



中国互联网安全大会



360互联网安全中心

电子取证技术分论坛



加密磁盘取证技术

Forensic analysis of encrypted drives

演讲人：徐志强

2016 中国互联网安全大会
China Internet Security Conference

协同联动 共建安全+命运共同体

个人简介



徐志强 (Henry Tsui)

中国政法大学, 法务会计研究中心特聘研究员

江西警察学院, 计算机犯罪中心特聘研究员

中华全国律师协会信息网络与高新技术专委会特邀委员

南昌大学, 工程硕士专业学位研究生导师

中国刑事警察学院, 客座讲师

- 美国EnCase认证调查员(EnCE)—中国大陆首位获得
- 美国EnCase认证讲师
- 美国ISC²认证电子取证专家(CCFP) —中国大陆首位获得
- 中国电子数据取证调查员(MCE)
- 美国高科技犯罪调查协会会员(HTCIA)
- 美国注册舞弊审查师协会会员(ACFE)



物理安保



大厦大门



房门

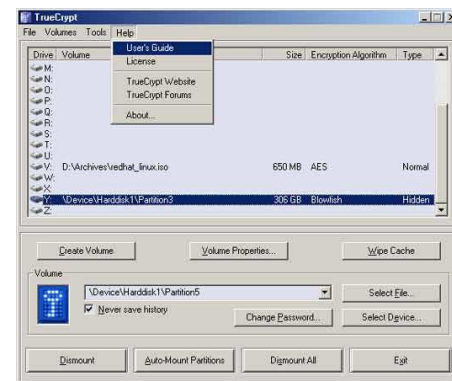
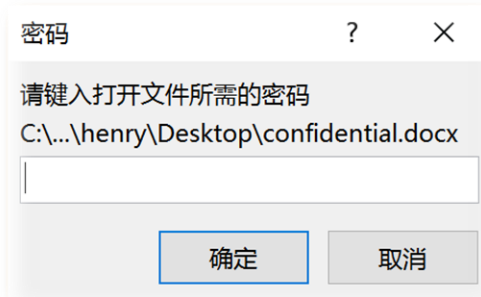


抽屉

电子数据安保



- 硬件：生物特征/数字密码
- 软件：全盘加密/加密容器
- 应用：文件加密



加密磁盘类型及应用

■ 磁盘加密类型

— 硬件级加密

- 磁盘固件
- 加密芯片

— 软件级加密

- 全盘/卷加密
- 加密容器



1. 磁盘固件加密

- 1997年发布ATA-3规范，开始支持硬盘数据安全保护。
- 硬盘可通过BIOS或第三方软件设置硬盘保护密码

■ 特性

- 支持两种密码：Master(主密码)和User(用户密码)
- 支持两种安全级别：High和Maximum

■ BIOS设置硬盘密码

- 多数商务型笔记本（如Thinkpad、Dell Latitude）均支持在BIOS直接设置硬盘密码)



ATA加密硬盘取证方法

■ 取证方法

- 获取磁盘固件信息直接提取硬盘密码
- 采用固件替换法绕过硬盘密码保护

■ 取证工具

- ATOLA Insight
- PC-3000 UDMA



ATA加密硬盘取证方法



Atola Insight Forensic interface showing the process of extracting and resetting the ATA password for a WDC WD1600AAJS-6084... drive.

主界面

- 诊断
- 设备恢复
 - 固件恢复
 - 口令恢复**
 - NVRAM 访问
- 映像
- 文件恢复
- 设备工具
 - 磁盘编辑器
 - 计算散列
 - 填充/擦除
 - SSD 修剪
 - 从文件中写入
 - 比较
 - 设备功能
 - 设备配置
 - 主机保护区域
 - 取消 HPA/DCO 限制
 - 安全特性
 - 介质恢复
 - 生成坏扇区

已提取口令并重置

提取到的口令: Delk#280.....

十六进制口令: 44 65 48 65 23 32 38 30 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

