

在之前的我们曾推荐过一些值得收藏的Powershell工具，想了想决定做一个工具推荐系列，嗯，其实算是个出装指南——



本文旨在分享部分取证工具，仅供安全学习，禁止非法利用。

1、[ChromeForensics](#)



谷歌浏览器及其他变种浏览器的一个自动取证分析工具。

2、[android-forensics](#)

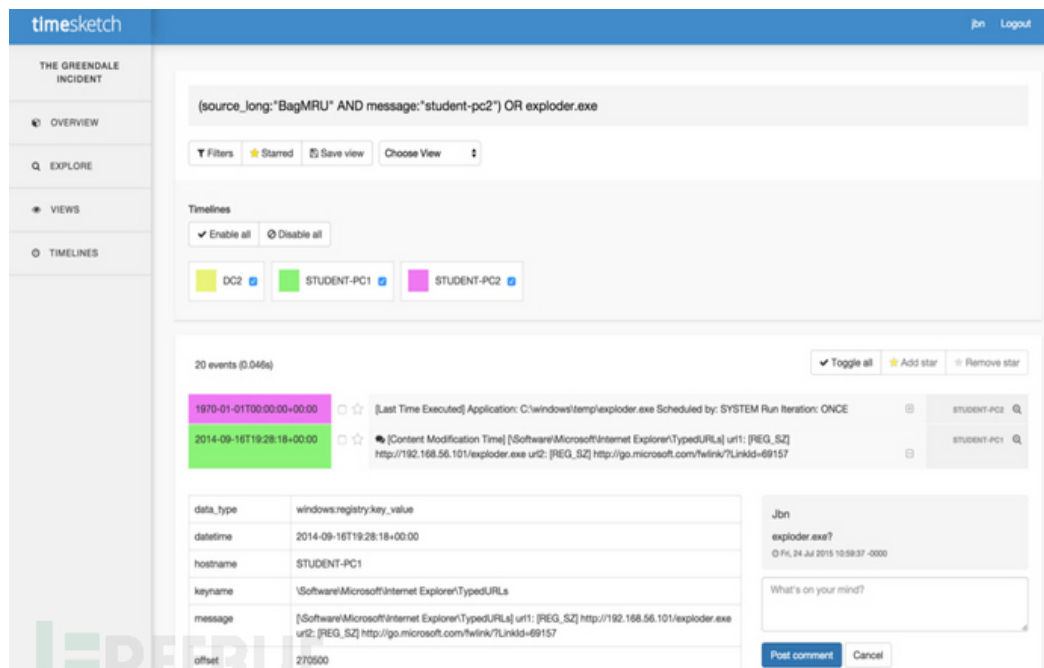




Android Forensics: Exploring Android Internals and Android Apps

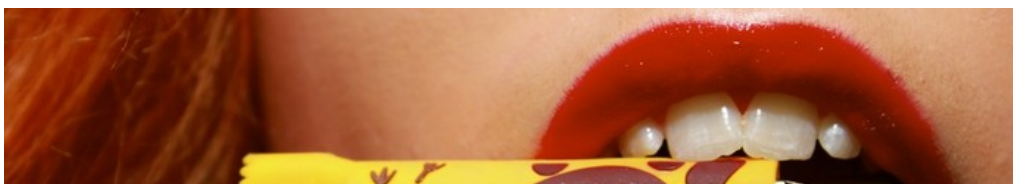
开源的安卓取证App和框架，它可以对安卓设备的 通话记录、联系电话、彩信、MMSParts、以及短信进行提取。

