



Forensics ToolKit



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

The screenshot displays the JaguarSoft Forensics Toolkit interface. The main window shows a 'Network Connections' table with columns for Protocol, Status, Local Port, Local Address, Remote Port, Remote Address, PID, and Process. Below this, a 'Service Manager' window is open, showing a list of services and their file paths.

Protocol	Status	Loc. Port	Local Address	Rem. Port	Remote Address	PID	Process
TCP	Listening	80	ASUSNB (0.0.0.0)	57532	-	4	System
TCP	Listening	443	ASUSNB (0.0.0.0)	2300	-	4	System
TCP	Listening	80	ASUSNB (0.0.0.0)	32839	-	4	System
TCP	Listening	52271	ASUSNB (0.0.0.0)	2	-	4	System
TCP	Established	1026	BOS (192.168.57.57)	1026	(107.46.107.68)	4	System
TCP	Listening	1046	ASUSNB (127.0.0.1)	28070	-	4	System
TCP	Listening	6657	ASUSNB (0.0.0.0)	26792	-	4	System
TCP	Listening	microsoft-4459	ASUSNB (0.0.0.0)	18956	-	4	System
TCP	Established	1078	BOS (192.168.57.57)	28672	(75.176.60.174)	4	System
TCP	Established	1026	BOS (192.168.57.57)	1026	(192.168.57.212)	4	System
TCP	Listening	1025	ASUSNB (0.0.0.0)	43207	-	4	System
TCP	Listening	sones1350	ASUSNB (0.0.0.0)	39038	-	4	System
TCP	Listening	netbios-ur139	netbios-ur(192.168.57.57)	45089	-	4	System
TCP	Listening	6657	ASUSNB (0.0.0.0)	26792	-	516	RMHSvc.exe
TCP	Listening	sones1350	ASUSNB (0.0.0.0)	39038	-	1082	pschbot.exe
TCP	Listening	1046	ASUSNB (127.0.0.1)	57532	-	1616	lsass.exe
TCP	Established	1078	BOS (192.168.57.57)	28672	(75.176.60.174)	1931	pschbot.exe
TCP	Listening	52271	ASUSNB (0.0.0.0)	2	-	3304	Skype.exe
TCP	Established	1026	BOS (192.168.57.57)	1026	(107.46.107.68)	3341	Skype.exe
UDP	0	4500	ASUSNB (0.0.0.0)	-	-	4	System
UDP	0	1069	ASUSNB (127.0.0.1)	-	-	4	System
UDP	0	1025	ASUSNB (0.0.0.0)	-	-	4	System
UDP	0	1026	ASUSNB (0.0.0.0)	-	-	4	System
UDP	0	net123	ASUSNB (127.0.0.1)	-	-	4	System
UDP	0	1048	ASUSNB (127.0.0.1)	-	-	4	System
UDP	0	1900	BOS (192.168.57.57)	-	-	4	System
UDP	0	net123	net(123)(192.168.57.57)	-	-	4	System



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

