



## **Computer Forensics Toolkit v 1.0.0.1**

JaguarForensics Toolkit is very rapid Forensics report generation application. It generates HTML report with selected options for inspected computer.

It runs on USB Flash Disk. It does not install and modify any program on inspected machines. Just collects the information and analyze with Mal-ware Databases, checks Hidden Programs, drivers. Especially checks the well-known mal-ware application such as Browser Helper Objects, Tool Bars and also identify Hidden processes, drivers. It uses self contained Mal-ware Database which can be upgraded from Internet.

The program creates quick web links on the generated reports for detailed search with program name , GUID and MD5 Hashes. It helps to get detailed information about the processes.

It can identify Hidden Processes, Hidden Drivers (**ROOTKIT-API HOOKS**) which can not be detect with well-known Anti-Virus, Anti-Spy programs.

## Features;

- Detailed Computer Info. (H/W, O/S, BIOS, Service Packs vs.)
- Users, Groups, Network Shares
- Running Programs (EXE, SYS, Service, Objects)
- Startup Programs
- Active Network Ports and Using Processes
- Inspector Form
- Event logs
- Device Drivers
- Digital Certificate Verifying
- Inspecting Well-known BHO, Key Logger, Screen Logger, Trojan Horse ve Backdoors
- ROOTKIT & API HOOK, Hidden Processes & Drivers
- Detailed Search on WEB with Program Name, GUID and MD5 Hashes

ile <u>H</u> elp			_								
8 🔌 🐧	Repo	ting 📫									
ASUSNB Hardware BIOS Info Physical MainBoar	temory		aguar	Soft	Forensi	cs Tooll	Kit			G	
Video Cor					Network Conn					-	
- Boot Hard - Logical Di	iDisk sks	Protocol TCP	Status Listening	ds db(3050)	Local Address ASUSNB (0.0.0)	Rem. Port 57532	Remote A	ddress	PID	Process System	
KeyBoard	Г.	TCP	Listening	https/4431	ASUSNB (0.0.0.0)	2080	i.		4	System	
USB Cont	rollers	TCP	Listening	http[80]	ASUSNB (0.0.0.0)	32839			4	System	
Printers Pointing I	evices	TCP	Listening	52271	ASUSNB (0.0.0.0)	2			4	System	
PEMEIA		TCP TCP	Established Listening	1058	BOS (192:163:57:57) ASUSNB (127:0:0.1)	1863 39070	(207.46.10	7.58)	4	System System	
Operating Sy		TCP	Listening	6697	ASUSNB (0.0.0.0)	26792	÷		4	System	
- System I Boot Con		TCP	Listening	microsoft-ds[445]	ASUSNB (0.0.0.0)	18595			4	System	
<ul> <li>Environment</li> <li>User Accounts</li> <li>System Accounts</li> <li>Groups</li> <li>Installed Patches</li> <li>System EventLog</li> <li>Security EventLog</li> <li>Application EventLog</li> <li>Applications</li> </ul>		TCP	Established	1078	805 (192.168.57.57)	29672	(75.176.60		4	System	
		TCP TCP	Established Listening	1538	BOS (192.168.57.57) ASUSNB (0.0.0.0)	43207	(192.168.5	/.212]	4	System System	
		TCP	Listening	epmap(135)	ASUSNB (0.0.0.0)	43207 39038			4	System	
		TCP	Listening	netbios-ssn[139]	netbios-ssn(139) (192.168.57.57)	45089			4	System	
		TCP	Listening	6697	ASUSNB (0.0.0.0)	26792			516	RMHSvc.exe	
		TCP TCP	Listening	epmap[135]	ASUSNB (0.0.0.0)	39038 57532				sychost.exe fbserver.exe	
		[epmap]	135] Locat	ion Service (RPC	- EPMAP	2080				inetinfo.exe	
Network	1	TCP	Listening	1035	ASUSNB (0.0.0.0)	43207			1968	inetinfo.exe	
Network	Adapters Connections	TCP	Listening	http[80]	ASUSNB (0.0.0.0)	32839				inetinfo.exe	
Network !	Shares	TCP TCP	Listening Established	1046	ASUSNB (127.0.0.1) BOS (192.168.57.57)	39070	175 176 60	1741	2060	alg.exe Skurne ave	
IP Route		TCP	Listening	52271	ASUSNB (0.0.0.0)	23572	110-110-50	(114)		Skype.exe	
Host Files Reporting		TCP	Established	1058	BOS (192.168.57.57)	1863	[207.46.10	7.58)	3344	mimoga exe	
		UDP	0	4500	ASUSNB (0.0.0.0)		•		4	System	
		UDP UDP	0	1068	ASUSNB (127.0.0.1) ASUSNB (0.0.0.0)				4	System System	
		UDP	0	1025	ASUSNB (0.0.0.0)				4	System	
		UDP	0	nto[123]	ASUSNB (127.0.0.1)				4	System	
		UDP	0	1048	ASUSNB (127.0.0.1)				4	System	
		UDP UDP	0	1900 nto[123]	BOS (192.168.57.57) ntp[123] (192.168.57.57)				4	System System	
Service Ma	nager		C:\P		Microsoft SQL Serve	r\80		Comm	on Sta		
BTTray			C:\ So	C: A C:\Program Files\Microsoft SOI Server\88					pn Startup		
Adobe Gamma Loader			C:1	\Tools\Binn\sqlmangr.exe					on Startup		
PGPtray			<u>Ga</u> <u>C:</u>	C:1 As C:1 Microsoft SQL Server					pn Startup		
- Adobe Reader Speed Launch			h C:1						pn Startup		
Hoontrol			C:1	GUUXIC search on Google						SOFTWARE Micro	
Certificated				C. ASOFTWARE WICH							
Company : Skype Technologies SA				P 400					1020000		
Company : Skype Technologies SA Description :				C: SOFTWARE Micro							
URL : http://www.skype.com/			<u>C:</u>							SOFTWARE Micro	
SunJavaUpdateSched			<u>"C</u>						SOF	TWARE\Micr	
SynTPLpr			<u>C:1</u>	Close					SOF	TWARE\Micr	
SynTPEnh				C:\Program Files\Synaptics\SynTP\SynTPEnh.exe				HKLM\SOFTWARE\Micr			
PRONoMgr.exe				<u>C:\Program</u> <u>Files\Intel\PROSetWireless\NCS\PROSet\PRONoMgr.exe</u> HK					KLM\SOFTWARE\Micr		
lgfxTray			<u>C:\\</u>						KLM\SOFTWARE\Micr		
HotKeysCmds				C:\WINDOWS\system32\hkcmd.exe				HKLM\SOFTWARE\Micr			
		BluetoothAuthenticationAgent			prons col Bluetoothåi	thentication	Agent	HKLM\SOFTWARE\Micr			
BluetoothA	uthentica	иопмуе			APAR Software				1001	1111112 10100	



For More Info and Sample Report please visit <u>http://www.jaguarsoft.com/forensics.asp</u>



