

隐写分析软件StegoHunt™ Suite



借助这整套技术，调查人员，事件响应者，数据泄露和数据泄漏预防团队以及审计师可以快速确定活动案例或工作环境中是否存在隐写术。

套件包含: StegoHunt™ , StegoAnalyst™ , StegoBreak™

STEGOHUNT 主要特点:

- 通过使用Fibonacci搜索方法扫描超过1,000个数据隐藏应用程序，可以快速确定调查中是否存在隐写术。
- 确定不易被检测到的可疑载体文件，包括程序工件，程序签名和统计异常。
- 利用多种操作发现模式，包括目录，驱动器，存档，驱动器映像和网络路径。
- 生成特定案例的报告以进行管理或法庭陈述。

STEGOANALYST 主要特点:

- 对检测到的图像和音频文件进行深入分析。
- 利用文件查看面板显示单个文件属性，包括图像详细信息，DCT系数和颜色对。这允许对识别出的载体进行完整的分析。
- 从各种过滤器选项中选择以进行进一步分析，例如最低有效位（LSB）的特定颜色。

STEGOBREAK 主要特点:

- 使用简单的点击界面即可破解并从许多运载文件中提取有效载荷。
- 利用随附的常用密码词典来执行字典攻击。
- 轻松引入其他词典，并创建自己的词典来扩展词典攻击。

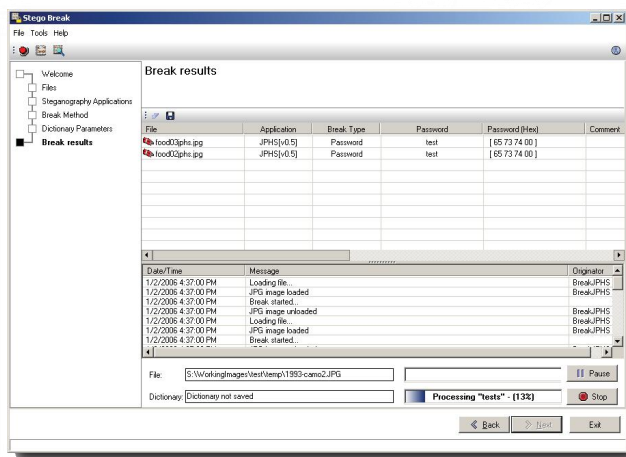
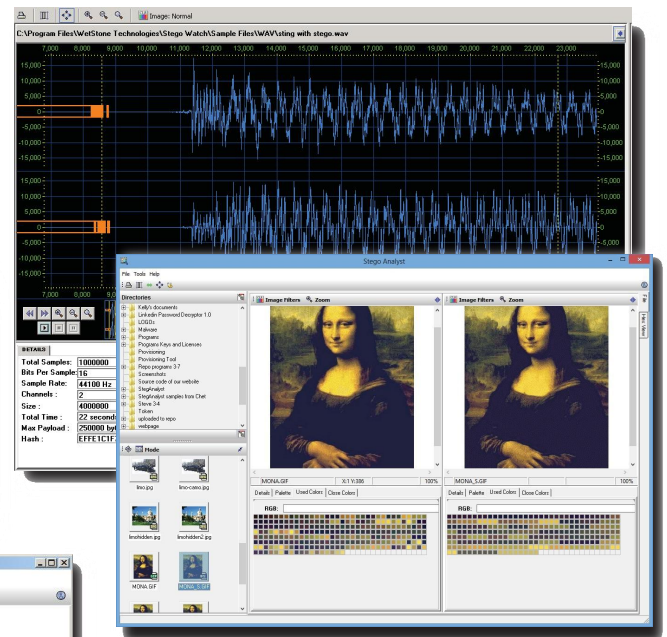
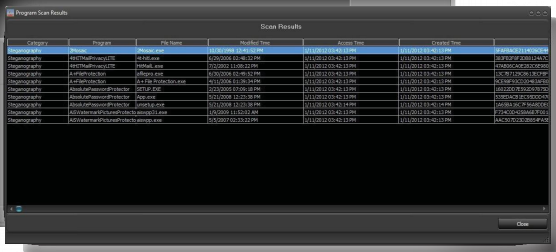
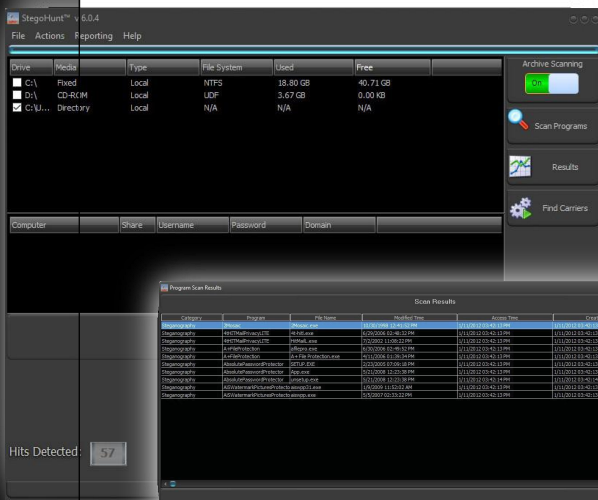
包括什么?

- 电子版软件下载
- 访问每月的数据集更新
- 建立客户支持账户
- 1年免费软件升级

系统要求:

为了正确地支持StegoHunt, 计算机系统必须满足或超过以下最低要求:

- Microsoft Windows® 2000, XP, VISTA, 7, 8, 8.1, 10
- Microsoft Windows® Server 2003, 2008, 2012, 2016
- 1 GB RAM
- 1 GHz 或更高的处理器



DATA SHEET

更多相关信息, 请联系 sales@wetstonetech.com

WetStone, WetStone logo, StegoHunt, StegAnalyst 和 StegoBreak 由 WetStone Technologies, Inc. 公司商标注册。是 Allen Corporation of America, Inc. 全资子公司。Copyright © Allen Corporation of America, 2017