3、Timesketch



Timesketch是一款实验性的依据时间轴进行协同取证分析的POC开源工具,使用sketchs你和你的同伴可以很容易的组织时间轴并同时进行分析。

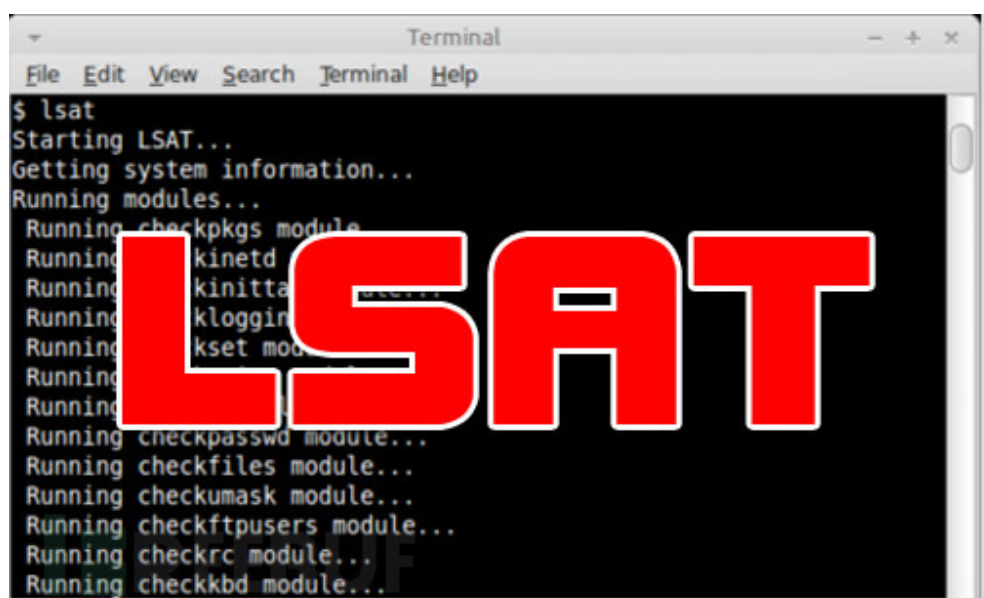
4、USBTracker





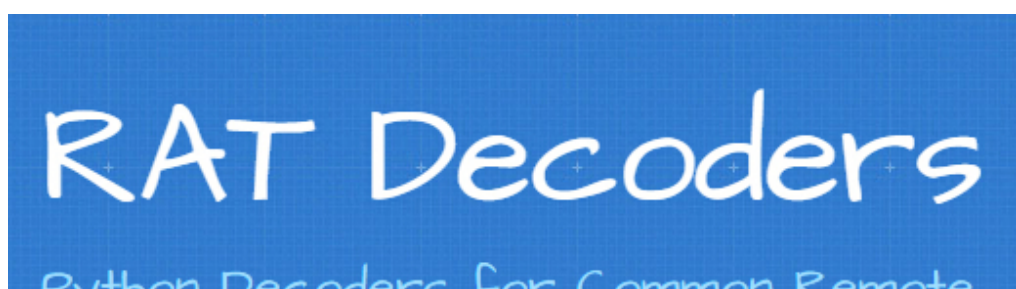
USBTracker可以对quick & dirty 代码进行应急响应并通过取证Python从windows系统去转储USB相关的信息等。

[5、Linux Security Auditing Tool \(LSAT\)](#)



Linux Security Auditing Tool (LSAT)是一个安装后安全审计工具，它采用了模块化设计使得新功能可以快速添加。它可以检查 inetd条目并扫描不需要的RPM包。

[6、RAT Decoders](#)





通过python脚本来获取木马中的配置文件，诸如ftp、ssh等信息，反向对黑客进行攻击。目前支持Adwind、Adzok、Albertino Advanced RAT等40多个木马。

7、Bro



Bro是一个与你所知道的典型IDS完全不同的强有力的网络分析框架，具有适应性强、高效、灵活、开放接口、开源等优点。

8、Xplico

A screenshot of the Xplico web interface. It shows a sidebar with navigation links like "Home", "Configuration", "Reports", and "Tools". The main area displays a table of network traffic analysis results, including columns for "Source", "Destination", "Protocol", "Size", and "Time".

Open Source

Network Forensic Analysis Tool

Protocols supported:
HTTP, IPv6, DNS, IRC, MSN, Facebook, VoIP,
SIP, RTP, MMS, FTP, ...

Xplico是一款开源网络取证分析工具，主要用于数字取证和渗透测试：Kali Linux, BackTrack, DEFT, Security Onion, Matriux, BackBox, CERT Forensics Tools and Pentoo。

9、PowerForensics



PowerForensics

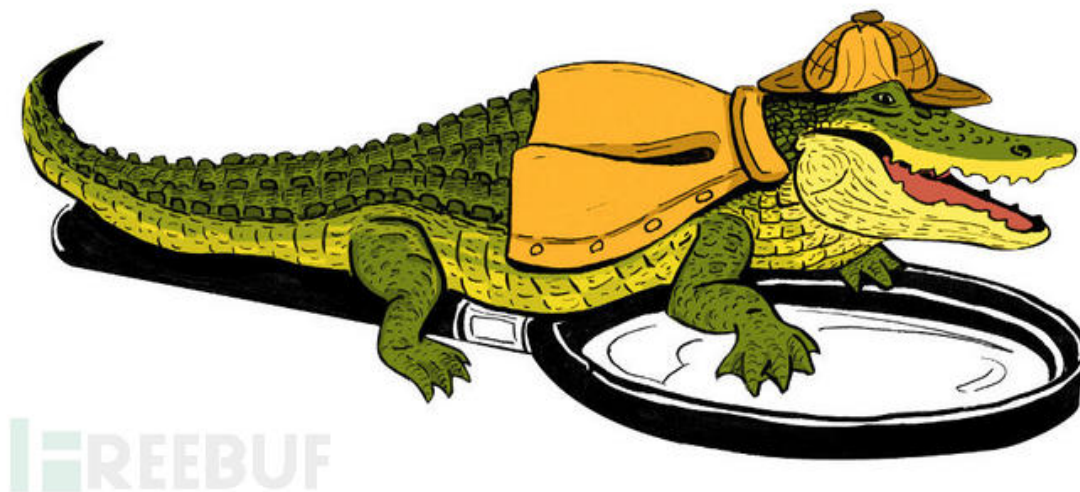
PowerForensics是一个Powershell数字取证框架。它目前支持NTFS，并且在论证过程中添加了ext4文件系统。

