用户手册

弘连火眼仿真取证软件 GE104

上海弘连网络科技有限公司

目 录

1 产品简介

1.1 产品概述

弘连火眼仿真取证软件（BootMagix）是专为硬盘/镜像仿真设计的一款产品，可以将硬盘/硬盘镜像等生成为可启动的仿真系统。该软件产品帮助取证调查人员以交互的方式和用户视角检查操作目标系统，收集相关证据。

1.2 产品特性

- 通过虚拟机技术，无痕启动 Windows、MacOS、Linux 等多种操作系统硬盘和镜像文件；
- 使用只读接口连接，取证过程中不改变物理磁盘与镜像文件状态；
- 可附加多个磁盘，支持多硬盘系统的仿真运行；
- 自动识别设备中的操作系统类型；
- 支持清除/绕过 Windows 登录密码；
- 支持 32 位、64 位的操作系统仿真。

1.3 运行环境

- 操作系统为 Windows7 x64 位以及更高版本；
- 计算机推荐 8G 内存以上，最低配置 4G 内存；
- 操作系统中安装 VMware 虚拟机软件，推荐安装 12 及以

上版本。

2 软件安装、更新、卸载

2.1 安装

步骤 1 双击 BootMagix 安装包。如果开启了 UAC 账户控制，请在弹出的对话框中点击“是”以继续,见图 2.1.1。

图 2.1.1 火眼仿真安装包

步骤 2 启动安装包后进入安装界面，见图 2.1.2。

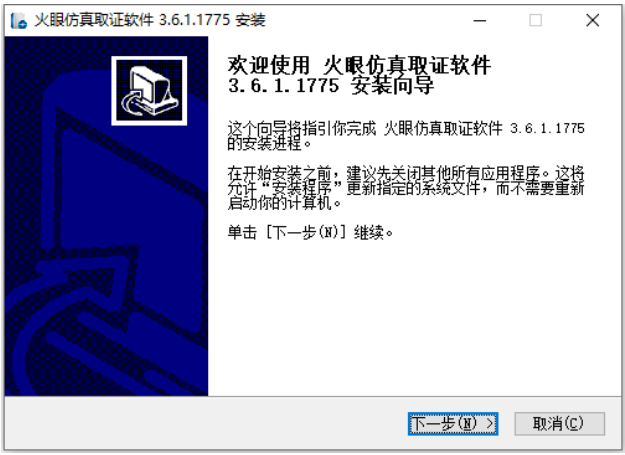

图 2.1.2 安装向导程序欢迎界面

步骤 3 单击【下一步】选择程序安装位置，见图 2.1.3。

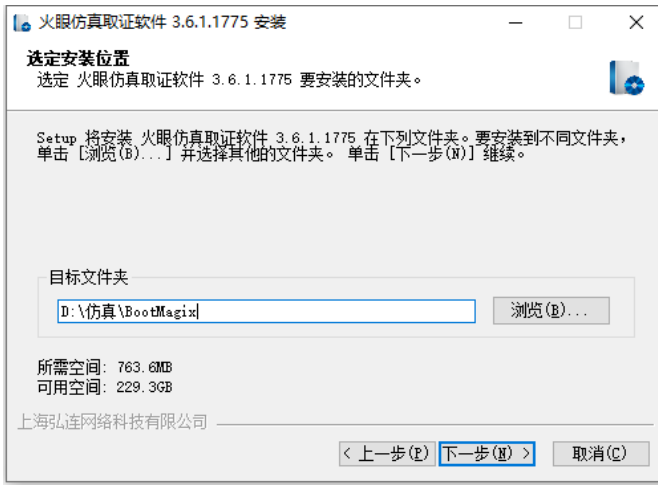

图 2.1.3　选择安装的目标文件夹

步骤 4 单击【下一步】设置“开始菜单”文件夹，见图 2.1.4。

