中南大學
CENTRAL SOUTH UNIVERSITY

Windows 取证工具

学生姓名	maybeLocalhost
学　　号	
专业班级	
指导教师	
学　　院	计算机学院
完成时间	2021.06

目录

一、Windows 取证框架

1.1 GRR Rapid Response

GRR Rapid Response 是一种事件响应框架，专注于对 Linux、macOS/OS X 和 Windows 客户端远程执行实时取证分析。调查人员将 Python 代理安装到目标系统上后，可以远程实时分析内存，以便收集用于取证分析的数据证据，并执行详细的系统监控，监控 CPU、处理器和输入/输出使用情况。GRR 还使用 SleuthKit 让调查人员可以访问原始文件系统，更底层的进行网络取证工作。

- GRR 由两部分组成：客户端和服务器：
  - GRR 客户端：部署在可能要调查的系统上。在每个这样的系统上，一旦部署，GRR 客户端会定期轮询 GRR 前端服务器以进行工作。“工作”意味着运行特定操作：下载文件，列出目录等。
  - GRR 服务器：基础架构由多个组件（前端，工作人员，UI 服务器）组成，并提供基于 Web 的图形用户界面和 API 端点，允许分析人员在客户端上安排操作并查看和处理收集的数据。
- GRR 客户端功能：
  - 跨平台支持 Linux，OS X 和 Windows 客户端。
  - 使用 YARA 库进行实时远程内存分析。
  - 强大的文件和 Windows 注册表搜索和下载功能。
  - 使用 SleuthKit（TSK）进行操作系统级和原始文件系统访问。
  - 专为 Internet 部署而设计的安全通信基础
  - 详细监控客户端 CPU，内存，IO 使用情况和自我限制。
- GRR 服务器功能：
  - 完全成熟的响应功能，可处理大多数事件响应和取证任务。
  - 企业狩猎（搜索机队）支持。
  - 快速简单地收集数百个数字取证单元。
  - AngularJS Web UI 和 RESTful JSON API，包含 Python，PowerShell 和

Go 中的客户端库。

- 强大的数据导出功能，支持各种格式和输出插件。
- 完全可扩展的后端，能够处理大型部署。
- 自动安排重复任务。
- 异步设计允许客户进行未来任务调度，旨在与大量笔记本电脑配合使用。

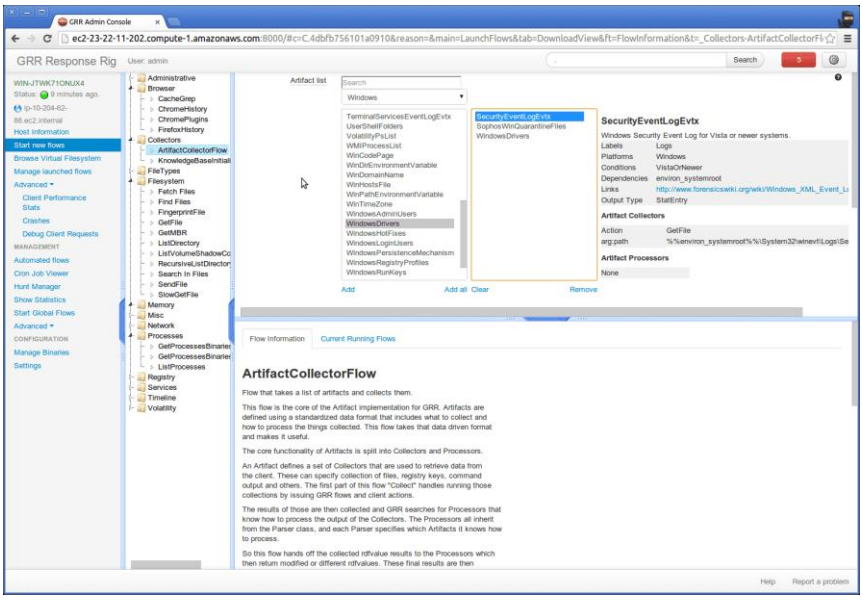

图 1 GRR Rapid Response

1.2 X-Ways Forensics

X-ways Forensics 是由德国 X-ways 出品的一个法证分析软件，它其实是 Winhex 的一个法证授权版，跟 Winhex 界面完全一样。它可以运行在所有可用的 Windows 版本上。下面是它的一些主要功能：

