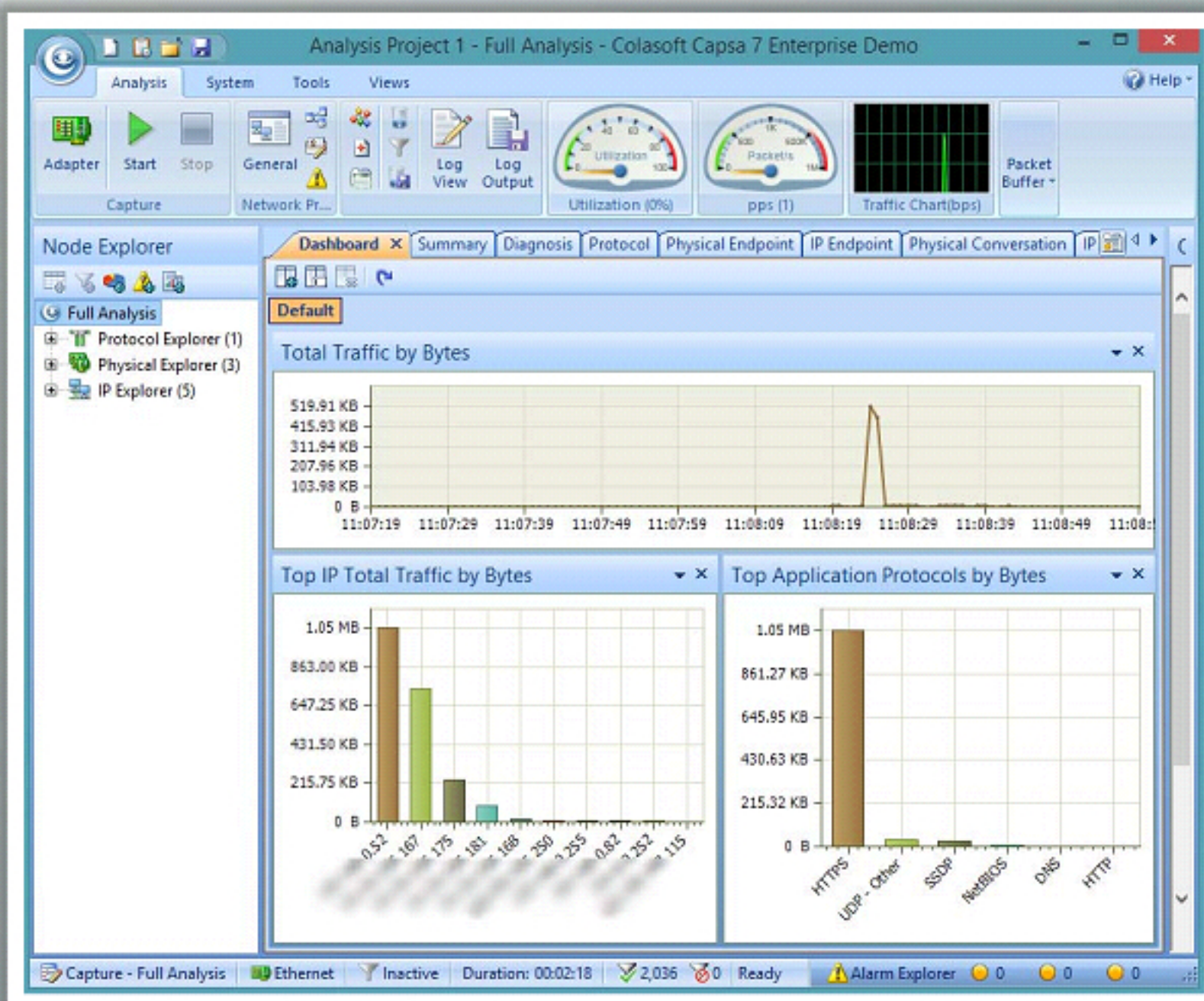
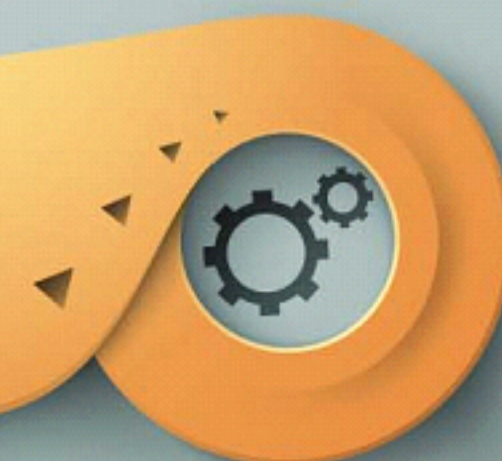
You can use tools such as **Wireshark**, **Capsa Network Analyzer**, etc. to monitor and capture live network traffic to and from the victim system during execution of the suspect program

02

Analyzing network traffic reveals **network capabilities** of the suspect program and its requirements

Detecting Trojans and Worms with Capsa Network Analyzer

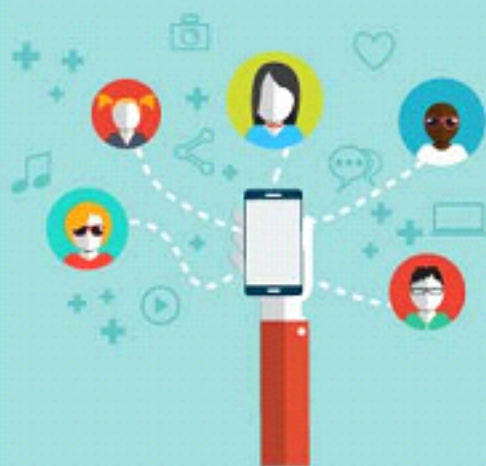
Capsa is an intuitive network analyzer, which provides detailed information to help check for any **Trojan** activities in a network



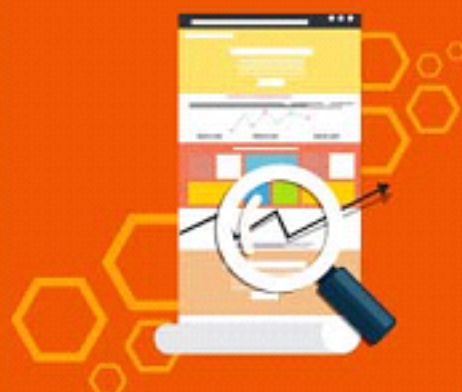
<http://www.colasoft.com>

Dynamic Malware Analysis:

Port Monitor



You can use tools such as CurrPorts, PortMon, SysAnalyzer, TCP View, etc., to monitor live open ports on the infected system and the remote system port numbers that are requested by the infected system while trying to connect to an email server



It reveals the network capabilities of the suspected program

Ex: Requesting remote system port number 25 implies Simple Mail Transfer Protocol



You can type 'netstat -an' in the command prompt to look for connection established to unknown or suspicious IP addresses

Administrator: Command Prompt

```
C:\Windows\system32>netstat -an
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:21	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:2869	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49155	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49157	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49158	0.0.0.0:0	LISTENING
TCP	10.0.0.4:139	0.0.0.0:0	LISTENING
TCP	10.0.0.4:2869	10.0.0.1:1088	TIME_WAIT
TCP	10.0.0.4:49693	10.0.0.2:445	ESTABLISHED
