“SafeImager Win”v5.0需求规格说明书

|  |  |  |
| --- | --- | --- |
| 文件状态：  [√] 草稿  [ ] 正式发布  [ ] 正在修改 | 文件标识： |  |
| 当前版本： | V1.1 |
| 作 者： | 王圣东 |
| 完成日期： | 2018-10-30 |

**盘石软件（上海）有限公司 产品中心**

**2018年9月6日**

**文档修订记录**

| **版本** | **作者** | **日期** | **备注** | **审核** |
| --- | --- | --- | --- | --- |
| V1.0 | 王圣东 | 2018-09-05 | 新建 |  |
| V1.1 | 王圣东 | 2018-10-30 | 修订流程 |  |
|  |  |  |  |  |

目录

[“SafeImager Win”v5.0需求规格说明书 1](#_Toc528657264)

[文档修订记录 2](#_Toc528657265)

[目录 3](#_Toc528657266)

[1 引言 6](#_Toc528657267)

[1.1 编写目的 6](#_Toc528657268)

[1.2 读者对象 6](#_Toc528657269)

[1.3 背景 6](#_Toc528657270)

[1.4 参考文档 6](#_Toc528657271)

[1.5 术语与定义 6](#_Toc528657272)

[2 需求概述 7](#_Toc528657273)

[2.1 产品目标 7](#_Toc528657274)

[2.2 产品功能 7](#_Toc528657275)

[2.3 用户特点 7](#_Toc528657276)

[2.4 一般约束 7](#_Toc528657277)

[2.5 相关假设、限制、依赖条件 8](#_Toc528657278)

[3 标准和规范 9](#_Toc528657279)

[3.1.1 引用的标准和规范 9](#_Toc528657280)

[3.1.2 拟制定的标准和规范 9](#_Toc528657281)

[4 功能性需求规格 10](#_Toc528657282)

[4.1 取证方式 10](#_Toc528657283)

[4.1.1 离线取证 10](#_Toc528657284)

[4.1.2 在线取证 10](#_Toc528657285)

[4.1.3 支持取证的设备 10](#_Toc528657286)

[4.2 取证流程 10](#_Toc528657287)

[4.3 启动程序 11](#_Toc528657288)

[4.4 数据复制 11](#_Toc528657289)

[4.5 文件提取 13](#_Toc528657290)

[4.6 数据分析 14](#_Toc528657291)

[4.7 任务列表 16](#_Toc528657292)

[4.8 历史取证 17](#_Toc528657293)

[4.9 帮助中心 17](#_Toc528657294)

[4.10 辅助功能 18](#_Toc528657295)

[4.11 报告 18](#_Toc528657296)

[4.12 ★重要描述 18](#_Toc528657297)

[5 非功能性需求规格 19](#_Toc528657298)

[5.1 界面设计 19](#_Toc528657299)

[5.1.1 界面结构说明 19](#_Toc528657300)

[5.1.2 配色说明 19](#_Toc528657301)

[5.2 报告样式 19](#_Toc528657302)

[5.3 运行环境 19](#_Toc528657303)

[5.3.1 设备 20](#_Toc528657304)

[5.3.2 支持的软件 20](#_Toc528657305)

[5.3.3 接口 20](#_Toc528657306)

[5.4 性能 20](#_Toc528657307)

[5.5 安全性 20](#_Toc528657308)

[6 外部接口 21](#_Toc528657309)

[7 业务规则与算法说明 22](#_Toc528657310)

[8 附录 23](#_Toc528657311)

# 引言

## 编写目的

本文是 “SafeImager Win”v5.0产品开发的指导性文件，明确“SafeImager Win”v5.0产品功能需求规格说明文档。将对产品的功能特点，界面原型进行描述，并在可能的情况下尽量给出量化的参数。

## 读者对象

本文档的预期读者为项目经理、设计人员、系统架构师、软件开发人员、软件测试人员、项目评审人员和用户。

## 背景

本文将描述“SafeImager Win”v5.0产品的所有需求以及原型界面。

## 参考文档

SafeImager v4.0软件

## 术语与定义

|  |  |
| --- | --- |
| **术语、定义** | **解 释** |
|  |  |
|  |  |
|  |  |

# 需求概述

## 产品目标

完成对SafeImager v4.0版本的升级，解决软件稳定性，适配更多硬件机型，优化文件快速提取功能和必要数据现场解析能力。全新的盘石风格界面，打通盘石软件取证产品的数据对接，赢得客户信心。

## 产品功能



## 用户特点

“SafeImager Win”v5.0的用户主要是电子数据调查和鉴定人员，主要涉及的行业包括公安执法部门的技侦、网安、刑侦、经侦、反恐、检务技术，党政机关的纪委、监委，行政执法部门的市场、税务、海关、烟草等。

