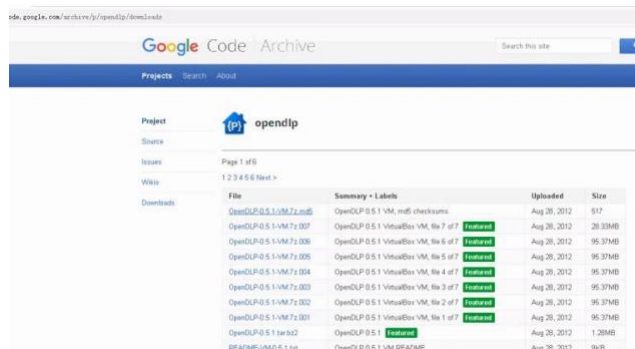


## 11 DLP

### 0x01 实验环境

数据防泄漏 DLP(Data Loss Prevention)就是该款工具的主要目的。该攻击可以全面扫描数据，无论数据是存在数据库中还是存放在文件系统里。Open DLP 会搜索与公司相关的敏感数据以发现数据的未授权复制和传输。这对防御恶意内部人或粗心大意的员工往外部发送数据很有用。该工具在 Windows 系统上运行良好，也支持 Linux,且可通过代理部署，或作为无代理工具使用。

下载地址：<https://github.com/ezarko/opendlp> 可以直接百度网盘下载：但这个环境搭建麻烦，现在主要靠 google 在维护，界面不好看。



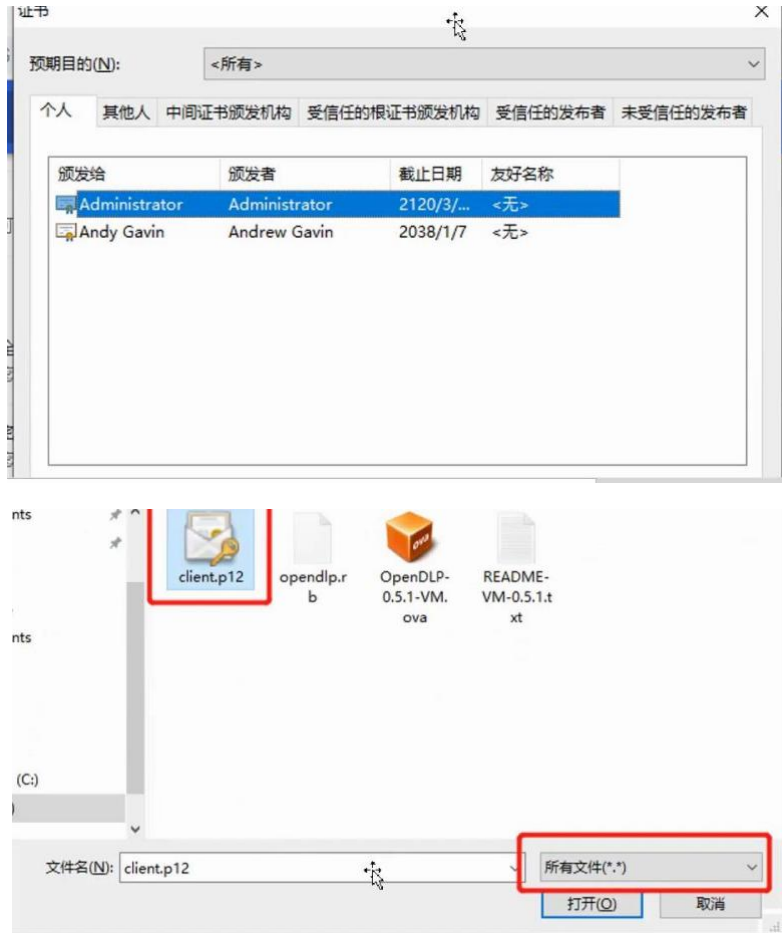
### 0x02 原理介绍

一个免费的，开源的，基于代理和无代理的，集中管理，可大规模分发的数据丢失防护工具。

### 0x03 实践操作

需要安装证书





登录

<https://192.168.2.113/OpenDLP/index.html>  
 username:dlpuser  
 password:QpenDLP

## 12 终端管理

这个东西更简单，统一的集中管理平台，管理终端，但这是个人谁都不愿意装，但领导特别喜欢的软件。。。。。

### 0x01 功能



功能详解			
<h4>文档操作管控</h4> <p>完整审计内部网络中的文档使用与传播全过程，发现违规使用行为，防止文档非法篡改或泄露</p> <ul style="list-style-type: none"> <li>记录创建/修改/复制/删除等多种操作</li> <li>控制文档读/写权限</li> <li>非法操作前备份</li> </ul>	<h4>设备管控</h4> <p>控制几乎所有计算机外部设备的使用，降低外设泄密风险，限制利用外设进行娱乐等无关应用</p> <ul style="list-style-type: none"> <li>支持大多数常见外设</li> <li>支持禁用一切新设备</li> <li>支持分时段弹性管理</li> </ul>	<h4>即时通讯管控</h4> <p>完整地审计QQ、MSN、阿里旺旺等即时通讯工具的聊天记录，防止重要文件经由即时通讯工具泄露</p> <ul style="list-style-type: none"> <li>支持几乎所有即时通讯软件</li> <li>控制在聊天中传递文件</li> <li>支持SKYPE等加密传输的记录</li> <li>支持群消息记录</li> </ul>	<h4>文档打印管控</h4> <p>有效审计每一次打印操作，灵活的控制打印权限，防止低质渠道的信息外泄与打印浪费</p> <ul style="list-style-type: none"> <li>映像格式记录打印内容</li> <li>记录OA、ERP等无文档打印</li> <li>支持虚拟/网络/共享/本地等多种打印机</li> </ul>