TCP	10.0.0.4:49794	123.176.32.139:80	ESTABLISHED
TCP	10.0.0.4:49795	123.176.32.139:80	ESTABLISHED
TCP	10.0.0.4:49796	10.0.0.1:56688	TIME_WAIT
TCP	10.0.0.4:49797	10.0.0.1:56688	TIME_WAIT
TCP	10.0.0.4:49798	10.0.0.1:56688	TIME_WAIT
TCP	10.0.0.4:49799	10.0.0.1:56688	TIME_WAIT
TCP	10.0.0.4:49802	10.0.0.1:56688	TIME_WAIT
TCP	10.0.0.4:49803	10.0.0.1:56688	TIME_WAIT
TCP	10.0.0.4:49804	10.0.0.1:56688	TIME_WAIT
TCP	10.0.0.4:49805	10.0.0.1:56688	TIME_WAIT
TCP	10.0.0.4:49808	10.0.0.1:56688	TIME_WAIT
TCP	10.0.0.4:49809	10.0.0.1:56688	TIME_WAIT
TCP	10.0.0.4:49810	10.0.0.1:56688	TIME_WAIT
TCP	10.0.0.4:49811	10.0.0.1:56688	TIME_WAIT



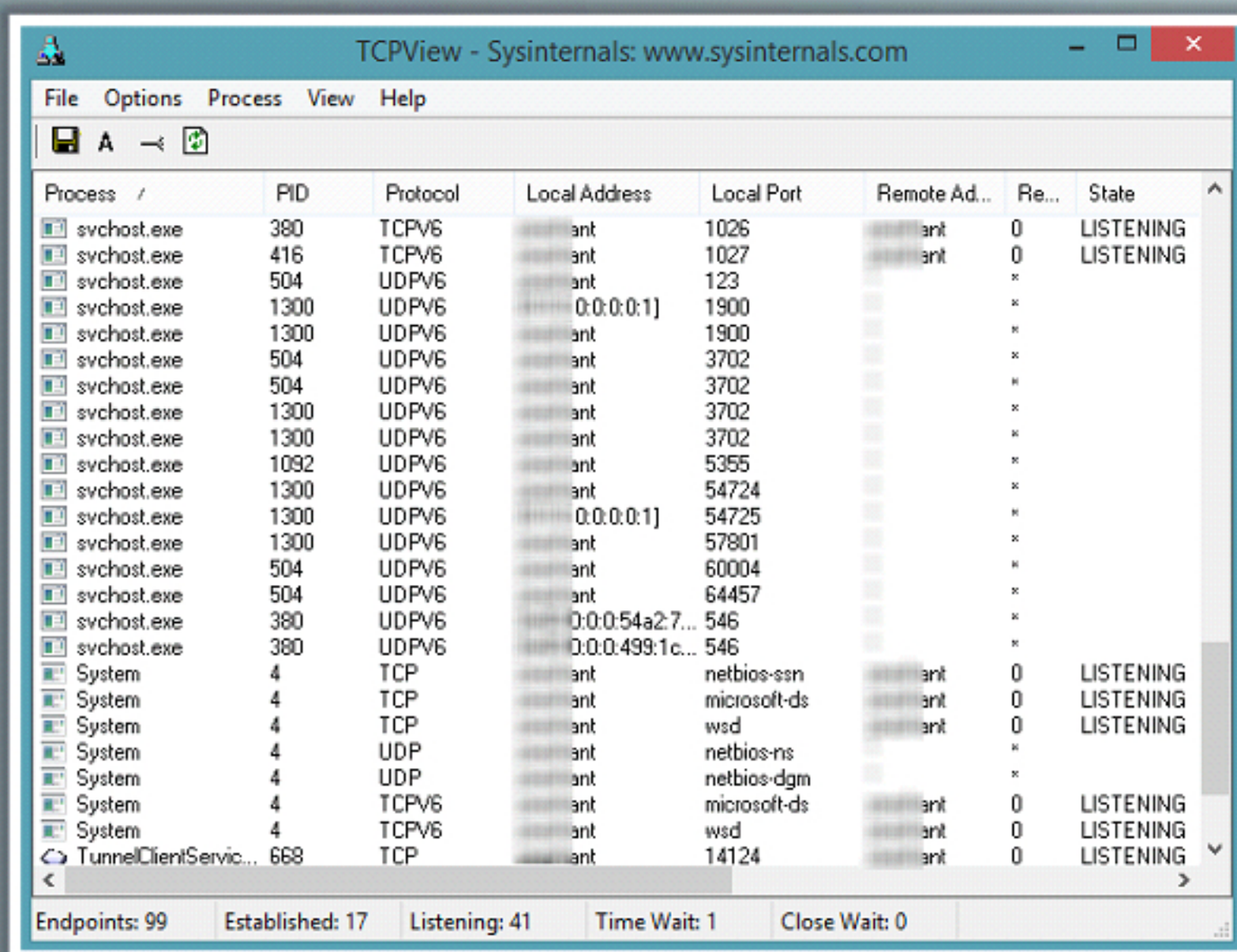
Port Monitoring Tools: **TCPView** and **CurrPorts**

TCPView

TCPView shows a detailed listings of all **TCP** and **UDP endpoints** on your system, including the local and remote addresses and state of **TCP connections**

CurrPorts

CurrPorts is a **network monitoring** software that displays the list of all currently opened **TCP/IP** and **UDP** ports on your local computer

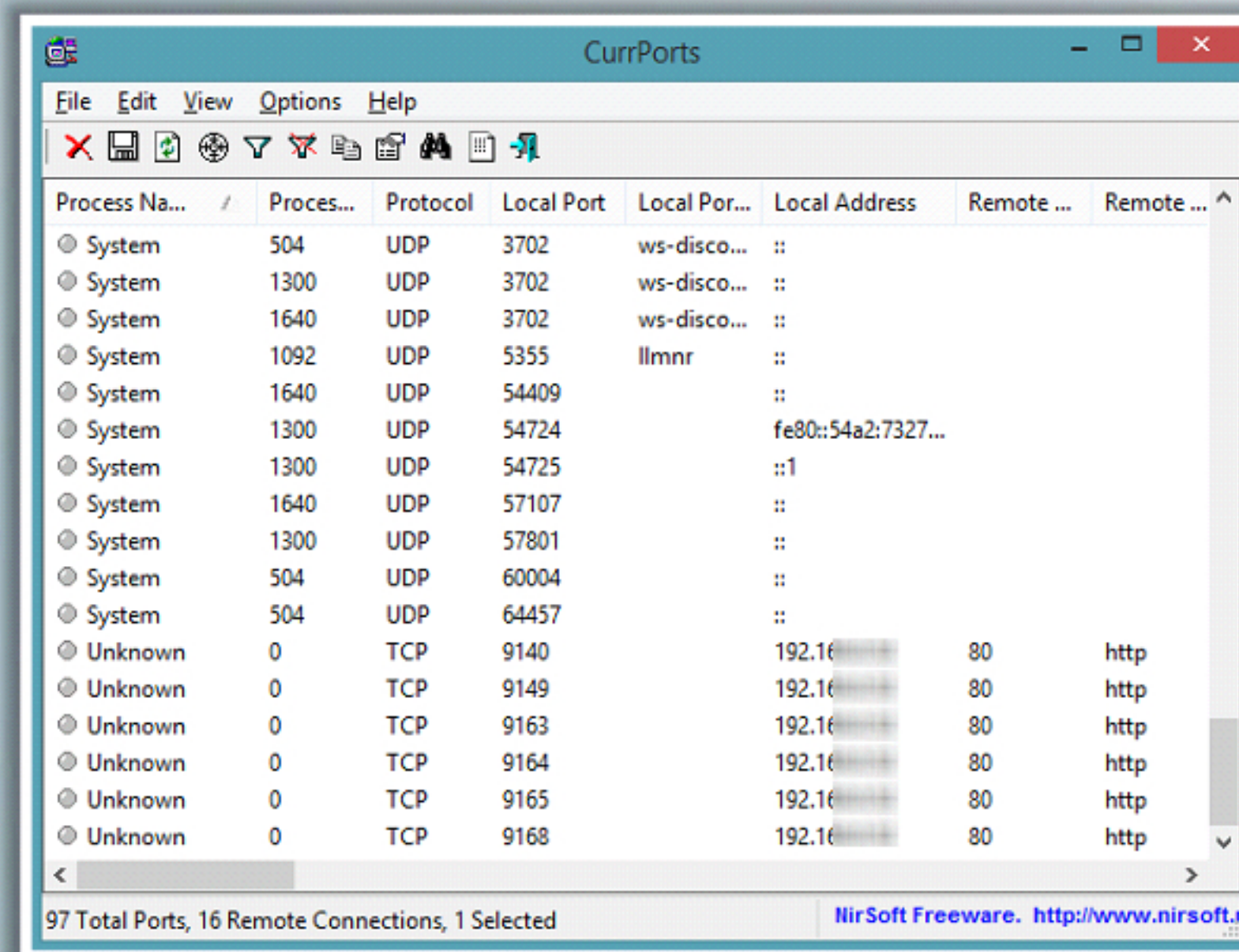


TCPView - Sysinternals: www.sysinternals.com

Process	PID	Protocol	Local Address	Local Port	Remote Ad...	Re...	State
svchost.exe	380	TCPV6	ant	1026	ant	0	LISTENING
svchost.exe	416	TCPV6	ant	1027	ant	0	LISTENING
svchost.exe	504	UDPV6	ant	123		*	
svchost.exe	1300	UDPV6	0:0:0:0:1	1900		*	
svchost.exe	1300	UDPV6	ant	1900		*	
svchost.exe	504	UDPV6	ant	3702		*	
svchost.exe	504	UDPV6	ant	3702		*	
svchost.exe	1300	UDPV6	ant	3702		*	
svchost.exe	1300	UDPV6	ant	3702		*	
svchost.exe	1092	UDPV6	ant	5355		*	
svchost.exe	1300	UDPV6	ant	54724		*	
svchost.exe	1300	UDPV6	0:0:0:0:1	54725		*	
svchost.exe	1300	UDPV6	ant	57801		*	