10、GRR Rapid Response



GRR Rapid Response是一款专注于远程现场取证的事件应急响应框架。它是一个被安装在目标系统的Python代理客户端，可以对Python基础设施进行管理和交流。

11、Mozilla InvestiGator



Mozilla InvestiGator 是一个进行远程端点的调查取证的OpSec平台，由安装在基础设施（实时查询的文件系统、网络状态、内存或端点配置）的所有系统的代理组成。

12、Autopsy

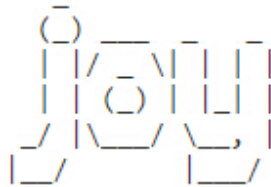


Autopsy® is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones. It has a plug-

in architecture that allows you to find add-on modules or develop custom modules in Java or Python.

Autopsy是一款数字取证平台，也是Sleuth Kit和其他数字取证工具的图形接口。它被用于关于计算机的法律执行、军事、企业审查等，甚至还可以用它来恢复从相机记忆卡中的照片。

[13. Joy](#)



A package for capturing and analyzing network flow data and intraflow data, for network research, forensics, and security monitoring.

可以用来捕获和分析网络流量数据和内网流量数据的包，主要用于进行网络调查、安全监控和取证。

[14. Rekall](#)

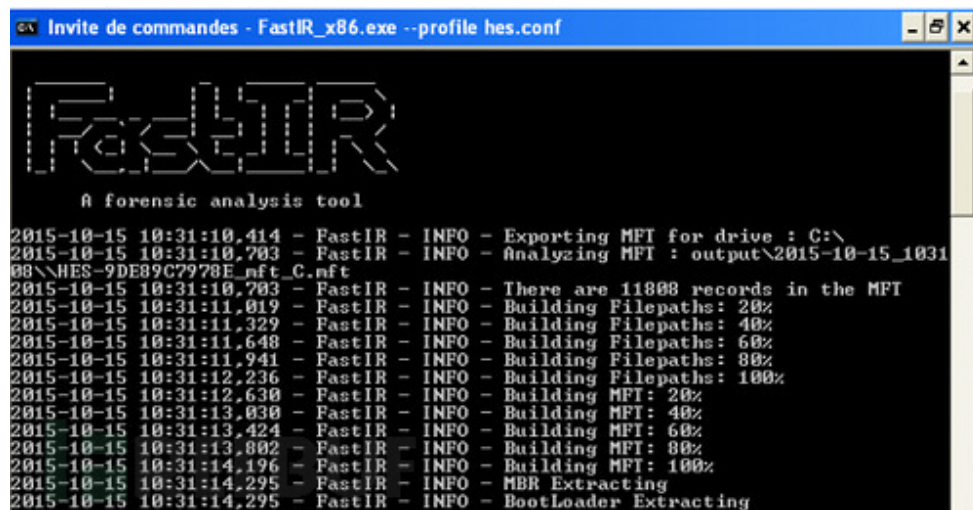


We can remember it for you wholesale!

Rekall框架是一个完全开放的工具集合，旨在向人们介绍技术以及从RAM中进行数字取证的复杂度，并提供一个平台来对这些数据进行进一步的分析。

提供一个平台去对这一领域进行进一步更为深入的研究。

15、FastIR Collector(红外刀)



```
Invite de commandes - FastIR_x86.exe --profile hes.conf

FastIR
A forensic analysis tool

2015-10-15 10:31:10.414 - FastIR - INFO - Exporting MFT for drive : C:\
2015-10-15 10:31:10.703 - FastIR - INFO - Analyzing MFT : output\2015-10-15_1031
008\HES-9DE89C7978E_nft_C.nft
2015-10-15 10:31:10.703 - FastIR - INFO - There are 11808 records in the MFT
2015-10-15 10:31:11.019 - FastIR - INFO - Building Filepaths: 20%
2015-10-15 10:31:11.329 - FastIR - INFO - Building Filepaths: 40%
2015-10-15 10:31:11.648 - FastIR - INFO - Building Filepaths: 60%
2015-10-15 10:31:11.941 - FastIR - INFO - Building Filepaths: 80%
2015-10-15 10:31:12.236 - FastIR - INFO - Building Filepaths: 100%
2015-10-15 10:31:12.630 - FastIR - INFO - Building MFT: 20%
2015-10-15 10:31:13.030 - FastIR - INFO - Building MFT: 40%
2015-10-15 10:31:13.424 - FastIR - INFO - Building MFT: 60%
2015-10-15 10:31:13.802 - FastIR - INFO - Building MFT: 80%
2015-10-15 10:31:14.196 - FastIR - INFO - Building MFT: 100%
2015-10-15 10:31:14.295 - FastIR - INFO - MBR Extracting
2015-10-15 10:31:14.295 - FastIR - INFO - BootLoader Extracting
```

Windows取证/信息收集神器，可收集的东西包括了所有你能想到的东西，不限于内存，注册表，文件信息等。

***作者：SecDarker，转载请注明来自FreeBuf黑客与极客（FreeBuf.COM）**