- 磁盘克隆和镜像功能，进行完整数据获取
- 可分析 RAW/dd/ISO/VHD/VMDK 格式原始数据镜像文件中的完整目录结构，支持分段保存的镜像文件
- 支持磁盘，RAID,扇区大小为 8KB 最大 2TB 的镜像的完全访问
- 支持对 JBOD、RAID0、RAID 5、RAID 5EE, RAID 6, Linux 软 RAID, Windows 动态磁盘和 LVM2 等磁盘阵列
- 自动识别丢失/删除的分区

- 支持 FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3, CDFS/ISO9660/Joliet, UDF 文件系统
- 无需修改原始硬盘或镜像纠正分区表或文件系统数据结构来解析文件系统
- 察看并获取 RAM 和虚拟内存中的运行进程
- 多种数据恢复功能，可对特定文件类型恢复
- 基于 GREP 符号维护文件头签名数据库
- 支持 20 种数据类型解释
- 使用模板查看和编辑二进制数据结构
- 数据擦除功能，可彻底清除存储介质中残留数据
- 可从磁盘或镜像文件中收集残留空间、空余空间、分区空隙中信息
- 创建证据文件中的文件和目录列表
- 能够非常简单地发现并分析 ADS 数据（NTFS 交换数据流）
- 支持多种哈希计算方法(CRC32，MD4，ed2k, MD5,SHA-1，SHA-256，RipeMD…)
- 强大的物理搜索和逻辑搜索功能，可同时搜索多个关键词
- 在 NTFS 卷中为文件记录数据结构
- 自动添加书签和注释
- 可以运行在 Windows FE 中等 Windows 环境
- 配合 F-Response 可进行远程计算机分析等

1.3 EnCase

Encase 是目前使用最为厂之的计算机取让工具,主少趋过 2000 家的法律执仃部门在使用它。它提供良好的基于 Windows 的界面，其功能包括：数据浏览、搜索、磁盘浏览、数据预览、建立案例、建立证据文件、保存案例等。

Encase 把硬盘中的文件镜像成只读的证据文件,这样可以防止调查人员修改数据而使其成为无效的证据。为了确定镜像数据与原始数据相同, Encase 会计算 CRC 校验码和 MD5 散列值进行比较。Encase 对硬盘驱动镜像后重新组织文件结构,采用 Windows CUI 显示文件内容,允许调查员使用多个工具完成多个任务。

与其他取证工具相比,Encase 主要具有以下几个特色:

(1) 在检查一个硬盘驱动时,Encase 深入操作系统底层查看所有的数据——包括 file slack ,未分配的空间和 Windows 交换分区(存有被删除的文件和其他潜在的证据)的数据。

(2) Encase 允许你将所有原始证据放到一个证据文件中(Encase 将 Encase DOS 创建的映像称为证据文件),然后把所有证据文件加到一个电子案例文件中,这样就可以一次搜索所有的介质。

(3) 在建立一个新的客例文件后程序就会提示你与该案例相关的信息将被放入 Encase 报告中。在这个程序里你可以对感兴趣的内容添加书签。你只要右击希望标记的数据,然后点击 Add Bookmark 就可以将书签添加进去。甚至有一个文本区域让你填写一些注释,用来提醒你在此处建立标记的原因。完成检测后,你可以右击报告并且选择 Export To File。Encase 导出的报告的格式为 RTF 格式。你可以在任何文字处理器上打开 RTF 文件进行其他的标注或者格式处理。

(4) Encase 的一个特色是图片浏览器。在其他大多数取证程序中,你必须先选定图片,再恢复被删除的文件,将其保存到外部存储介质中,然后用其他程序打开它们进行浏览。Encase 消除了中间步骤,使你可以直接对图片进行分类,选择你想浏览的图片,然后点击它的预览模式来观看。