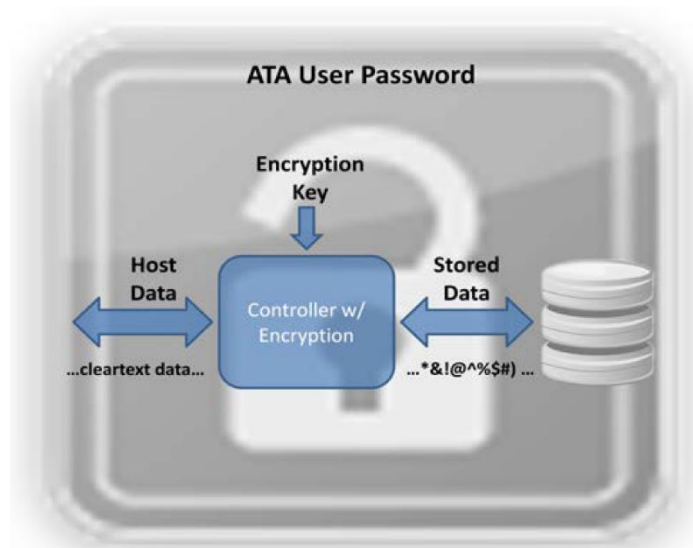
备注: 当前附加设备的写保护已关闭。

状态: ERR INDX CORR DREQ DRSC FAULT DRDY BUSY

错误: AMNF TONF A8RT - IDNF - UNC ICRC

2. 加密芯片

- 基于独立加密芯片的磁盘加密，可采用工业级加密算法（如AES）实现数据真正加密。
- 符合美国FIPS 197信息处理标准



加密磁盘类型及应用



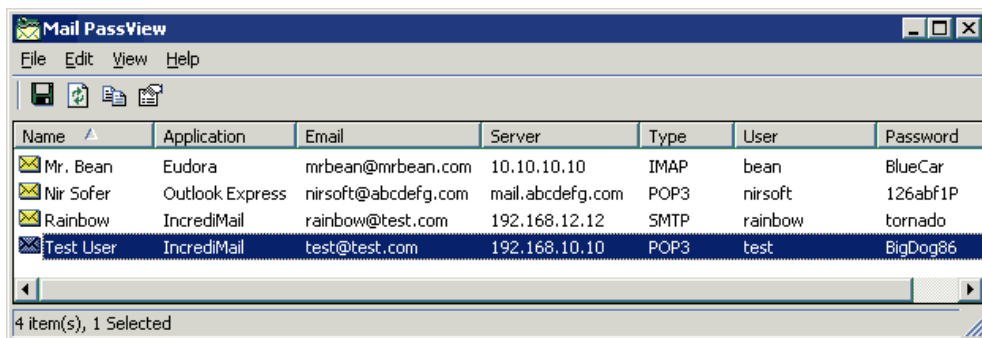
2. 加密芯片

- 越来越多的硬盘厂商提供支持加密的移动硬盘，内置硬盘加密管理工具。

| | | | |
|-----------------------------------|---|--|-----------------------|
| 磁盘 0 基本 238.35 GB 联机 | 260 MB 状态良好 (EFI 系统分区) | Windows (C:) 237.26 GB NTFS (BitLocker 已加密) 状态良好 (启动, 页面文件, 故障转储, 主分区) | 850 MB 状态良好 (恢复分区) |
| 磁盘 1 未知 1862.99 GB 没有初始化 | 1862.99 GB 未分配 | | |
| 磁盘 0 基本 238.35 GB 联机 | 260 MB 状态良好 (EFI 系统分区) | Windows (C:) 237.26 GB NTFS (BitLocker 已加密) 状态良好 (启动, 页面文件, 故障转储, 主分区) | 850 MB 状态良好 (恢复分区) |
| 磁盘 1 基本 1862.99 GB 联机 | My Passport (F:) 1862.98 GB NTFS 状态良好 (主分区) | | |

芯片加密磁盘取证

- 提取生物特征进行解密
- 提取相关密码辅助解密



Mail PassView

File Edit View Help

| Name | Application | Email | Server | Type | User | Password |
|-----------|-----------------|---------------------|------------------|------|---------|----------|
| Mr. Bean | Eudora | mrbean@mrbean.com | 10.10.10.10 | IMAP | bean | BlueCar |
| Nir Sofer | Outlook Express | nirsoft@abcdefg.com | mail.abcdefg.com | POP3 | nirsoft | 126abf1P |
| Rainbow | IncrediMail | rainbow@test.com | 192.168.12.12 | SMTP | rainbow | tornado |
| Test User | IncrediMail | test@test.com | 192.168.10.10 | POP3 | test | BigDog86 |

4 item(s), 1 Selected



3. 全盘/卷加密

- 常见的加密软件BitLocker、SafeBoot、PGP、CheckPoint等

■ 特点

- 基于软件的磁盘加密部署起来更灵活简单，适用性强。
- 支持对操作系统所在分区也加密，大大提升系统分区的数据安全性。

常见全盘加密软件



- McAfee Safeboot /McAfee Endpoint Encryption
- Bitlocker/BitLockerToGo
- Check Point PointSec PC/Endpoint Full Disk Encryption
- PGP WDE / Symantec Encryption
- Utimaco SafeGuard Easy
- WinMagic SecureDoc
- GuardianEdge
- Sophos SafeGuard
- FileVault (Macintosh OSX)
- LUKS (Linux)

