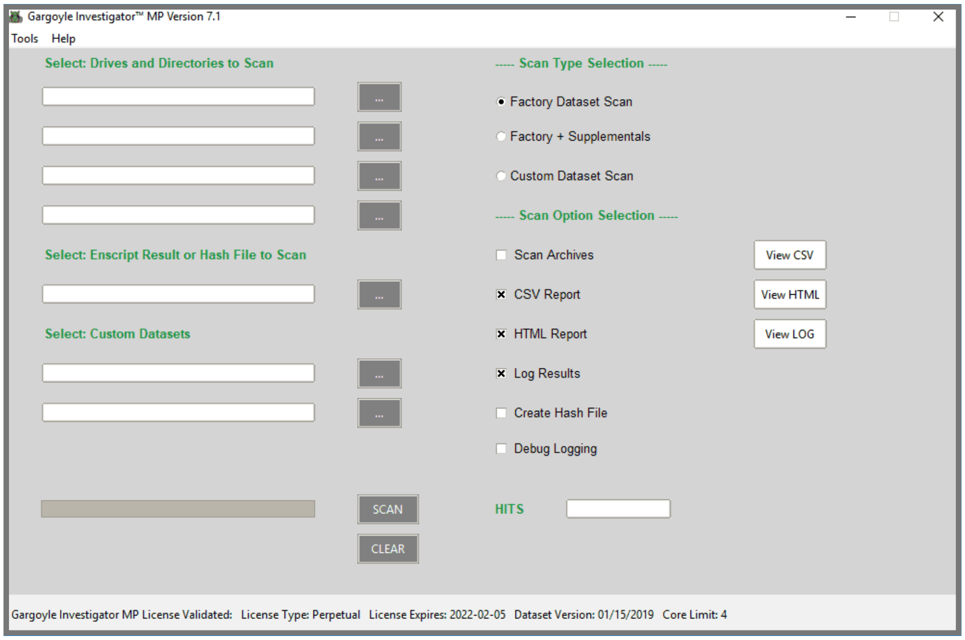
Gargoyle Investigator™ MP

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, advanced private investigators, and enterprise cyber security personnel.

Gargoyle Investigator™ MP is a multiplatform software tool that conducts a search on a computer or drive image for known contraband and hostile programs. Gargoyle 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)
- Scan factory, supplemental, and custom datasets
- Generate a hash file within EnCase using Gargoyle EnScript
- Detailed evidence report in both HTML, and CSV formats



Select: Drives and Directories to Scan

Select: Encript Result or Hash File to Scan

Select: Custom Datasets

----- Scan Type Selection -----

● Factory Dataset Scan
○ Factory + Supplementals
○ Custom Dataset Scan

----- Scan Option Selection -----

□ Scan Archives
☒ CSV Report
☒ HTML Report
☒ Log Results
□ Create Hash File
□ Debug Logging

HITS

Gargoyle Investigator MP License Validated: License Type: Perpetual   License Expires: 2022-02-05   Dataset Version: 01/15/2019   Core Limit: 4

DATA SHEET

LICENSING:

- Your choice of either:

  ESD: Electronic software download for us on a single system. Available as a perpetual or subscription license. Not transferable. Basic license is 2 cores. Additional core licensing available

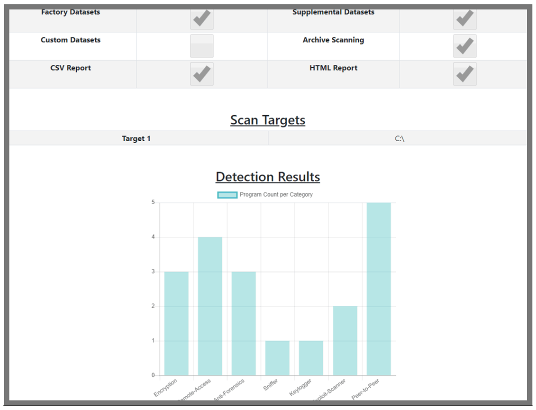
  FLASH: 16GB USB 3.0 device for use in field investigations, and on multiple systems. Limited to 2 cores

- Access to monthly Dataset updates
- Customer support portal account
- 1-Year maintenance

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
- LINUX: Ubuntu (14,16,18), Red Hat Enterprise Linux 7, Fedora 29, CentOS 7, Debian 9, Kali Linux
- 2 GB RAM
- 1 GHz processor or better

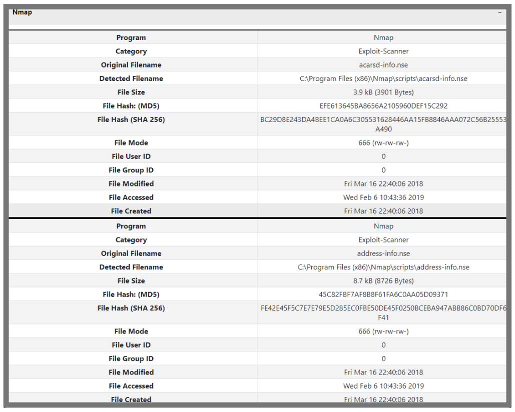


Factory Datasets	☑	Supplemental Datasets	☑
Custom Datasets	□	Archive Scanning	☑
CSV Report	☑	HTML Report	☑

Scan Targets

Target 1	C:\

Detection Results



Nmap

Program	Nmap
Category	Exploit-Scanner
Original Filename	acarsd-info.nse
Detected Filename	C:\Program Files (x86)\Nmap\scripts\acarsd-info.nse
File Size	3.9 kB (3901 Bytes)
File Hash: (MD5)	EFE613645BA8656A2105960DEF15C292
File Hash (SHA 256)	BC29D8E243DA4BEE1CA0A6C305531628446AA15FB8846AAA072C56B25553 A490
File Mode	666 (rw-rw-rw-)
File User ID	0
File Group ID	0
File Modified	Fri Mar 16 22:40:06 2018
File Accessed	Wed Feb 6 10:43:36 2019
File Created	Fri Mar 16 22:40:06 2018
Program	Nmap
Category	Exploit-Scanner
Original Filename	address-info.nse
Detected Filename	C:\Program Files (x86)\Nmap\scripts\address-info.nse
File Size	8.7 kB (8726 Bytes)
File Hash: (MD5)	45C82FBF7AF8B8F61FA6C0AA05D09371
File Hash (SHA 256)	FE42E45F5C7E7E79E5D285EC0FBE50DE45F0250BCEBA947ABB86C0BD70DF6 F41
File Mode	666 (rw-rw-rw-)
File User ID	0
File Group ID	0
File Modified	Fri Mar 16 22:40:06 2018
File Accessed	Wed Feb 6 10:43:36 2019
File Created	Fri Mar 16 22:40:06 2018

For more information, contact sales@wetstonetech.com

DATA SHEET