中南大學
CENTRAL SOUTH UNIVERSITY

Linux 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、Linux 取证框架

1.1 SIFT – SANS 调查取证工具包

SIFT 具备检查原始磁盘（比如直接从硬盘或其他任何存储设备上获取的字节级数据）、多种文件系统及证据格式的能力。该工具包基本基于 Ubuntu 系统，从高级取证格式(AFF)到 RAW(dd)证据格式都支持，是包含了执行深度取证调查或响应调查所需工具的一张 Live CD。

SIFT 的主要特点有：

(1) 基于 Ubuntu LTS 14.04；

(2) 支持 64 位系统；

(3) 内存利用率更高；

(4) 自动数字取证及事件响应(DFIR)包更新及自定义设置；

(5) 最新的取证工具和技术；

(6) 可用 VMware Appliance 进行取证；

(7) 兼容 Linux 和 Windows；

(8) 可选择通过(.iso)镜像文件单独安装或经 VMware Player/Workstation 使用 ReadTheDocs 上有在线文档项目；

(9) 扩展了支持的文件系统。

1.2 CAINE

CAINE 基于 Linux 系统打造，通常是包含了一系列取证工具的一张 Live CD。由于最新版 CAINE 建立在 Ubuntu Linux LTX、MATE 和 LightDM 上，熟悉这些系统的人便可以无缝使用 CAINE。

CAINE 的主要功能有：

(1) CAINE 界面——集成了一些著名取证工具的用户友好界面，其中很多工具都是开源的；

(2) 经过更新优化的取证分析环境；

(3) 半自动化的报告生成器。

1.3 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。

1.4 HELIX3

HELIX3 是一个基于 Linux 的 Live CD，用于事件响应构建，计算机取证和电子发现方案。它包含了许多开源工具，从十六进制编辑器到数据刻画软件到密码破解工具等。当使用 HELIX3 向导时，会询问是要加载 GUI 环境还是将 HELIX3 安装到磁盘。如果选择直接加载 GUI 环境(推荐)，将出现一个基于 Linux 的屏幕，你可以选择运行捆绑工具的图形化版本。

二、磁盘数据工具

2.1 Linux DD

dd 命令作用是用指定大小的块拷贝一个文件，并在拷贝的同时进行指定的转换。可以用于测试磁盘命令、数据备份或恢复等，可用于复制文件并对原文件的内容进行转换和格式化处理。用的比较多的还是用 dd 来备份裸设备。但是不推荐，如果需要备份 oracle 裸设备，可以使用 rman 备份，或使用第三方软件备份，使用 dd 的话，管理起来不太方便。建议在有需要的时候使用 dd 对物理磁盘操作，如果是文件系统的话还是使用 tar backup cpio 等其他命令更加方便。另外，使用 dd 对磁盘操作时，最好使用块设备文件。

2.2 Bulk Extractor

在数字取证中，通常需要面对海量的数据，如几百 GB 甚至 TB 级别的数据。从这些海量数据中，提取有价值的数据是一个漫长、枯燥、繁琐的过程。Kali Linux 提供一款批量数据提取工具 bulk-extractor。该工具采用 C++语言

编写，可以从备份镜像文件中自动提取各种数据，如电话号码、信用卡号、邮件地址、EXIF、GPS、Prefetch 等信息。为了方便分析，该工具还会对提取的信息进行分析，统计信息出现的频率。该工具的每项信息收集提取功能均以插件形式实现。这样，渗透测试人员可以根据项目选择对应的插件，从而更快速的完成分析工作。