全盘加密的模式特征



| 类型 | 存储位置 | 偏移量 | 特征字符 |
|--|-----------|---------------|---|
| BitLocker (Vista) | VBR 扇区 | Offset 0 | Hex: EB 52 90 2D 46 56 45 2D 46 53 2D ASCII: ëR --FVE--FS- |
| BitLocker (Win7/Win8) | VBR 扇区 | Offset 0 | Hex: EB 58 90 2D 46 56 45 2D 46 53 2D ASCII: ëX --FVE-FS- |
| SafeBoot | MBR 扇区 | Offset 3 | Hex: 53 61 66 65 42 6F 6F 74 ASCII: SafeBoot |
| Check Point FDE | VBR 扇区 | Offset 90 | Hex: 50 72 6F 74 65 63 74 ASCII: Protect |
| GuardianEdge Encryption Plus/Anywhere | MBR 扇区 | Offset 6 | Hex: 50 43 47 4D ASCII: PCGM |
| Symantec Endpoint Encryption | MBR 扇区 | Offset 6 | Hex: 50 43 47 4D ASCII: PCGM |
| Sophos Safeguard Enterprise | MBR 扇区 | Offset 119 | Hex: 53 47 4D 34 30 30 3A ASCII: SGM400 |
| Safeguard Easy | MBR 扇区 | Offset 144 | Hex: 53 47 45 34 30 30 3A ASCII: SGE400 |

全盘加密的模式特征



| 类型 | 存储位置 | 偏移量 | 特征字符 |
|---------------------------|-------|---------------|---|
| Symantec PGP WDE | MBR扇区 | Offset 3 | Hex: EB 48 90 50 47 50 47 55 41 52 44 ASCII: ëH PGPGUARD |
| WinMagic SecureDoc FDE | MBR扇区 | Offset 246 | Hex: 57 4D 53 44 ASCII: WMSD |
| Apple FileVault | 容器 | Offset 0 | Hex: 65 6E 63 72 63 64 73 61 ASCII: encrdsa |

全盘加密的模式特征



EnCase Law Enforcement

File Edit View Tools Help

New Open Save Print Add Device Search Refresh Find

Cases

Home Entries Bookmarks Search

Home File Extents Permissions

Entries

1

C

D

Table Report Gallery Timeline Disk Code

| | Name | Filter | In Report | File Ext | File Type | File Category | Signature |
|---|----------------------|--------|-----------|----------|-----------|---------------|-----------|
| 1 | Unallocated Clusters | | | | | | |

Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage

EnScript Hits Filters

EnScript

- Examples
- Forensic
- Include
- Main
- Source Processor

Case 1\1D\Unallocated Clusters (PS 65664 LS 0 CL 0 SO 000 FO 0 LE 11)

/ista

/in7-
/in10

Safe
Boot

支持全盘加密的取证软件



| 加密类型 | | EnCase v6 | EnCase v7 | FTK V6 | 取证大师 V4 |
|------------------------|---------------|--------------|--------------|-----------|------------|
| Microsoft BitLocker | Vista | 支持 | 支持 | 支持 | 支持 |
| | Win7 | 支持 | 支持 | 支持 | 支持 |
| | Win8 | 不支持 | 支持 | 未知 | 支持 |
| | Win10 | 不支持 | 支持 | 未知 | 支持 |
| | BitLockerToGo | 支持(Win7) | 支持 | 未知 | 支持 |
| McAfee SafeBoot | 4.x | 支持 | 支持 | 支持 | 不支持 |
| | 5.x | 支持 | 支持 | 支持 | 不支持 |
| | 6.x | 支持 | 支持 | 支持 | 不支持 |
| | 7.x | 支持 | 支持 | 未知 | 不支持 |
| FileVault | V1 | 不支持 | 未知 | 支持 | 不支持 |
| | V2 | 不支持 | 未知 | 支持 | 支持 |
| TrueCrypt | V6-V7 | 不支持 | 不支持 | 不支持 | 支持 |

支持全盘加密的取证软件



| 加密类型 | | EnCase v6 | EnCase v7 | FTK V6 | 取证大师 V4 |
|-------------------------|------|--------------|--------------|-----------|------------|
| Check Point PointSec | 6.x | 不支持 | 支持 | | 不支持 |
| | 7.x | 不支持 | 支持 | | 不支持 |
| | 8.x | 不支持 | 支持 | | 不支持 |
| Sophos SafeGuard | 4.x | 支持 | 支持 | 支持 | 不支持 |
| | 5.x | 支持 | 支持 | 支持 | 不支持 |
| | 6.x | 支持 | 支持 | 未知 | 不支持 |
| Linux | LUKS | 不支持 | 不支持 | 不支持 | 支持 |
| Symantec PGP FDE | 9.x | 支持 | 支持 | 不支持 | 不支持 |
| | 10.x | 支持 | 支持 | 不支持 | 不支持 |
| Symantec Endpoint | 7.x | 不支持 | 支持 | 不支持 | 不支持 |
| | 8.x | 不支持 | 支持 | 不支持 | 不支持 |