(5) Encase 另一个特点是可以对证据进行快捷、方便的搜索。除了标准的搜索,Encase 还提供了多种搜索选项方便用户搜索。

1.4 Digital Forensics Framework

DFF 是一个能通过命令行和界面使用的取证框架。能被用于硬盘和内存调查并创建序使用者和系统活动情况的调查报告。该框架具有模块化、可编程性以及通用性三个特点。

1.5 Computer Online Forensic Evidence Extractor

COFEE，计算机在线法庭科学证据提取器，是专为计算机取证专家开发设计的一款工具包。该工具由 Microsoft 开发，用于从 Windows 系统收集证据。它可以被安装在 USB 驱动器或外部硬盘上。取证人员只需将 USB 插入目标计算机中，即可进行实时的分析。COFEE 包含了超过 150 个信息收集、密码破解、网络嗅探等工具。而且它的分析速度也非常的快，大概在 20 分钟左右就可以完成对目标系统的完整分析。对于执法机构，此外，Microsoft 还为使用该工具的执法机构，提供免费的技术支持。

二、系统监测工具

2.1 进程监测：Process Explorer

Process Explorer 是一款增强型的任务管理器，你可以使用它方便地管理你的程序进程，能强行关闭任何程序。它还详尽地显示计算机信息：CPU、内存使用情况，DLL、句柄信息。其功能包括：

(1) 更直观查看进程父子关系，结束指定进程，尤其是存在同名进程时更易识别

(2) 看到进程的实时创建、销毁情况

(3) 查看进程实时加载模块情况 （经常查看我们的钩子 dll 是否注入）

(4) 查看进程内句柄 （检查一些命名内核对象是否创建成功、检查是否存在句柄占用）

(5) 查看进程的相关属性 （文件路径、位数、版本、命令行等）

(6) 查看进程的资源占用情况 （CPU、内存）

(7) 查看进程的线程数、执行情况 （排查一些卡死进程的备用方案）

(8) 把进程两次运行（一次正常一次异常）的模块和句柄情况输出到文件，进行比对分析

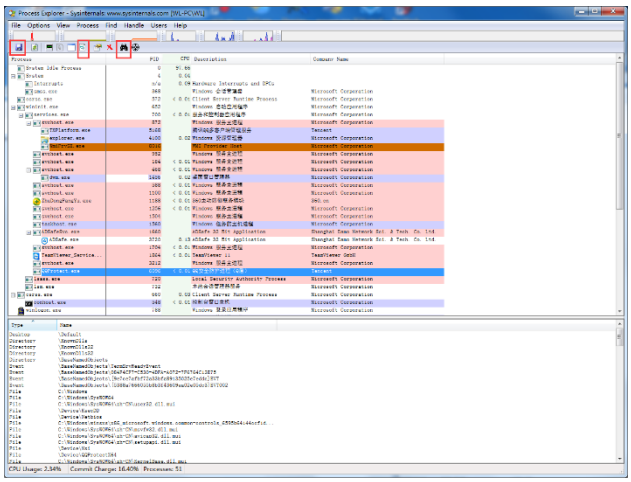

图 2 Process Explorer

2.2 文件监测：Filemon

Filemon 是一款文件系统监视软件，它可以监视应用程序进行的文件读写操作，监视文件系统的性能，并且报告代表逻辑文件、虚拟内存段、逻辑卷和物理卷的 I/O 活动。它将所有与文件一切相关操作（如读取、修改、出错信息等）全部记录下来以供用户参考，并允许用户对记录的信息进行保存、过滤、查找等处理，这就为用户对系统的维护提供了极大的便利。

但目前使用较多的是 Process Monitor，它一款系统进程监视软件，总体来说，Process Monitor 相当于 Filemon+Regmon，其中的 Filemon 专门用来监视系统中的任何文件操作过程，而 Regmon 用来监视注册表的读写操作过程。

2.3 注册表监测：Regmon

Regmon (Registry Monitor) 是一个注册表数据库监视软件，它将与注册表数据库相关的一切操作(如读取、修改、出错信息等)全部记录下来以供用户参考，并允许用户对记录的信息进行保存、过滤、查找等处理，这就为用户对系统的维护提供了极大的便利。

但目前使用较多的是 Process Monitor，它一款系统进程监视软件，总体来说，Process Monitor 相当于 Filemon+Regmon，其中的 Filemon 专门用来监视系统中的任何文件操作过程，而 Regmon 用来监视注册表的读写操作过程。