三、密码破解工具

3.1 HashCat

HashCat 号称世界上最快的密码破解，世界上第一个和唯一的基于 GPGPU 规则引擎，免费多 GPU（高达 128 个 GPU），多哈希，多操作系统（Linux 和 Windows 本地二进制文件），多平台（OpenCL 和 CUDA 支持），多算法，资源利用率低，基于字典攻击，支持分布式破解等等。HashCat 目前支持各类公开算法高达 247 类，市面上面公开的密码加密算法基本都支持。HashCat 系列软件在硬件上支持使用 CPU、NVIDIA GPU、ATI GPU 来进行密码破解。在操作系统上支持 Windows、Linux 平台，并且需要安装官方指定版本的显卡驱动程序，如果驱动程序版本不对，可能导致程序无法运行。

HashCat 主要分为三个版本：HashCat、oclHashCat-plus、oclHashCat-lite。这三个版本的主要区别是：HashCat 只支持 CPU 破解。oclHashCat-plus 支持使用 GPU 破解多个 HASH，并且支持的算法高达 77 种。oclHashCat-lite 只支持使用 GPU 对单个 HASH 进行破解，支持的 HASH 种类仅有 32 种，但是对算法进行了优化，可以达到 GPU 破解的最高速度。如果只有单个密文进行破解的话，推荐使用 oclHashCat-lite。

四、数据恢复工具

4.1 Linux debugfs

用 Unix 下的恢复工具如 debugfs 恢复被删除的文件，保存到准备好的外置 USB 硬盘上，并查看是否找回了所有的删除文件，对恢复文件进行检查和分析，找出图片文件，获得有效的证据。

(1) 首先模拟在根目录下建立文件并删除。

(2) 运行 debugfs，进入调度模式执行“open /dev/sda1”执行 ls -d 会列出此目录最近的操作，其中可以看到“jin_ju_ning_meng”的删除记录。

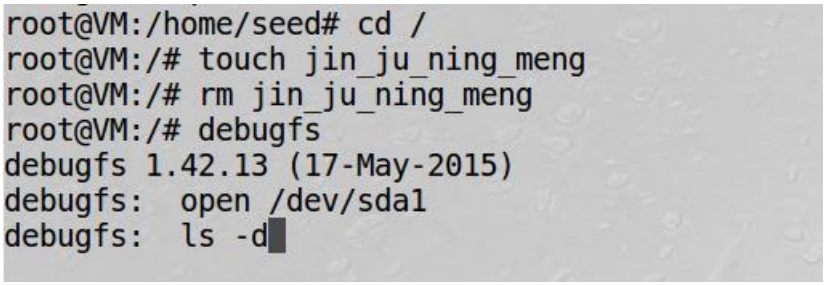

图 1 open /dev/sda1

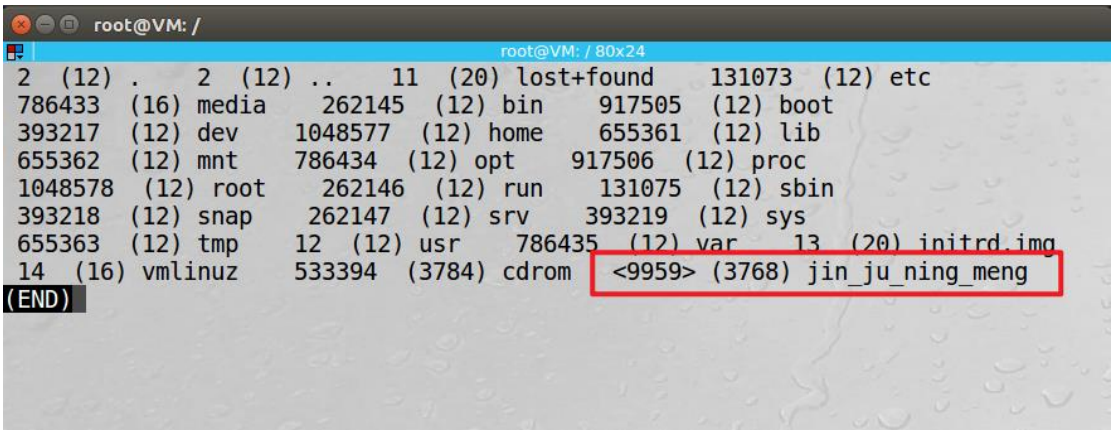

图 2 “jin_ju_ning_meng"的删除记录

(3) 执行 logdump -i <num>显示此日志内容（这里 num 为上图指出的 9959），并记录 blockid = 1624，offset = 768。