## 一般约束

本产品开发周期为1.5个月。

## 相关假设、限制、依赖条件

产品成功的关键依赖：

1. 数据解析功能中的密钥获取（三方工具）技术。

产品的应用场景依赖：

特别注意，对于复制模块设计的4个取证基础功能之间的逻辑关系定义：

（1）硬盘克隆任务进行时，选择的目标介质不允许再次使用。

（2）硬盘镜像任务进行时，选择的目标介质不允许再当作克隆任务的目标介质，仍可以当作镜像的目标介质。

（3）硬盘克隆和镜像任务执行时，不允许执行擦除任务，不在执行任务时，可以执行擦除任务。

（4）任务的默认保存路径空间不足时，提示用户重新选择新的目标介质。

（5）硬盘擦除任务执行时，选择的目标介质不允许再次使用，直到擦除任务完成或停止后才可以使用。

# 标准和规范

### 引用的标准和规范

遵照盘石软件开发中的规范和标准文件。

### 拟制定的标准和规范

无。本项目不涉及标准和规范的制定。

# 功能性需求规格

首先，利用思维导图展现产品整体功能。



## 取证方式

### 离线取证

离线取证通过离线启动程序的方式取证，离线启动要求支持光盘启动和U盘启动两种方式。

### 在线取证

在线取证要求程序能够在Microsoft Windows XP及以上的全系系统上运行取证程序，实现在线取证功能。在线取证应支持一般取证和密取两种方式取证。

### 支持取证的设备

平板、笔记本、台式机。

## 取证流程

取证流程描述从程序启动到取证结束的概要过程。便于开发项目相关人员理解。



限制条件，取证前必须新建取证，录入取证检材信息。

## 启动程序

启动程序后，默认出现检材信息录入对话框。



检材编号必须录入，如此处关闭“检材信息”录入对话框，可以浏览软件全部界面，不能进行取证操作，如果执行取证操作，弹出“检材信息”对话框，让调查者填写必要信息。

## 数据复制

数据复制模块包含了磁盘镜像、分区镜像、内存镜像（在线取证功能）、磁盘克隆、磁盘擦除5个功能。

其中磁盘镜像、分区镜像、内存镜像功能原型设计如下。



磁盘克隆功能原型设计如下。

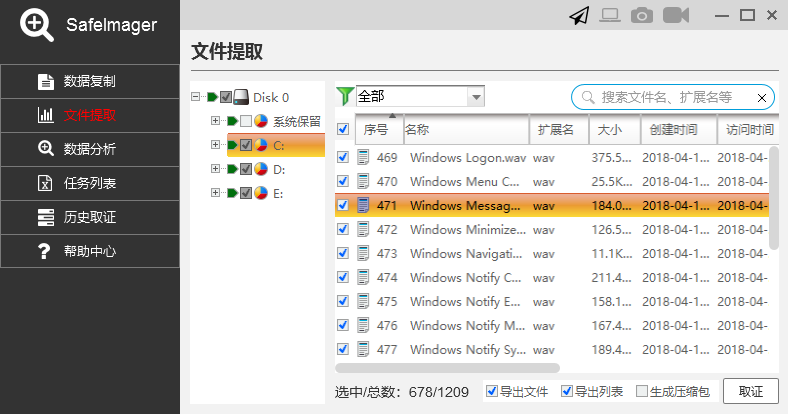


磁盘擦除功能原型设计如下。

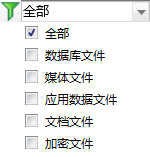


## 文件提取

文件提取模块通过离线文件系统解析，然后对选择文件进行提取的功能模块。原型设计如下。



过滤功能默认项目包含全部、数据库文件、媒体文件、应用程序数据文件、文档文件、加密文件，通过下拉菜单方式供调查者选择，如下图。



过滤功能选项可以通过维护工具（或者直接编辑）维护，过滤文件类型依照扩展名过滤，每种类型的扩展名可通过维护工具编辑。

搜索功能是对过滤结果的二次搜索。

## 数据分析

数据分析功能指对取证检材的重要信息直接分析的功能。原型设计如下。



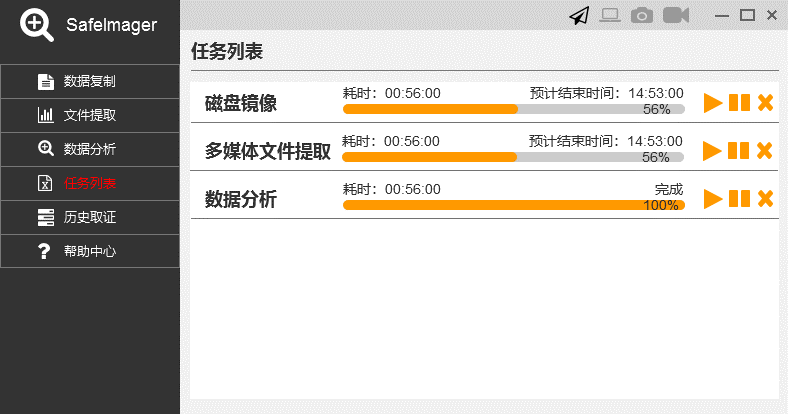
数据分析的项目和内容通过一颗树全部展现，具体提取哪些内容，调查者可以通过目录前的复选框进行选择。