svchost.exe	504	UDPV6	ant	60004		*	
svchost.exe	504	UDPV6	ant	64457		*	
svchost.exe	380	UDPV6	0:0:0:54a2:7...	546		*	
svchost.exe	380	UDPV6	0:0:0:499:1c...	546		*	
System	4	TCP	ant	netbios-ssn	ant	0	LISTENING
System	4	TCP	ant	microsoft-ds	ant	0	LISTENING
System	4	TCP	ant	wsd	ant	0	LISTENING
System	4	UDP	ant	netbios-ns		*	
System	4	UDP	ant	netbios-dgm		*	
System	4	TCPV6	ant	microsoft-ds	ant	0	LISTENING
System	4	TCPV6	ant	wsd	ant	0	LISTENING
TunnelClientServic...	668	TCP	ant	14124	ant	0	LISTENING

Endpoints: 99 Established: 17 Listening: 41 Time Wait: 1 Close Wait: 0

<http://technet.microsoft.com>



CurrPorts

Process Na...	Proces...	Protocol	Local Port	Local Por...	Local Address	Remote ...	Remote ...
System	504	UDP	3702	ws-disco...	::		
System	1300	UDP	3702	ws-disco...	::		
System	1640	UDP	3702	ws-disco...	::		
System	1092	UDP	5355	llmnr	::		
System	1640	UDP	54409		::		
System	1300	UDP	54724		fe80::54a2:7327...		
System	1300	UDP	54725		::1		
System	1640	UDP	57107		::		
System	1300	UDP	57801		::		
System	504	UDP	60004		::		
System	504	UDP	64457		::		
Unknown	0	TCP	9140		192.16...	80	http
Unknown	0	TCP	9149		192.16...	80	http
Unknown	0	TCP	9163		192.16...	80	http
Unknown	0	TCP	9164		192.16...	80	http
Unknown	0	TCP	9165		192.16...	80	http
Unknown	0	TCP	9168		192.16...	80	http

97 Total Ports, 16 Remote Connections, 1 Selected

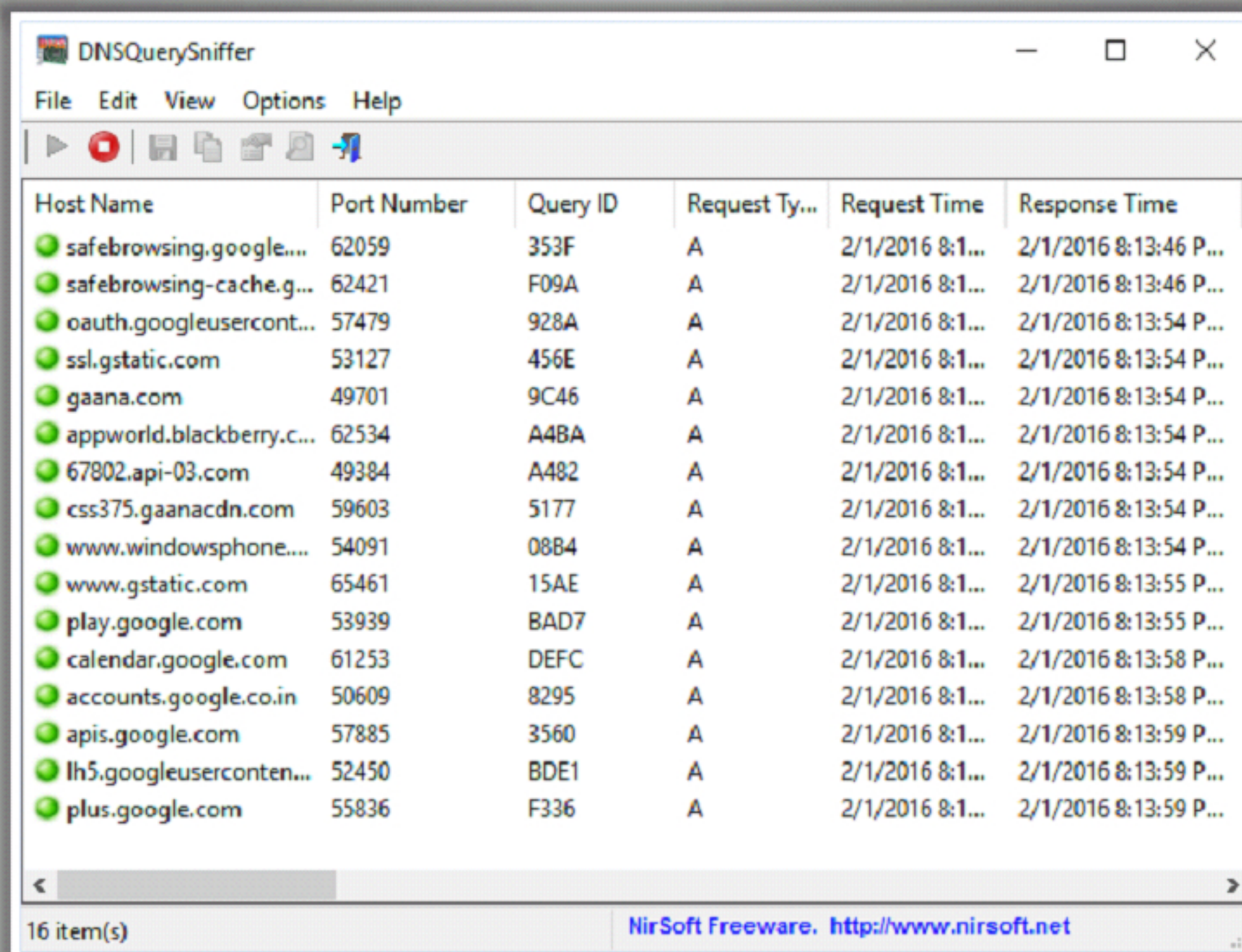
NirSoft Freeware. <http://www.nirsoft.net>

<http://www.nirsoft.net>

Dynamic Malware Analysis:

DNS Monitoring/Resolution

You can use tools such as **DNSstuff**, **DNSQuerySniffer**, etc. to verify the DNS servers malware try to connect and identify the **type of connection**



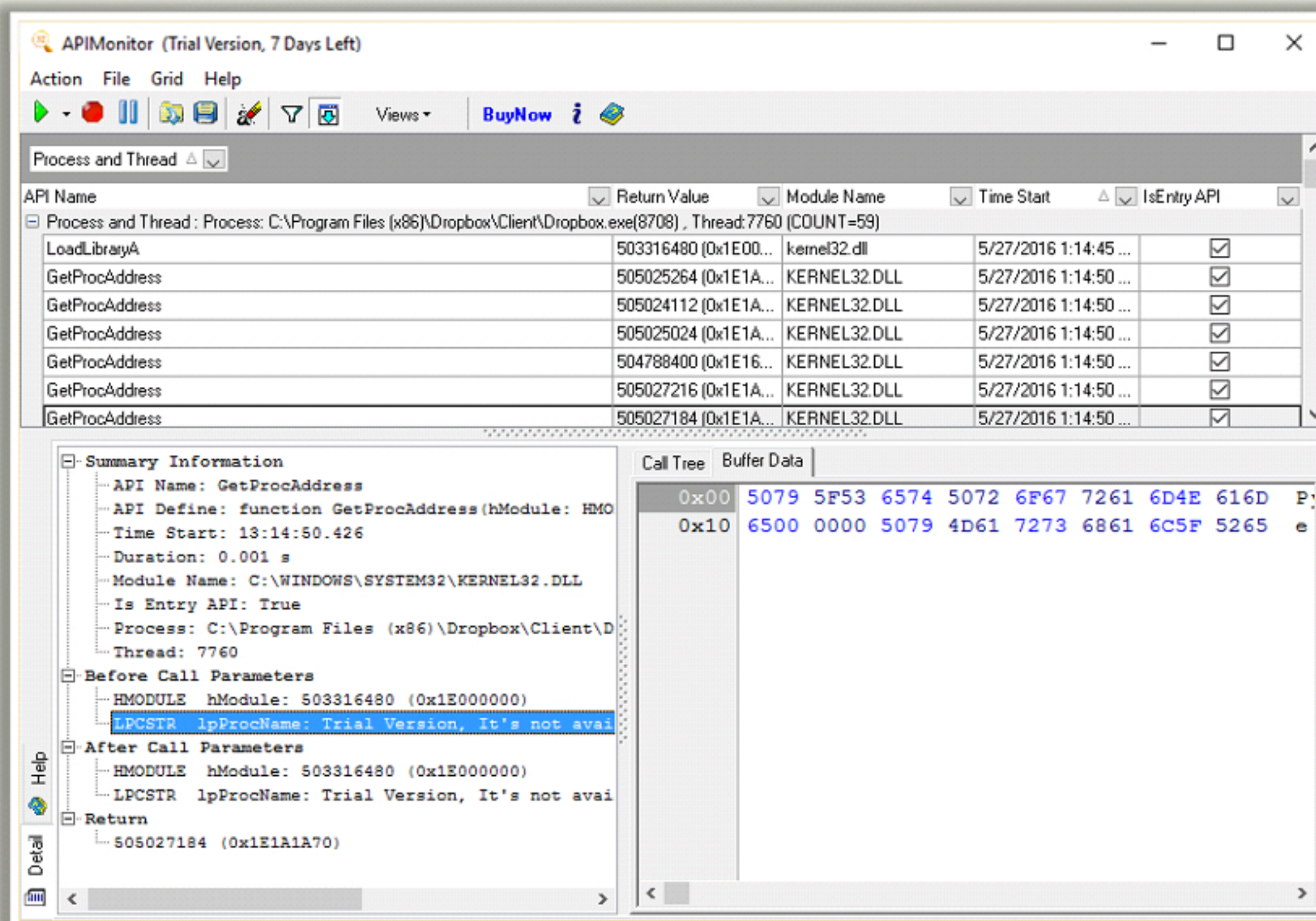