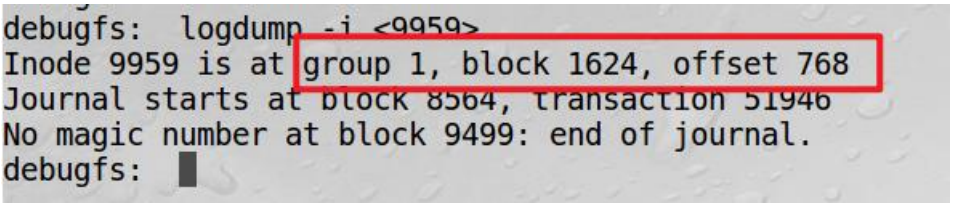

图 3 logdump -i 9959

(4) 最后运行命令“dd if=/dev/sda1 of=/jin_ju_ning_meng bs=[offset] count=1 skip=[blockid]”（这里填入上面的记录）即可恢复文件。

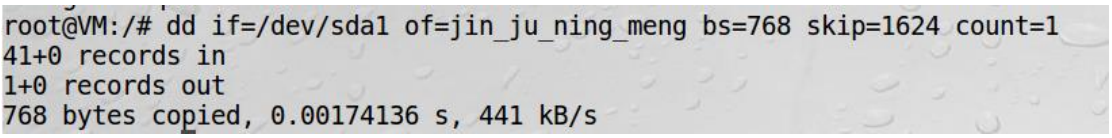

图 4 dd if=/dev/sda1 of=/jin_ju_ning_meng bs=768 count=1 skip=1624

图 5 文件成功恢复

五、网络取证工具

5.1 Xplico

Xplico 是又一款开源网络取证分析工具，可以重建 Wireshark、ettercap 等包嗅探器抓取的网络流量内容，来自任何地方的内容都可以。

Xplico 的特性包括：

(1) 支持 HTTP、SIP、IMAP、POP、SMTP、TCP、UDP、IPv4、IPv6 协议；

(2) 端口无关的协议识别(PIPI)；

(3) 多线程；

(4) 可在 SQLite 数据库或 Mysql 数据库及文件中输出数据和信息；

(5) Xplico 重组的每个数据都与一个 XML 文件相关联，该 XML 文件唯一标识了该数据流及包含该重组数据的 pcap 包；

(6) 对数据记录的大小或文件数量没有任何限制（唯一的限制只存在于硬盘

大小）；

(7) 模块化：每个 Xplico 组件都是模块化的。

(8) 某些数字取证及渗透测试操作系统，如 Kali Linux、BackTrack 等，默认安装了 Xplico。

5.2 WireShark

WireShark 可以捕获并描述网络数据包，其最大的优势就是免费、开源以及多平台支持，在 GNU 通用公共许可证的保障范围下，用户可以免费获取软件和代码，并拥有对其源码修改和定制的权利，如今其已是全球最广泛的网络数据包分析软件之一。

WireShark 中数据包的结构：

- 第一行：数据包整体概述；
- 第二行：链路层详细信息，主要的是双方的 mac 地址；
- 第三行：网络层详细信息，主要的是双方的 IP 地址；
- 第四行：传输层的详细信息，主要的是双方的端口号；
- 第五行：传输使用的协议和传输的 DATA，DNS 这是域名的相关信息。