<p><b>邮件管控</b></p> <p>帮助记录和审计用户收发电子邮件，发现违规行为，同时控制电子邮件收发，防止重要信息泄露</p> <ul style="list-style-type: none"> <li>支持标准协议、Exchange、lotus、网页邮件</li> <li>完整记录附件</li> <li>控制邮件附件发送</li> <li>收件人/发件人黑白名单</li> </ul>	<p><b>移动存储管控</b></p> <p>分类规范移动存储设备的使用，应用权限控制与移动盘加密实现“内盘内用，外盘外用”，防范移动存储泄密</p> <ul style="list-style-type: none"> <li>控件读/写权限</li> <li>加密盘制作</li> <li>写/读文档时自动加/解密</li> <li>支持分类管理</li> </ul>	<p><b>网页浏览管控</b></p> <p>完整记录用户的网页浏览，限制与工作无关或有风险的网页访问，降低安全风险，提升工作效率</p> <ul style="list-style-type: none"> <li>支持几乎所有主流浏览器</li> <li>支持分时段弹性管理</li> <li>支持分类管理</li> </ul>	<p><b>应用程序管控</b></p> <p>帮助管理者清楚了解用户使用了哪些应用程序，直观多样的报表辅助制定黑白名单，防范风险提升工具效率</p> <ul style="list-style-type: none"> <li>支持分类管理</li> <li>支持分时段弹性管理</li> <li>查询统计方便</li> </ul>
--	---	---	---

<p><b>网络控制</b></p> <p>控制内网计算机之间以及内网与外网的通讯权限，阻止内部计算机的非法外联，检测并阻止来自外部的网络入侵，保护关键网络位置的通讯安全</p> <ul style="list-style-type: none"> <li>根据IP/端口/方向限制流量</li> <li>支持分时段弹性管理</li> </ul>	<p><b>风险审计报告</b></p> <p>通过日志记录发现安全隐患，了解企业运维，针对风险预警，趋势分析，实现内网动态全掌握</p> <ul style="list-style-type: none"> <li>统计表，有效统计用户行为</li> <li>趋势表，直观展现行为变化</li> <li>征兆表，及时预警潜在风险</li> <li>支持个性化的私人订制报表</li> <li>支持自动生成周期报表，并且提供邮件自动订阅功能</li> </ul>	<p><b>文档云备份</b></p> <p>帮助企业管理者对终端计算机上的文件进行集中存储和管理，解决企业文档管理难、容易损坏、丢失以及感染病毒被勒索的难题</p> <ul style="list-style-type: none"> <li>自动备份，统一管理</li> <li>恢复损毁、丢失文档</li> <li>快速检索，备份文档</li> <li>分级管理，防止泄密</li> </ul>	<p><b>基本功能</b></p> <p>提供集中的内网管理平台架构，简化大量重复性的基础管理工作，帮助总揽内网全局</p> <ul style="list-style-type: none"> <li>内网计算机基本信息与策略配置综览</li> <li>IP/MAC绑定</li> <li>触发策略报警/警告</li> </ul>
---	---	--	---

## 0x02 厂商

360、奇安信、腾讯、北信源等。。。

## 0x03 奇安信天擎试验

天擎 6.0 下载地址:

[http://down.360safe.com/skylar6/360skylarsetup\\_f7f974da5bf38c6b24988c0f7e2f11c0\\_6.0.0.3100.exe](http://down.360safe.com/skylar6/360skylarsetup_f7f974da5bf38c6b24988c0f7e2f11c0_6.0.0.3100.exe)

或者提供的云盘

下载的为试用版，30 天试用

360新天擎

127.0.0.1:8080

SQL+ XSS+ Encryption+ Encoding+ Other+

Load URL  
Split URL  
Execute

Enable Post data Enable Referrer

### 安全概况

您尚未上最新扫描结果，建议立即扫描

最新扫描：自 在线率：%

### 待处理任务：

全网电子安全状态：暂无待处理

### 安全动态

时间	来源名	事件
暂无安全动态		

### 授权提醒

您的授权即将到期，请及时联系我们更新授权：4008-136-360

#### windows终端

- 补丁管理模块还有30天过期
- 防病毒模块还有30天过期
- 健康评估模块还有30天过期
- 软件分发模块还有30天过期
- 移动存储管理模块还有30天过期
- 运维管控模块还有30天过期
- 资产管理模块还有30天过期
- 补丁管理更新服务模块还有30天过期
- 病毒查杀更新服务模块还有30天过期
- XP维护模块还有30天过期

#### windows服务器

国产系统

Linux服务器

下次不再弹出

确定