The screenshot shows the DNSQuerySniffer application window. It has a menu bar (File, Edit, View, Options, Help) and a toolbar with icons for play, stop, save, print, and zoom. Below the toolbar is a table with 6 columns: Host Name, Port Number, Query ID, Request Ty..., Request Time, and Response Time. The table contains 16 rows of data, each with a green status icon in the first column. At the bottom of the window, it says '16 item(s)' and 'NirSoft Freeware. http://www.nirsoft.net'.

Host Name	Port Number	Query ID	Request Ty...	Request Time	Response Time
safebrowsing.google....	62059	353F	A	2/1/2016 8:1...	2/1/2016 8:13:46 P...
safebrowsing-cache.g...	62421	F09A	A	2/1/2016 8:1...	2/1/2016 8:13:46 P...
oauth.googleusercont...	57479	928A	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
ssl.gstatic.com	53127	456E	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
gaana.com	49701	9C46	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
appworld.blackberry.c...	62534	A4BA	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
67802.api-03.com	49384	A482	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
css375.gaanacdn.com	59603	5177	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
www.windowsphone....	54091	08B4	A	2/1/2016 8:1...	2/1/2016 8:13:54 P...
www.gstatic.com	65461	15AE	A	2/1/2016 8:1...	2/1/2016 8:13:55 P...
play.google.com	53939	BAD7	A	2/1/2016 8:1...	2/1/2016 8:13:55 P...
calendar.google.com	61253	DEFC	A	2/1/2016 8:1...	2/1/2016 8:13:58 P...
accounts.google.co.in	50609	8295	A	2/1/2016 8:1...	2/1/2016 8:13:58 P...
apis.google.com	57885	3560	A	2/1/2016 8:1...	2/1/2016 8:13:59 P...
lh5.googleusercontent...	52450	BDE1	A	2/1/2016 8:1...	2/1/2016 8:13:59 P...
plus.google.com	55836	F336	A	2/1/2016 8:1...	2/1/2016 8:13:59 P...