数据分析应包含以下列表中的项目。

| **序号** | **一级** | **二级** | **三级** | **备注** |
| --- | --- | --- | --- | --- |
|  | 存储介质信息 | 磁盘信息 |  |  |
|  |  | 分区信息 |  |  |
|  | 操作系统#1 | 操作系统信息 |  |  |
|  |  | 系统程序 |  |  |
|  |  | 应用软件 |  |  |
|  |  | 账号密码 | 系统用户密码 |  |
|  |  |  | 浏览器密码 |  |
|  |  |  | 邮件密码 |  |
|  |  |  | 密码输入框密码 |  |
|  |  |  | 即时通讯密码 |  |
|  |  |  | Outlook个人文件夹密码 |  |
|  |  |  | VNC密码 |  |
|  |  |  | 无线密码 |  |
|  |  |  | 拨号/VPN密码 |  |
|  |  | 用户记录 | 活动登录会话 |  |
|  |  |  | 当前登录用户 |  |
|  |  |  | 进程信息 |  |
|  |  |  | 进程依赖模块 |  |
|  |  |  | 服务信息 |  |
|  |  |  | 打开文件进程句柄 |  |
|  |  |  | 剪贴板信息 |  |
|  |  |  | 计划任务信息 |  |
|  |  |  | SAM哈希 |  |
|  |  |  | 自启动项与程序 |  |
|  |  |  | 访问过的快捷方式 |  |
|  |  |  | 运行过的程序列表 |  |
|  |  |  | 用户登录记录 |  |
|  |  |  | 账户密码策略和域信息 |  |
|  |  |  | %windir%tasks里的内容 |  |
|  |  |  | 最近打开的文件列表 |  |
|  |  | 网络活动 | 网络连接列表 |  |
|  |  |  | TCP/IP端口信息 |  |
|  |  |  | 网络接口信息 |  |
|  |  |  | 混杂模式端口 |  |
|  |  |  | 路由信息 |  |
|  |  |  | 网络文件信息 |  |
|  |  |  | 网络协议统计 |  |
|  |  |  | 共享资源信息 |  |
|  |  |  | ARP信息 |  |
|  |  |  | 网络会话信息 |  |
|  |  |  | NETBIOS统计信息 |  |
|  |  |  | 网络活动连接 |  |

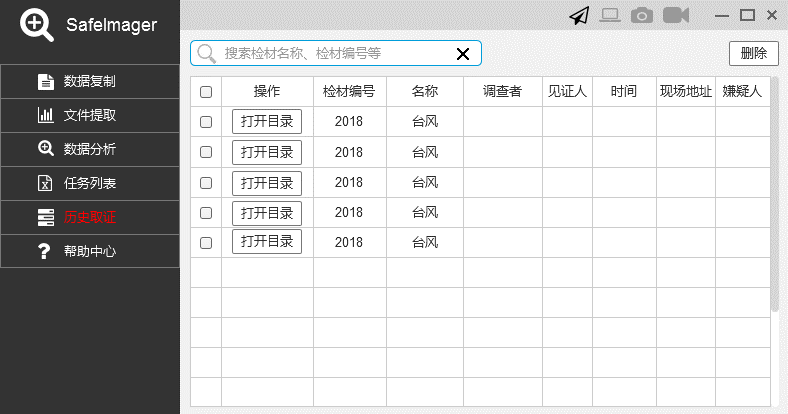
## 任务列表

记录当前取证任务的进展情况，原型设计如下。



## 历史取证

检材列表展现调查者创建的取证检材信息记录。



检材列表应包含检材编号、名称、调查者、见证者、时间、地址、嫌疑人、检材描述信息。对检材列表中的检材记录可做编辑、生成报告、删除操作。

支持对检材列表中的记录进行搜索操作。

## 帮助中心

帮助中心作为用产品信息展示，用户帮助说明等，原型设计如下。



## 辅助功能

辅助功能指取证过程中的必要记录操作，比如截图、录像、可行命令行。功能按钮维语标题栏中。



辅助功能按钮依次是【新建取证】、【可行命令行】、【截图】、【录像】。

## 报告

参照SafeImager v4.0报告样式开发。

## ★重要描述

“SafeImager Win”v5.0在SafeImager v4.0功能基础上进行优化设计而来，本文档中对功能细节描述不到位的地方，参照SafeImager v4.0功能执行。

# 非功能性需求规格

## 界面设计

运行程序界面结构和配色要求拥有盘石软件元素。

### 界面结构说明

界面整体结构如下。



### 配色说明

采用向风系列设计系列配色。

## 报告样式

## 运行环境

在线支持Windows xp及以上全系列系统，离线运行环境为乌班图系统。

### 设备

程序载体为具备启动能力的定制U盘。

### 支持的软件

无。

### 接口

无。

## 性能

复制速度

镜像速度

擦除速度

数据解析速度

文件提取速度

## 安全性

使用软狗授权，防止产品被克隆（复制）销售。

# 外部接口

略。

# 业务规则与算法说明

略。

# 附录

“SafeImager Win”v5.0原型图。