2.4 系统通信监测：TCPView

TCPView 是一个用来显示系统中所有的 TCP 和 UDP 端点（endpoint）列表的 Windows 程序，包括本地和远程的网络地址，以及 TCP 连接的状态。在 Windows Server 2008、Vista、NT、2000 和 XP 上，TCPView 还会显示拥有端点的进程名。TCPView 是 Windows 自带的 netstat 程序的一个子集，但是信息更加丰富且方便实用。

2.5 隐藏文件监测：Windows File Analyzer

Windows File Analyzer 工具可以对一些隐藏的系统文件（缓存文件）进行恢复，这也是取证过程中可以扩展信息来源的途径之一。

三、密码破解工具

3.1 AOPR

Advanced Office Password Recovery，简称 AOPR，是一款专业的 Office 密码破解软件。其主要功能如下：

(1) AOPR 可解密 Microsoft Office 所有版本（从 2.0 版至 2016 版）

(2) AOPR 非常熟悉密码保护的各种方法和技巧，所以几分钟内可恢复受保护文档

(3) AOPR 初步攻击会匹配缓存密码，试图最快打开文档

(4) 使用小型字典，AOPR 会尝试在不同的情况下恢复密码。

(5) AOPR 拥有六种特色攻击方式，同时恢复多个密码。

3.2 L0phtCrack

L0phtCrack，现在称为 L0phtCrack 6，是旨在测试密码强度的密码审核和恢复工具。它可以通过蛮力，字典，彩虹表和混合攻击来检索丢失的 Unix 和 M

icrosoft Windows 密码。 LOphtCrack 6 包括对升级的 Rainbow 表和 64 位 Windows 平台的支持。

3.3 Passware Kit Forensics

Passware Kit Forensic 是一款国外知名的用于密码恢复合集工具。软件的功能涵盖恢复文件密码、恢复因特网和网络密码、重置 Windows 管理员密码、搜索受保护的文件和恢复硬盘密码等。几乎能破解目前所有主流文件的密码，如 Zip、RAR、7Z 和 CAB 等主流压缩文件完全不在话下，且破解速度快，操作简单方便好用。Passware Kit Forensic 包含一个加密分析器，可以定位计算机上受密码保护的文件并分析其安全性。软件使用先进的密码恢复方法，其中针对不同情况的密码有不同的破解方式，词典、Xieve、暴力、已知的密码或其部分、先前的密码，以及它们的组合。支持多格式压缩文件密码找回；支持密码修改，能修改大小写、反向词等。

3.4 Cmospwd

工具软件 Cmospwd 可以破解 CMOS 密码。Cmospwd 是专门破解 CMOS 密码的工具软件。只要在 DOS 下启动该程序，它就会将用户的 CMOS 密码显示出来。该工具软件支持 Acer、AMI、AWARD、COMPAQ、 DELL、IBM、PACKARD BELL、PHOENIX、ZENITH AMI 等多种 BIOS，并且使用非常方便。

四、数据恢复工具

4.1 EasyRecovery

EasyRecovery 的具有“磁盘诊断”、“数据恢复”、“文件修复”和“邮件修复”等功能，可以使用 EasyRecovery 对删除的文件或数据进行恢复。

五、网络取证工具

5.1 WinDump 与 Ethereal

WinDump 可以根据指定的网卡对数据包进行抓包，并显示双方主机名称，还可以通过使用“-n”参数显示数据包的源 IP 地址和目的 IP 地址。

Ethereal 同样是根据指定的网卡对数据包进行抓取，但 Ethereal 抓取的包的信息更详细，并且能够查看包内的具体字节数据，而且 Ethereal 还提供过滤规则，这对于数据包的检索是很方便的，而 Windump 如果直接在命令行里运行使用是很难找到目标数据包的。Ethereal 后发展为现在常用的 WireShark。

5.2 CacheMonitor

CacheMonitor 可以监控 Internet 缓存，进而获取证据。

5.3 Sniffer Pro

Sniffer Pro 是一款的便携式网管和应用故障诊断分析软件，不管是在有线网络还是在无线网络中，它可以进行实时的网络监视、数据包捕获以及故障诊断分析能力。对于在现场进行快速的网络和应用问题故障诊断，基于便携式软件的解决方案具备最高的性价比，却能够让用户获得强大的网管和应用故障诊断功能。