<http://www.nirsoft.net>

Dynamic Malware Analysis: API Calls Monitor

- You can use tools such as **API Monitor** to intercept the API calls from the suspected program to the OS
- Analyzing the API calls may reveal the suspected program's interaction with the OS, which is of investigative value (may provide correlative clues regarding system and network activity)

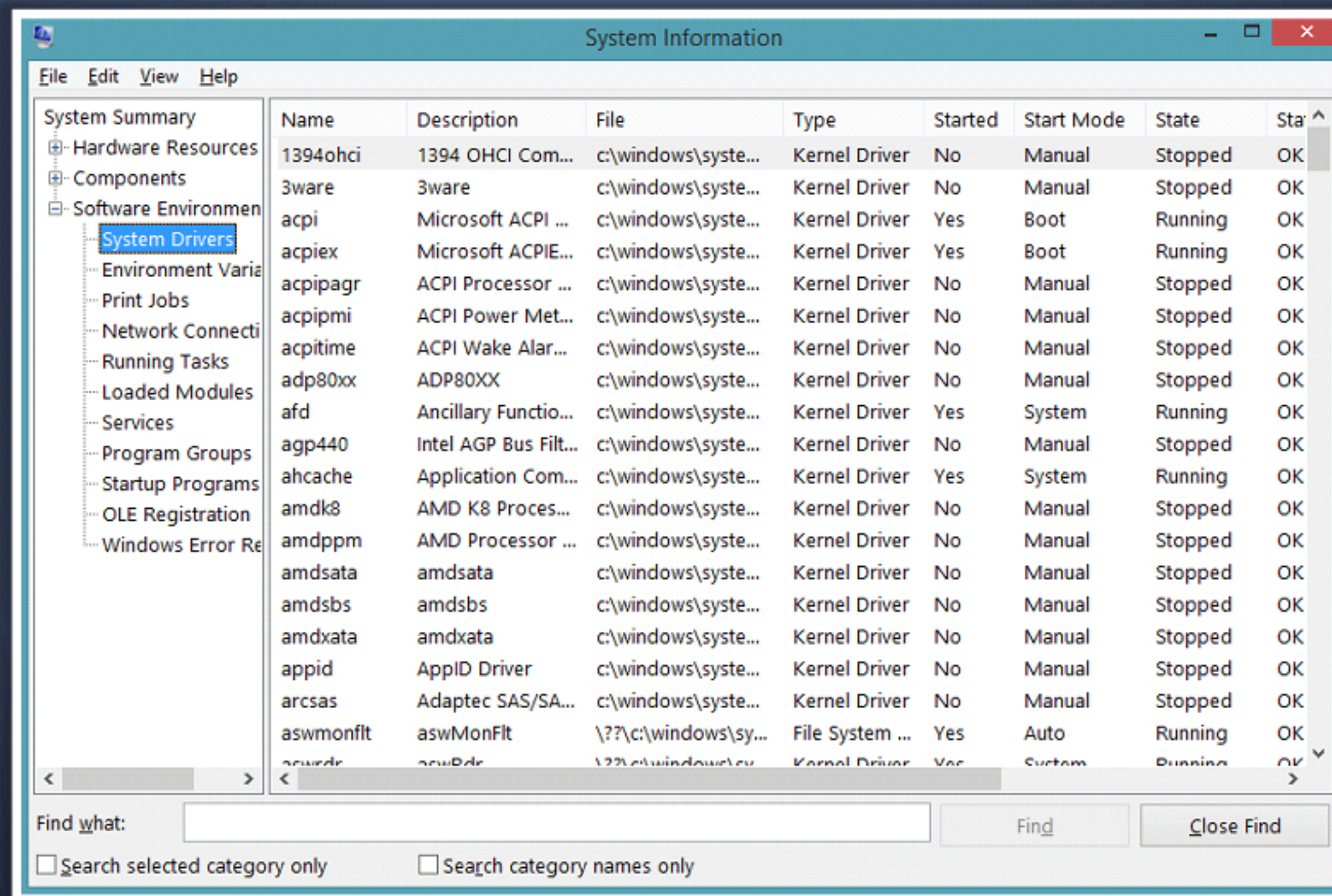


<http://www.apimonitor.com>

Dynamic Malware Analysis:

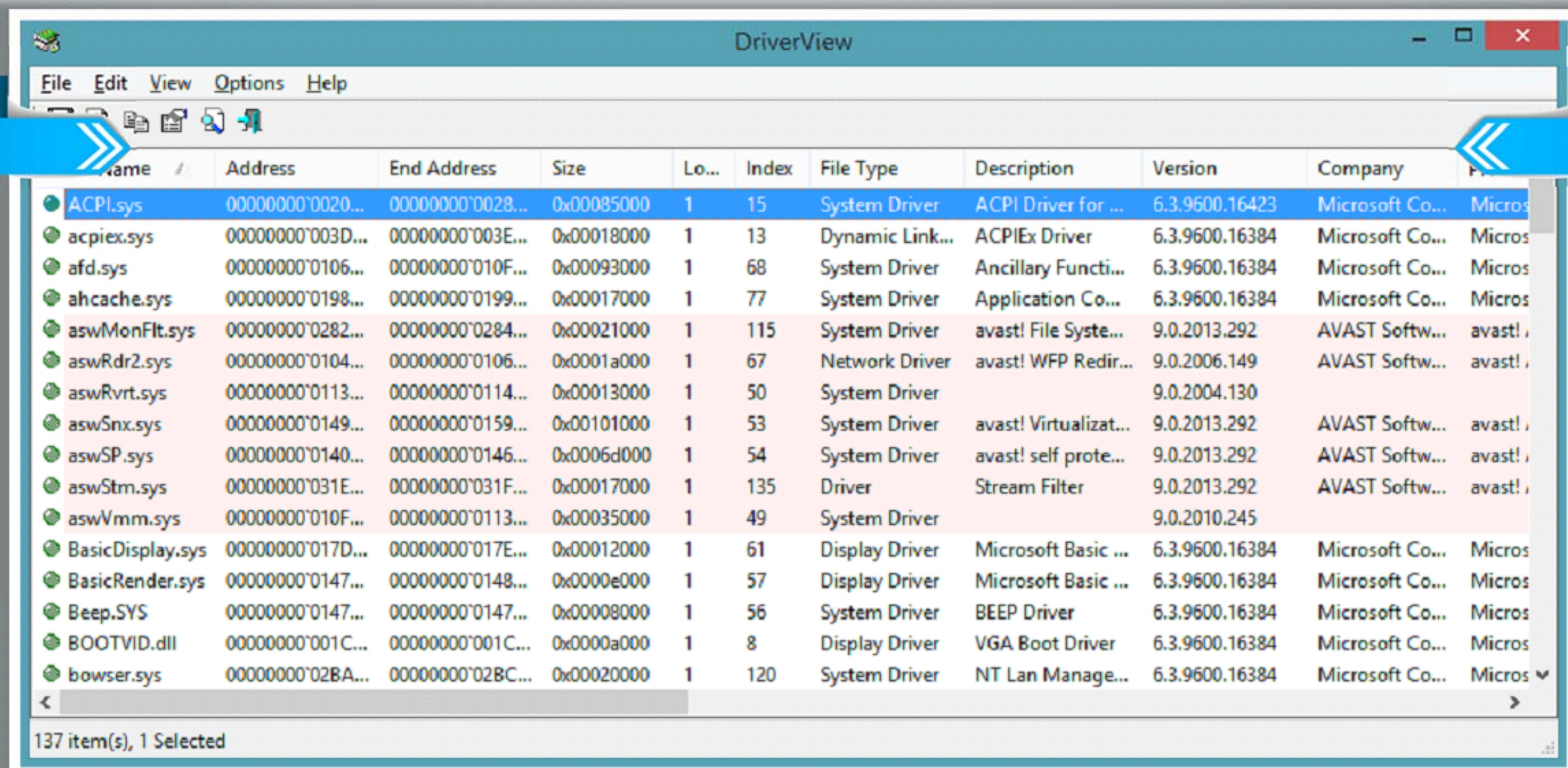
Device Drivers Monitor

- Malware gets installed along with device drivers **downloaded from untrusted sources** and use these as shield to avoid detection
- You have to scan for **suspicious device drivers** and verify if they are genuine and downloaded from the publisher's original site
- Go to **Run** → **Type msinfo32** → **Software Environment** → **System Drivers**



Device Drivers Monitoring Tool: DriverView

DriverView utility displays a list of all **device drivers** currently loaded on the system. For each driver in the list, **additional information** is displayed such as load address of the driver, description, version, product name, and the company that created the driver, etc.



