



Cyber criminals are becoming increasingly proficient at covering their tracks and hiding incriminating data. With over 1,000 known methods of hiding data within images, audio files, digital video, network protocols and other carriers it has never been more important to discover these methods and artifacts.

StegoHunt™ Flash (StegoFlash) allows investigators, auditors, incident responders, breach and data leak prevention teams to quickly identify if steganography is present in active cases or work environment.

Features:

- Quickly identify if steganography is present by scanning for over 1,000 data hiding applications using Fibonacci search methods
- Identify suspect carrier files that otherwise go undetected (program artifacts, program signatures, statistical anomalies)
- Generate case reports for management or court presentations
- Operational discovery modes (directory, drive, archive, drive image, network path)

What's Included:

- A 2GB encrypted USB device equipped with 256-bit AES encryption
- Multiple system and mobile scanning
- 24/7 access to our customer support portal
- One year of maintenance and monthly malware dataset updates

System Requirements:

- Microsoft Window® 2000-Windows® 8, Window® 2003 Server and Windows® 2008 Server
- 1GB RAM
- Pentium® 1 GHz processor or better
- Available USB port

NOTE: StegoFlash includes StegoAnalyst™ and StegoBreak™ as an Electronic Software Delivery.



StegoHunt™ Flash
(StegoFlash)

To purchase or inquire further, contact sales@wetstonetech.com.