

# Gargoyle Investigator

## Forensic Pro Edition

### Supercharging Digital Investigation

#### Features:

- Ability to conduct scans on a stand-alone system or network resource for known contraband and hostile programs.
- 19 datasets containing thousands of types of malicious software.
- Dataset Creator™-ability to create or extend datasets.
- Interoperable with popular forensic tools such as EnCase™ and FTK™.
- 32-Bit and 64-Bit drive mounting and management integration.
- Detailed forensic evidence reports with secure source timestamping.
- Ability to scan within archive files (.zip, .rar, .jar, .bh, .arj, .lha, .lzh, .tar, .war, .enc, .bz2)
- Windows Vista Support



#### What is Gargoyle Investigator?

Gargoyle Investigator is an invaluable software tool for digital investigations. When performing incident response, digital forensic analysis, threat management, or compliance audits, Gargoyle Investigator performs a quick search for known contraband, hostile, or 'bad' programs, and provides significant clues regarding the activities, motives and the intent of suspects or potential suspects.

Gargoyle Investigator Forensic Pro is fast and easy to use, it provides investigators with valuable information regarding the contents of a suspect's computer along with essential information about it's owner's computer use. Once identified, Gargoyle also maps the detected files to the associated cyber weapons, and classifies them into a category of malware. With the ability to identify potentially hostile or suspicious programs based on the loaded dataset, the classification of those hostile programs, and the ability to view the suspect from a new aspect, while ascertaining incriminating behaviors or methods; this becomes a core tool for your investigation.

#### What is malware detection?

Gargoyle quickly and easily determines whether malware is present on a system under investigation. Malware, short for malicious software, is designed to wreak havoc, hide potentially incriminating information, and/or disrupt or damage computer systems.

Gargoyle employs custom datasets containing thousands of malware software signatures. Because the search is done for the individual files associated with a particular program, it is possible to find remnants even if the program has been deleted.

#### What can be identified?

Gargoyle provides the investigator with the ability to glean important suspect characteristics from the information revealed. The computer sophistication, covert behaviors, and paranoia levels (has the suspect tried to delete incriminating programs?) can all be derived when searching for applications with a common theme. These behaviors can assist in assessing suspect capability, activities, intent, threat or "consciousness of guilt".

#### What is a dataset?

A dataset is simply a collection of malware applications and files, organised into a relational database. The database is formatted similarly to the NSRL distributions. One dataset (database file) is created for each malware category.

Separate datasets can be created for various classifications of malware (i.e. steganography software, vulnerability assessment tools, network sniffers, port scanners, hacker tools, password cracking tools, Denial of Service tools, etc.).\* Additional datasets are released on a monthly basis.

#### What is included in the package?

Gargoyle Forensic Pro is designed for forensic investigators, examiners, law enforcement personnel, private investigators, and forensic lab use. The Forensic Pro version includes all the malware datasets, Dataset Creator, Dataset Converter, embedded into Gargoyle is drive mounting software to mount EnCase, dd, raw, ISO and safeback images, detailed forensic evidence reports with 1 year of software maintenance and dataset updates.

  
Data Duplication Ltd

4 Station Approach, Wendover, Bucks HP22 6BN  
Tel: 01296 621121 Fax: 01296 621125  
e-mail: info@dataduplication.co.uk  
www.dataduplication.co.uk

# ***Other Forensic Software Products***

## **AccessData Forensic Toolkit™ (FTK)**

### **The Ultimate Toolkit for the Forensics Specialist**

Includes Forensic Toolkit, Password Recovery Toolkit, Registry Viewer, 500 Client DNA License and the Oracle database.

## **AccessData Password Recovery Toolkit™ (PRTK)**

### **Recover Passwords Quickly & Easily**

The Password Recovery Toolkit gives you the ability to recover passwords from well-known applications and gain access to encrypted files and drives, including the encrypted file system (EFS) from Microsoft.

## **AccessData Distributed Network Attack**

### **Putting Idle Time To Work**

In the past, recoveries have been limited to the processing power of one machine. DNA uses the power of machines across the network or across the world to decrypt passwords.

## **Spector**

### **Automatically Record Everything Someone Does on Their PC**

Spector AUTOMATICALLY takes hundreds of screen snapshots every hour, very much like a surveillance camera. With Spector, you will be able to see EVERY instant message, e-mail, web-site visited and keystroke typed.

#### ***Other Products:-***

- Forensic Tools
- Hard Disk Duplicators
- Floppy Disk Copiers
- CD/DVD Duplicators
- CD/DVD Printers

---

#### ***Media Duplication Services For:-***

- Floppy Disk
- CD
- DVD
- Tape
- Blank Media Supply
- Standard or Customised Packaging
- Fulfilment Service