Name	Address	End Address	Size	Lo...	Index	File Type	Description	Version	Company	Product Name
ACPI.sys	00000000`0020...	00000000`0028...	0x00085000	1	15	System Driver	ACPI Driver for ...	6.3.9600.16423	Microsoft Co...	Micros...
acpiex.sys	00000000`003D...	00000000`003E...	0x00018000	1	13	Dynamic Link...	ACPIEx Driver	6.3.9600.16384	Microsoft Co...	Micros...
afd.sys	00000000`0106...	00000000`010F...	0x00093000	1	68	System Driver	Ancillary Functi...	6.3.9600.16384	Microsoft Co...	Micros...
ahcache.sys	00000000`0198...	00000000`0199...	0x00017000	1	77	System Driver	Application Co...	6.3.9600.16384	Microsoft Co...	Micros...
aswMonFlt.sys	00000000`0282...	00000000`0284...	0x00021000	1	115	System Driver	avast! File Syste...	9.0.2013.292	AVAST Softw...	avast!
aswRdr2.sys	00000000`0104...	00000000`0106...	0x0001a000	1	67	Network Driver	avast! WFP Redir...	9.0.2006.149	AVAST Softw...	avast!
aswRvrt.sys	00000000`0113...	00000000`0114...	0x00013000	1	50	System Driver		9.0.2004.130		
aswSnx.sys	00000000`0149...	00000000`0159...	0x00101000	1	53	System Driver	avast! Virtualizat...	9.0.2013.292	AVAST Softw...	avast!
aswSP.sys	00000000`0140...	00000000`0146...	0x0006d000	1	54	System Driver	avast! self prote...	9.0.2013.292	AVAST Softw...	avast!
aswStm.sys	00000000`031E...	00000000`031F...	0x00017000	1	135	Driver	Stream Filter	9.0.2013.292	AVAST Softw...	avast!
aswVmm.sys	00000000`010F...	00000000`0113...	0x00035000	1	49	System Driver		9.0.2010.245		
BasicDisplay.sys	00000000`017D...	00000000`017E...	0x00012000	1	61	Display Driver	Microsoft Basic ...	6.3.9600.16384	Microsoft Co...	Micros...
BasicRender.sys	00000000`0147...	00000000`0148...	0x0000e000	1	57	Display Driver	Microsoft Basic ...	6.3.9600.16384	Microsoft Co...	Micros...
Beep.SYS	00000000`0147...	00000000`0147...	0x00008000	1	56	System Driver	BEEP Driver	6.3.9600.16384	Microsoft Co...	Micros...
BOOTVID.dll	00000000`001C...	00000000`001C...	0x0000a000	1	8	Display Driver	VGA Boot Driver	6.3.9600.16384	Microsoft Co...	Micros...
bowser.sys	00000000`02BA...	00000000`02BC...	0x00020000	1	120	System Driver	NT Lan Manage...	6.3.9600.16384	Microsoft Co...	Micros...

137 item(s), 1 Selected

Device Drivers Monitoring Tools



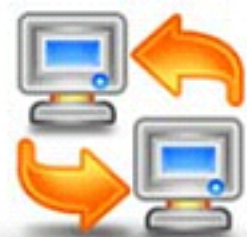
Driver Detective

<http://www.drivershq.com>



Driver Reviver

<http://www.reviversoft.com>



Unknown Device Identifier

<http://www.zhangduo.com>



ServiWin

<http://www.nirsoft.net>



DriverGuide Toolkit

<http://www.driverguidetoolkit.com>



Driver Fusion

<https://treexy.com>



InstalledDriversList

<http://www.nirsoft.net>



My Drivers

<http://www.zhangduo.com>



Driver Magician

<http://www.drivermagician.com>



DriverEasy

<http://www.drivereasy.com>

Dynamic Malware Analysis: Startup Programs Monitor

Check startup
program entries
in the registry

Details are covered in next slide



Check automati-
cally loaded

C:\Windows\System32\drivers



Check
boot.ini

Check **boot.ini** or **bcd** (bootmgr) entries



Check Windows
services automatic
started

Go to **Run** → Type **services.msc** → Sort by
Startup Type



Check startup
folder

C:\ProgramData\Microsoft\Windows\Start
Menu\Programs\Startup

C:\Users\<User Name>\AppData\Roaming\
Microsoft\Windows\Start Menu\Programs\Startup

Windows 10 Startup Registry Entries

Windows Startup Setting

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Runonce



Explorer Startup Setting

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup



IE Startup Setting

HKCU\SOFTWARE\Microsoft\Internet Explorer\URLSearchHooks
HKLM\SOFTWARE\Microsoft\Internet Explorer\Toolbar
HKLM\SOFTWARE\Microsoft\Internet Explorer\Extensions
HKCU\SOFTWARE\Microsoft\Internet Explorer\MenuExt



Startup Programs Monitoring Tool: Security AutoRun

Security AutoRun displays the **list of all applications** that are loaded automatically when Windows starts up



Security Autorun - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services]

Left sidebar (Tree View):

- Current User
 - Run (0)
 - Run Once (0)
 - Policies (0)
 - Desktop (1)
 - Load Run (2)
- Local Machine
 - Run (2)
 - Run Once (0)
 - Run OnceEx (0)
 - RunServicesOnce (0)
 - RunServices (0)
 - Policies (0)
 - ShellObject (1)
 - Installed Components (5)
- WinLogon
 - WinLogon (9)
- Startup Folder
 - Common (0)
 - User (1)
- Startup Services
 - services (35)
- Driver List
 - Drivers (265)
- Know DLLs
 - List DLLs (0)
- AppInit DLLs
 - AppInit DLLs (1)
- Scheduled Tasks
 - Task Scheduler (2)
- Ini Startup
 - Win.ini (1)
 - System.ini (1)

Top tabs:

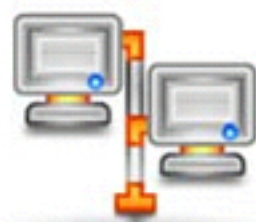
- HKCU / Run (0)
- HKLM / Run (2)
- Startup (user) - (1)
- Startup (common) - (0)
- HKCU / Explorer-Run (0)
- HKCU / Desktop (1)
- HKLM / RunServices (0)
- HKLM / RunServicesOnce (0)
- Drivers - (265)
- AppInit DLLs (1)
- Know DLLs (0)
- Scheduled Tasks (2)
- Ini Startup (2)
- HKLM / Run Once (0)
- HKLM / ShellObject (1)
- HKLM / Run OnceEx (0)
- Startup (services) - (35)

Service Name	Description	Status	Path
COMSysApp	COM+ System Application	Stopped	C:\Windows\system32\clbcatq.dll /Processid:{02D4B3F...