抓包时首先在 WireShark 中选择合适的网卡，然后开始抓包：

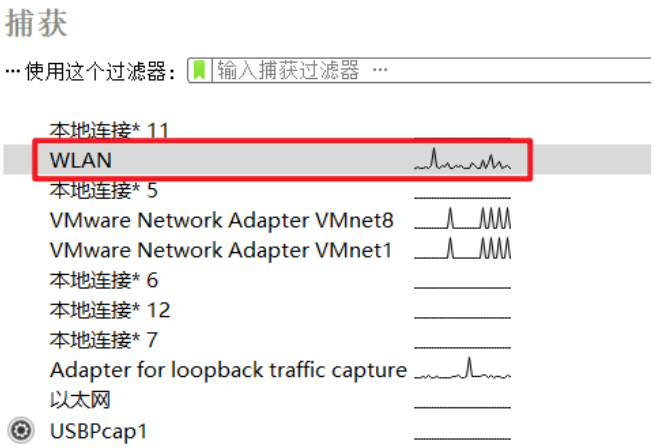

图 6 选择合适的网卡

运行“ping www.baidu.com”，并在 WireShark 中查看捕获到的数据包。Wire Shark 中可以通过设置关键词进行过滤显示，在这里我们查找“ICMP”数据包。

```
C:\Users\乐>ping www.baidu.com

正在 Ping www.a.shifen.com [183.232.231.174] 具有 32 字节的数据:
来自 183.232.231.174 的回复: 字节=32 时间=45ms TTL=51
来自 183.232.231.174 的回复: 字节=32 时间=69ms TTL=51
来自 183.232.231.174 的回复: 字节=32 时间=78ms TTL=51
来自 183.232.231.174 的回复: 字节=32 时间=75ms TTL=51

183.232.231.174 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 45ms, 最长 = 78ms, 平均 = 66ms

C:\Users\乐>
```

图 7 ping www.baidu.com

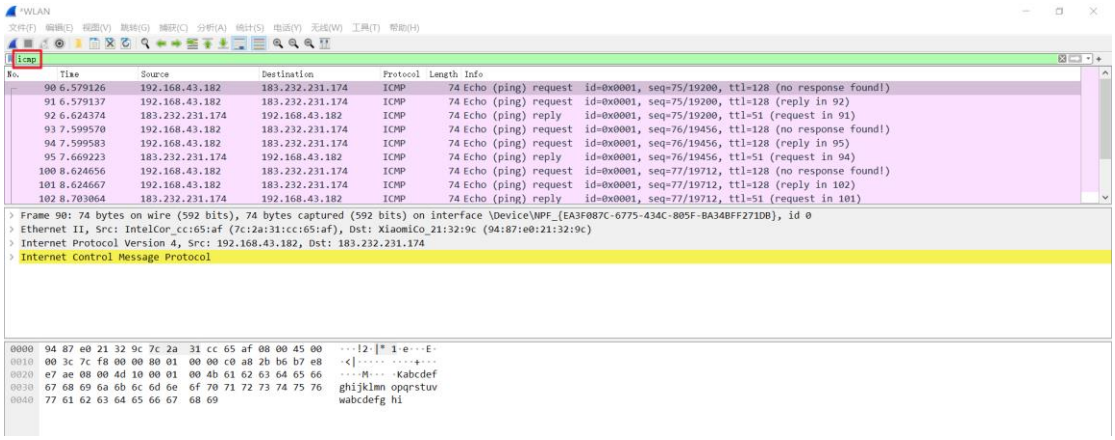

图 8 查找“ICMP”数据包

六、数据分析工具

6.1 The Coroner's Toolkit（TCT）

TCT 是由 Dan Farmer 和 Wietse Venema 编写的用于 UNIX 系统被攻破后进行事后分析的程序集,主要包括以下几部分:

- grave-robber:捕获信息。
- ils and mactime:显示死亡和存活的文件的访问模式。unrm and lazarus:

恢复被删除的文件。

- findkey:恢复文件或正在运行的进程的密钥。

其适用的操作系统包括 Solaris、 SunOS、 FreeBSD、LINUX、BSD/OS 和 OpenBSD 等。

它提供了强大的调查能力,它的特点是可以对运行着的主机的活动进行分析,并捕获目前的状态信息。其中的 grove-robber 可以收集大量的正在运行的讲程、网络连接以及硬盘驱动器方面的信息。数据基本上以挥发性顺序收集,收集所有的数据是个很缓慢的过程.要花上几个小时的时间。TCT 包括数椐恢复和浏览工具 unrm&lazarns、获取 MAC 时间的工具 mactime ,还包括一些小工具.如 ils（用来显示被删除的索引节点的原始资料）、icat(用干取得特定的索引节点对应文件的内容)，等等。

TCT 并不是用于收集传统的法庭证据，而是用来确定在被攻破的主机发生了什么。它必须在被攻破的主机上运行，这可能会被看作是对证据的破坏。
TCT 最不同的特点是他可以对运行的主机的活动进行分析，并捕获当前的状态信息，而这对于手动方式是不可能的或者是非常困难的。TCT 的 grave-robber 工具可以收集大量的正在运行的进程、网络连接以及硬盘驱动器方面的信息。数据基本上以挥发性顺序收集。运行 grave-robber 最合适的方法是只对运行的系统收集可变的数据，然后关闭系统，对驱动器做映像。

Mac 工具可以对每个索引节点（inode）收集一个按照时间排序的修改/访问/改变时间列表,同时还有它们相关的文件名，可以帮助分析系统文件访问和系统行为之间的联系。Mac 可以应用到任何系统中。

TCT 的 unrm 可以试图从比特流重构成一系列连贯的数据，也可以从文件系统中创建一个比特流。它能产生一个单独的对象，包括文件系统未分配空间中所有的数据。一旦创建了对象后,接下来就可以使用 lazarus 工具系统地分析整个对象，判断其中是否有特殊的文本或二进制文件。该工具的分析效果非常好,从中可以得到很多细节信息，最终该工具会建立一个“数据地图”来显示它认为已发现的数据类型。

6.2 ForensiX

ForensiX 主要运行于 Linux 环境，是一个以收集数据和分析数据为主要目的的工具。它与配套的硬件组成专门工作平台，支持多种类型的硬件，而且包括对硬盘驱动器、软盘驱动器、磁带、光盘以及 Jazz 驱动器的支持。任何它所支持的媒体都可以被快速地映像，进行 MD5S 核查，并且记采到案例数据库中。这种非常有效的批处理操作,使映像大量的软盘驱动器变得很方便。

Linux 比其他操作系统支持更多的文件系统,ForensiX 正是利用了这一点，提供在不同的文件系统里自动装配映像等能力、能够发现分散空间里的数据、可以分析 UNIX 系统是否含有木马程序。文件系统的装配是只读的,这样做是为了防止因疏忽而造成的更改。一旦文件系统或映像被装配,就可以对简单的字符串进行搜索，或者可以进行更复杂的模糊搜索。

它包含许多的插件，可以进行不同类型的搜索。一个图形文件功能的插件能够使它自动搜索映像并显示位图。这里所说的映像分析是把整个磁盘的映像作为一个目标,因此,它能够发现分散空间里的数据。它的大多数功能都是通过图形用户终端实现的。

Forensix 拥有几个不同寻常的功能，例如，可以对 UNIX 系统可能存在的漏泪进行检查。它也能建立一个文件系统的基线图、存储散列值和文件名,然后将基线同其他文件系统的映像作比较。这种特点可以分析 UNIX 系统的映像，例如，看它是否包含了木马程序。另外，其中的 Webtrace 可以自动搜索互联网上的域名，为网络取证进行必要的收集工作。它的其他网络功能还包括建立和分析 TCP dump，新版本具有识别隐藏文件的工具。

6.3 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

7.1 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。

7.2 PlainSight

PlainSight 是一个基于 Knoppix(Linux 发行版)的 Live CD，它允许用户执行数字取证任务，如查看互联网历史记录，数据刻画，USB 设备使用信息收集，检查物理内存转储，提取哈希密码等。