Gargoyle Investigator™ MP



Gargoyle Investigator[™] MP is the next generation of WetStone's advanced malware discovery solutions for computer forensic investigators and incident response teams. It is designed for forensic laboratories, law enforcement, field investigators and private investigators specializing in cybercrime, and enterprise cyber security personnel.

Gargoyle Investigator MP is a multiplatform software tool used to conduct a search on a computer or drive image for known contraband and hostile

programs. Gargoyle Investigator MP searches for individual files associated with programs, so it is possible to find remnants even if a program has been deleted. Gargoyle is intended to be a quick and easy scan requiring a minimal amount of technical knowledge.

KEY FEATURES:

- Conduct scans on a stand-alone system or drive images
- Multiplatform (Windows, Windows Server, and Linux platforms)
- Identify and categorize malware and potentially unwanted applications using WetStone-supplied hash datasets.
- Scan live systems and disk and memory images using user-generated custom datasets and YARA rules
- Import hash files from third-party digital forensics toolkits, such as EnCase, FTK, Autopsy, Paraben, and Forensic Explorer
- Generate detailed evidence report in HTML, PDF, and CSV formats

elect: Drives and Directories to Scan	Scan Type Selection	
	🗵 Factory Dataset Scan	
	Supplemental Dataset Scan	View CSV
	Custom Dataset Scan	View HTML
	- YARA Scan	View PDF
Select: EnScript Result or Hash File to Scan	Allow YARA Scan of Active Processes	View LOG
	Scan Option Selection	
Select: Custom Datasets	Scan Archives	HITS
	Scan Network Files	
	💌 CSV Report	
Directories to Exclude From Scanning	IN HTML Report	SCAN
	🗵 Log Results	CLEAR
	Create Hash File	
	Debug Logging	

DATA SHEET

LICENSING:

Perpetual or subscription license for:

- ESD Electronic software download for us on a single system. Not transferable. Basic license is 2 cores. Additional core licensing available.
- FLASH 16GB USB 3.0 device for use in field investigations, and on multiple systems. Limited to 2 cores.

What is included*:

- Customer support portal account
- Access to monthly dataset updates
- Web and email support
- Software updates, as they become available
- * For one year following purchase of a perpetual license or the term of a subscription license. Additional years of maintenance may be purchased.

SYSTEM REQUIREMENTS:

In order to properly support Gargoyle Investigator, a computer system must meet or exceed the following minimum requirements:

- Microsoft Windows[®] XP, VISTA, 7, 8, 8.1, 10
- Microsoft Windows[®] Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016
- 2 GB RAM
- 1 GHz processor or better

👗 Enter Scan Details			- 0
Investigator. *	LM. Investigator		
Organization: *	WetStone Technologies		
Case ID: *	123456789-0		
Case Specifics:	Demo Scan		
	Output Passwor	d-Protected Archives	
× Write Scan Results to Default Directory	C:\Program Files (x86)\WetStone Tech	nologies\GargoyleMP\Reports	-
	Select All	Deselect All	
× Anti-Forensics	× Botnet	× Fraud Tool	× Denial of Service
× Encryption	× Exploit Scanner	× Keylogger	× Password Cracking
× Peer-to-Peer	× Piracy	× Remote Access	× Rootkit
× Scareware	× Sniffer	× Spyware	× Toolkit
× Trojan	× Web Threat	× Wireless Tool	× Ransomware
× Cryptomining	× Cryptojacking	× Exploit Kit	× OSINT
	Start Scan	Cancel	
	Status: Enteri	ng Scan Details	

Password Cracking		
Expand All Password Cracking Files	Collapse All Password Cracking Files	
John the Ripper	-	
Program	John the Ripper 📋	
Category	Password Cracking	
Original Filename	john.exe	
Detected Filename	C:\Users\wil_c\Desktop\Investigation\GMP\john.exe	
File Size	10.6 MB (10582263 Bytes)	
File Hash: (MD5)	291277D0B3E2A173823B6FB020A9B61A	
File Hash (SHA 256)	02E085A98D5342B324243B5D6790C4688CFC2CB31E0A683743F261879E314 959 [
File Mode	666 (rw-rw-rw-)	
File User ID	0	
File Group ID	0	
File Modified	Thu Dec 19 10:27:54 2019	
File Accessed	Fri Oct 21 03:46:35 2022	
File Created	Mon Dec 6 12:55:28 2021	

For more information, contact sales@wetstonetech.com

WetStone, the WetStone logo, and StegoHunt, StegoAnalyst, and StegoBreak are all registered trademarks of SquareML, Inc. a wholly-owned subsidiary of Sivisoft, Inc. Other marks and brands may be claimed as the property of others. Copyright © Sivisoft, Inc.