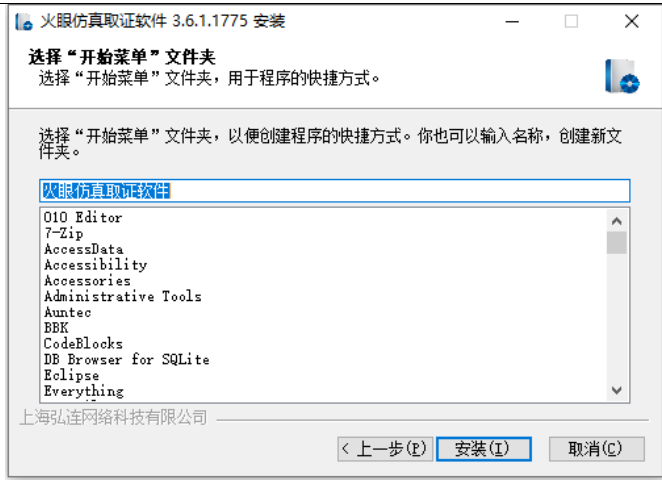

图 2.1.4　选择“开始菜单”文件夹

步骤 5 单击【安装】开始安装，见图 2.1.5。

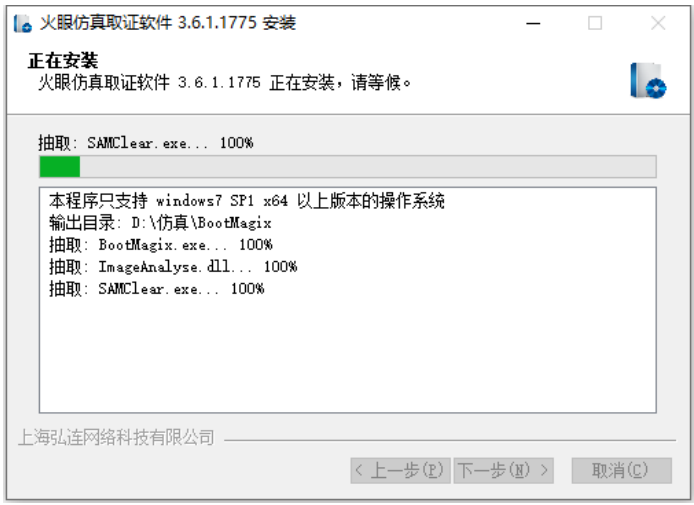

图 2.1.5　正在安装

步骤 6 单击【完成】，完成安装，见图 2.1.6。

图 2.1.6 完成安装

2.2 更新

点击标题栏中的【菜单键】打开菜单，点击【检查更新】按钮，程序会启动软件更新功能。

2.3 卸载

步骤 1 右键桌面仿真程序图标并点击打开文件所在位置，双击 uninst.exe 文件，见图 2.3.1。

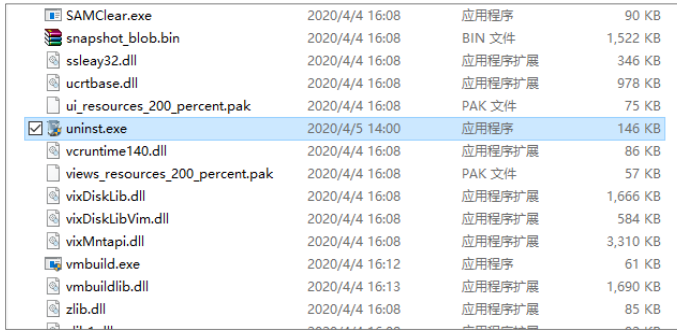

图 2.3.1 BootMagix 卸载文件

步骤 2 确认是否卸载火眼仿真证据分析软件，见图 2.3.2。

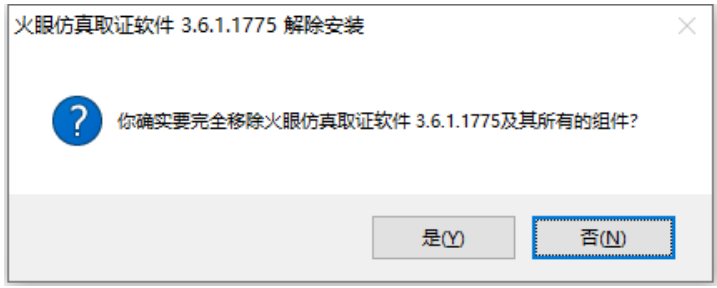

图 2.3.2 确认是否卸载

步骤 3 开始卸载火眼仿真证据分析软件的过程，见图 2.3.3。

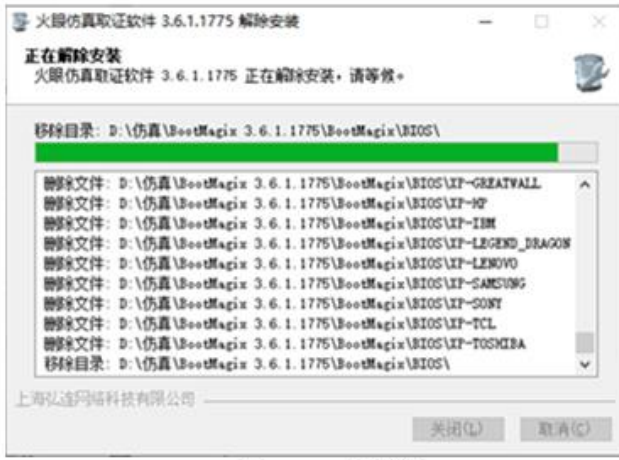

图 2.3.3 卸载过程

步骤 4 完成卸载火眼仿真证据分析软件，见图 2.3.4。

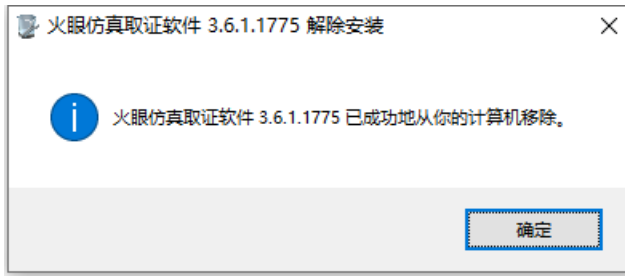

图 2.3.4 卸载成功

3 应用实例

3.1 创建虚拟机

（1）点击功能区域右侧的绿色按钮创建虚拟机，进入虚拟机配置界面。

图 3.1　点击创建虚拟机

（2）虚拟机配置界面主要由选择磁盘或者镜像、操作系统、虚拟机、共享目录、生成位置等输入框和按钮组成。

磁盘或镜像：点击磁盘配置按钮，进入磁盘配置菜单，可以选择已经检测到的磁盘或者从资源管理器中添加磁盘镜像，点击确定按钮，添加成功。