defragsvc	Optimize drives	Stopped	C:\Windows\system32\svchost.exe -k defragsvc
Fax	Fax	Stopped	C:\Windows\system32\fxssvc.exe
gupdate	Google Update Service (gupdate)	Stopped	"C:\Program Files (x86)\Google\Update\GoogleUpdate.e...
gupdatem	Google Update Service (gupdatem)	Stopped	"C:\Program Files (x86)\Google\Update\GoogleUpdate.e...
IEEtwCollectorSer...	Internet Explorer ETW Collector Se...	Stopped	C:\Windows\system32\IEEtwCollector.exe /V
MSDTC	Distributed Transaction Coordinator	Stopped	-
msiserver	Windows Installer	Stopped	C:\Windows\system32\msiexec.exe /V
nvsvc	NVIDIA Display Driver Service	Running	"C:\Windows\system32\nvsvc.exe"
nvUpdatusService	NVIDIA Update Service Daemon	Running	"C:\Program Files (x86)\NVIDIA Corporation\NVIDIA Upd...
ose	Office Source Engine	Stopped	"C:\Program Files (x86)\Common Files\Microsoft Shared\...
osppsvc	Office Software Protection Platform	Running	"C:\Program Files\Common Files\Microsoft Shared\Office...
PerfHost	Performance Counter DLL Host	Stopped	C:\Windows\SysWow64\perfhost.exe
rpcapd	Remote Packet Capture Protocol v...	Stopped	"C:\Program Files (x86)\WinPcap\rpcapd.exe" -d -f "C:\P...
RpcLocator	Remote Procedure Call (RPC) Locator	Stopped	C:\Windows\system32\locator.exe
smphost	Microsoft Storage Spaces SMP	Stopped	C:\Windows\System32\svchost.exe -k smphost
SNMPTRAP	SNMP Trap	Stopped	C:\Windows\System32\snmptrap.exe
Spooler	Print Spooler	Running	C:\Windows\System32\spoolsv.exe
sppsvc	Software Protection	Stopped	-
Stereo Service	NVIDIA Stereoscopic 3D Driver Ser...	Running	"C:\Program Files (x86)\NVIDIA Corporation\3D Vision\pv...
stisvc	Windows Image Acquisition (WIA)	Stopped	C:\Windows\system32\svchost.exe -k imgsvc
swprv	Microsoft Software Shadow Copy P...	Stopped	C:\Windows\System32\svchost.exe -k swprv
TrustedInstaller	Windows Modules Installer	Stopped	-
UI0Detect	Interactive Services Detection	Stopped	C:\Windows\system32\UI0Detect.exe

(35) Items HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

<http://tcpmonitor.altervista.org>

Startup Programs Monitoring Tools



Autoruns for Windows

<http://technet.microsoft.com>



PCTuneUp Free Startup Manager

<http://www.pctuneupsuite.com>



WinTools.net 16.0.0 Premium

<http://www.wintools.net>



Ccleaner

<https://www.piriform.com>



StartEd Pro

<http://www.outertech.com>



WinPatrol

<http://www.winpatrol.com>



Startup Delayer

<http://www.r2.com.au>



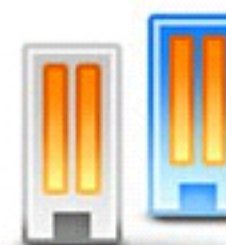
Chameleon Startup Manager

<http://www.chameleon-managers.com>



WhatInStartup

<http://www.nirsoft.net>



Startup Booster

<http://www.smartpctools.com>

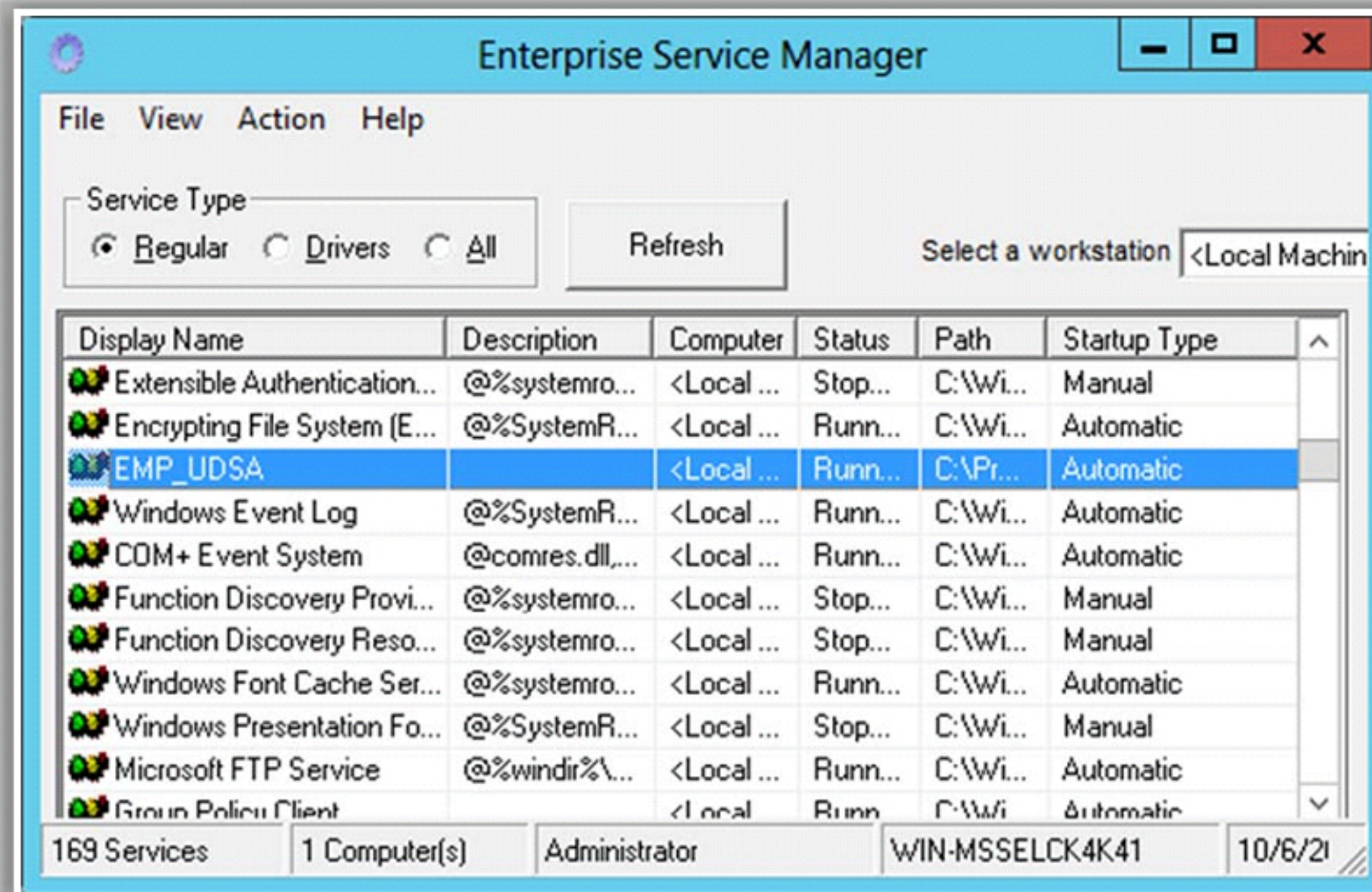
Dynamic Malware Analysis: Windows Services Monitor

1

Malware may **rename their processes** to look like a genuine Windows service in order to avoid detection

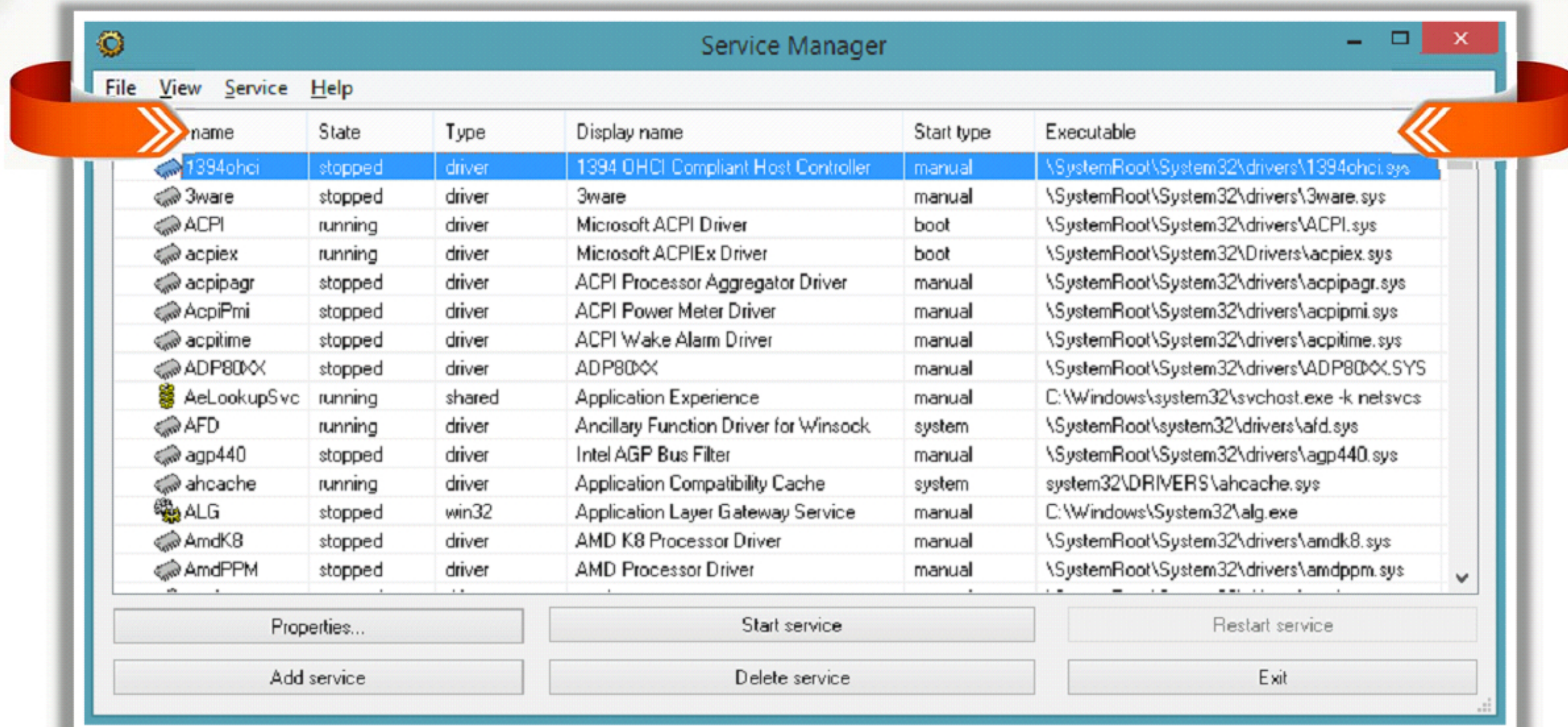