六、数据分析工具

6.1 WinHex/UltraEdit

16 进制的文本编辑器与磁盘编辑软件。专门用来对付计算机取证、数据恢复、低级数据处理、以及 IT 安全性、各种日常紧急情况的高级工具：用来检查和修复各种文件、恢复删除文件、硬盘损坏、数码相机卡损坏造成的数据丢

失等；可以进行 Hex 和 ASCII 编码的编辑与修改，支持多文件搜寻替换功能模式，一般和逻辑运算，磁盘磁区的编辑（包括 FAT16、FAT32 和 NTFS 分区格式），文件比对和分析功能。

6.2 Sleuth Kit

Sleuth Kit 是用于分析 Microsoft 和 UNIX 文件系统和磁盘的开源取证工具包。Sleuth Kit 使研究人员能够从事件响应过程中或实时系统中获取的图像中识别并恢复证据。Sleuth Kit 是开源的，它使研究人员可以验证工具的操作或根据特定需要对其进行自定义。该工具允许用户分析创建的磁盘或文件系统映像或创建原始映像的类似应用程序，对文件系统进行深入分析以及其他各种功能。

七、证据提取工具

8.1 FTK Imager

FTK Imager 是一款电子数据预览和镜像提取工具，可以快速创建计算机数据的合规复制文件（取证镜像），且不会更改原始证据。具有以下三个特点：

- 速度更快

  FTK Imager 的最新 4.3.0 版本在镜像创建方面有显著的速度改进，我们已经看到将设备的镜像提取时间减少到原来的一半，允许您更快地保存数据并更快地开始分析。

- 精准度高

  FTK Imager 可以在不改变原始证据的情况下创建和规的计算机数据拷贝或电子数据镜像。镜像文件在各个方面都与原始存储设备相同，包括文件空闲和未分配空间或驱动器可用空间部分数据。这样可以在使用镜像文件进行调查时，将原始存储媒介存放在安全区域免受篡改。

- 完整性强

  自动生成常规文件和磁盘镜像的哈希值报告，用作证明案例证据完整性的基

准。当对完整驱动器进行镜像时，可以使用 FTK Imager 生成的哈希值来验证镜像创建后镜像哈希值和驱动器哈希值是否完全匹配，以及镜像文件自获取以来是否保持不变。

8.2 Volatility

Volatility 是一款开源内存取证框架，能够对导出的内存镜像进行分析，通过获取内核数据结构，使用插件获取内存的详细情况以及系统的运行状态。该工具实验 Python 编写，易于和基于 python 的主机防御框架集成。支持多平台，如：Windows，Mac，Linux，可以通过插件来扩展 Volatility 的分析能力 imageinfo：显示目标镜像的摘要信息，这常常是第一步---获取内存的操作系统类型及版本，之后可以在 –profile 中带上对应的操作系统，后续操作都要带上这一参数

- pslist：该插件列举出系统进程，但它不能检测到隐藏或者解链的进程，psscan 可以
- psscan：可以找到先前已终止(不活动)的进程以及被 rootkit 隐藏或解链的进程
- pstree：以树的形式查看进程列表，和 pslist 一样，也无法检测隐藏或解链的进程
- mendump：提取出指定进程，常用 foremost 来分离里面的文件(历年美亚杯有此题)
- filescan：扫描所有的文件列表
- hashdump：查看当前操作系统中的 password hash，例如 Windows 的 SAM 文件内容(实际中没有 mimikatz 效果好)
- svcscan：扫描 Windows 的服务
- connscan：查看网络连接
- cmdscan：可用于查看终端记录
- dlllist: 列出某一进程加载的所有 dll 文件
- dumpfiles：导出某一文件(指定虚拟地址)

- hivelist: 列出所有的注册表项及其虚拟地址和物理地址
- timeliner: 将所有操作系统事件以时间线的方式展开

8.3 WindowsSCOPE

WindowsSCOPE 是 Windows 的内存取证和逆向工程产品，用于获取和分析易失性存储器。其用途之一是对 rootkit 和其他恶意软件进行检测和逆向工程。WindowsSCOPE 支持通过 Windows 10 获取和分析运行 Windows XP 的 Windows 计算机。它主要用于恶意软件的逆向工程。它提供分析 Windows 内核、驱动程序、DLL、虚拟和物理内存的功能。