操作系统：添加磁盘或镜像后，软件会自动进行操作系统的识别，如果没有能够正确识别操作系统，点击右侧的自定义

按钮，可以手动修改操作系统。

虚拟机：添加正确的磁盘或镜像后会自动生成对应文件名的虚拟机名称，点击输入框可以重新进行修改，默认设置的内存大小为 4096MB，点击可以手动输入。

高级设置：点击高级设置按钮，可以对虚拟机进行特定的设置，主要包括了主板品牌及系统设置，启动参数（处理 7B 蓝屏、处理 21A 蓝屏、清除登录密码、绕过登录密码、禁用网卡）等。

共享目录：点击共享目录输入框旁的【…】按钮，打开资源管理器，选择需要共享的目录路径，点击打开目录，可以快速访问到已经选择的路径进行查看。

生成位置：点击生成位置输入框旁的【…】按钮，打开资源管理器，选择需要生成的虚拟机保存路径，点击打开目录，可以快速访问到已经选择的路径进行查看。

图 3.2　虚拟机配置界面

图 3.3　磁盘或镜像配置

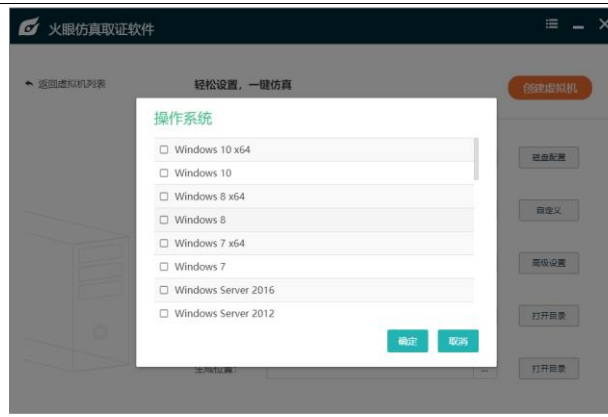

图3.4 操作系统自定义

图 3.5　虚拟机高级设置

（3）选择输入所有虚拟机配置后，点击功能区域右上方的橙色创建虚拟机按钮，进行虚拟机创建，状态栏上方会出现创建任务进度条。

图 3.6　创建虚拟机

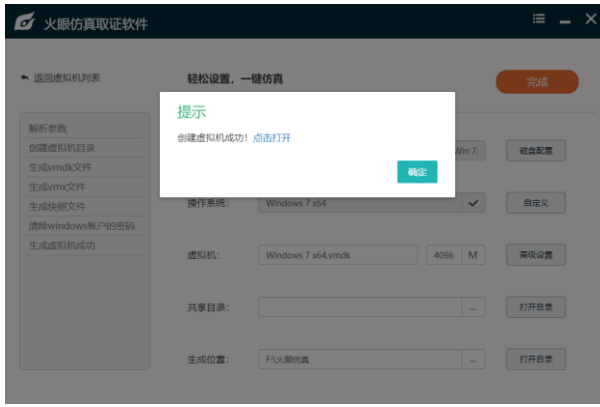

图 3.7　创建完成提示

（4）点击蓝色的点击打开文字按钮，可以自动打开 VMware 程序，启动虚拟机仿真。

4 常见问题

清除登录密码与绕过登录密码功能，需要 VMware 虚拟机映射虚拟磁盘功能正常可用。

检查方法：打开本地 VMware 虚拟机软件，点击文件——映射虚拟磁盘。若无出现报错则该功能正常。若遇到报错请修复 VMware 软件。