2

You can use various tools to identify such suspicious Windows Services



Windows Services Monitoring Tool: Windows Service Manager (SrvMan)

Windows Service Manager (SrvMan) simplifies all common tasks related to Windows services. It can create services (both Win32 and Legacy Driver) without restarting Windows, delete existing services, and change the service configuration



<http://tools.sysprogs.org>

Windows Services Monitoring Tools



Advanced Win Service Manager

<http://securityxploded.com>



AnVir Task Manager

<http://www.anvir.com>



Netwrix Service Monitor

<http://www.netwrix.com>



Process Hacker

<http://processhacker.sourceforge.net>



PC Services Optimizer

<http://www.smartpcutilities.com>



Free Windows Service Monitor Tool

<http://www.manageengine.com>



ServiWin

<http://www.nirsoft.net>



Nagios XI

<http://www.nagios.com>



PRTG Network Monitor

<https://www.paessler.com>



Service+

<http://www.activeplus.com>

Analysis of Malicious Documents

Steps to detect malware in PDF and MS Office document files:



Enlist the common **vulnerabilities and exploits**

Find the uncertain **scripts or code**



Examine the file for **suspicious elements** or **pointers of malware**

Search for **encrypted scripts** and decrypt



Inspect the **metadata**

Extract the **scripts** and analyze



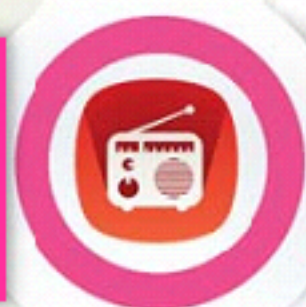
Verify the **structure** and **content**

Scan with **malware scanner**



Note: Refer lab manual for demonstration of malicious document analysis

Malware Analysis Challenges



Accuracy of the analysis process



Detection of malware pieces and traits



Amount of data to be analyzed



Changing technologies and dynamics of malware creation and propagation



Anti-analysis procedures such as encryption, code obfuscation, and deletion of records

Module Summary

- ☐ Malware is a malicious software that damages or disables computer systems, and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud
- ☐ Components of a malware software relies on the requirements of the malware author who designs it for a specific target to perform the intended tasks
- ☐ Malware forensics deals with identifying and capturing malicious code, and evidences of its effect on the infected system
- ☐ To analyze malware, a dedicated laboratory system is required, which can be infected keeping the production environment safe
- ☐ Performing malware analysis enables you to know the type of malware, how it works, its behavior, and impact on the target system
- ☐ Static analysis/code analysis involves going through the executable binary code without actually executing it to have a better understand of the malware and its purpose
- ☐ Dynamic analysis/behavioral analysis involves executing the malware code to know how it interacts with the host system and its impact on it