4. 加密容器(虚拟磁盘)

– 常见的加密软件TrueCrypt、Private Disk、PGP等

■ 特点

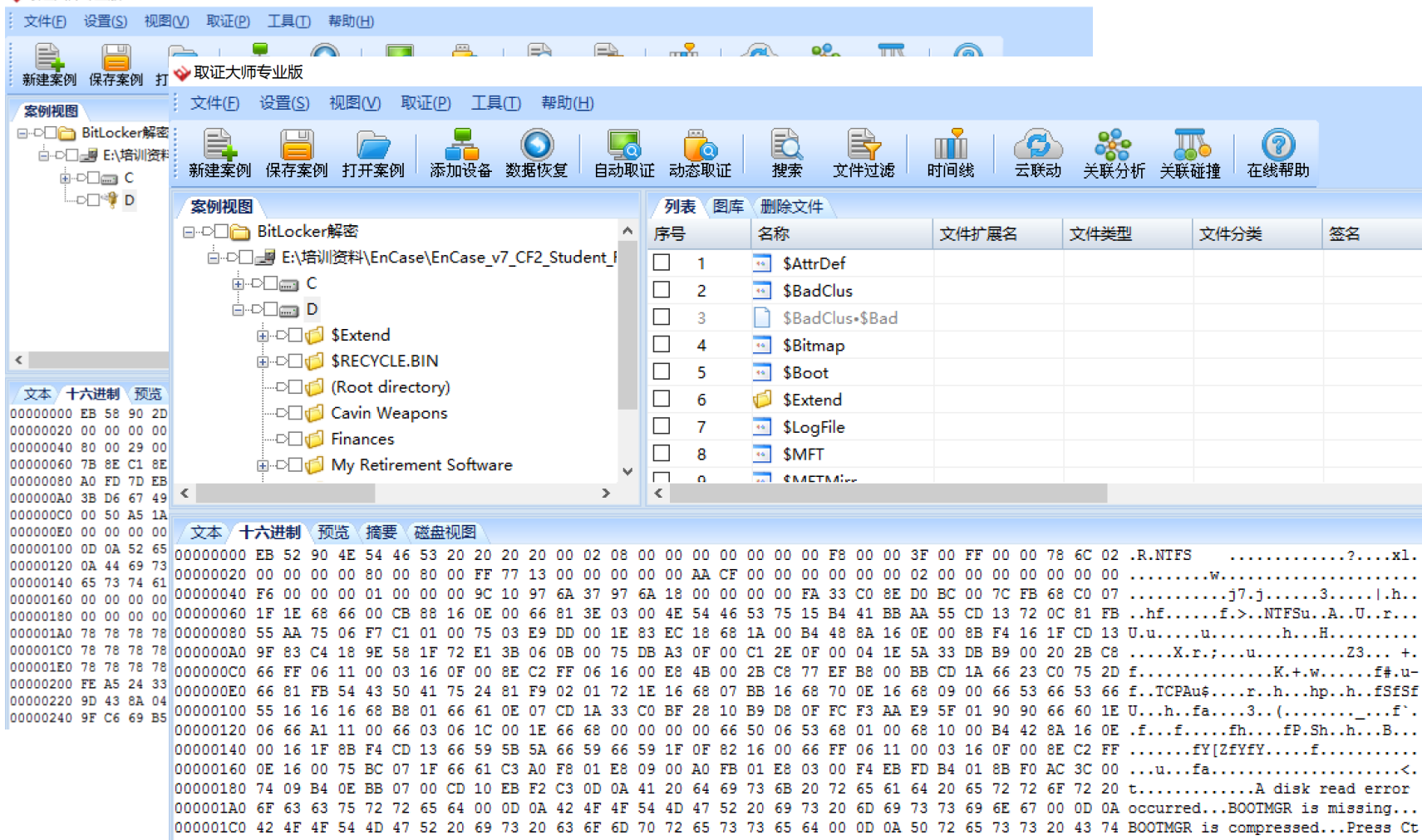
- 所有数据存在于单个加密容器文件中，使用简单。
- 数据迁移非常方便，只需移动加密容器文件。
- 支持各种高强度加密算法，破解难度极大。

基于加密密钥或用户密码的解密



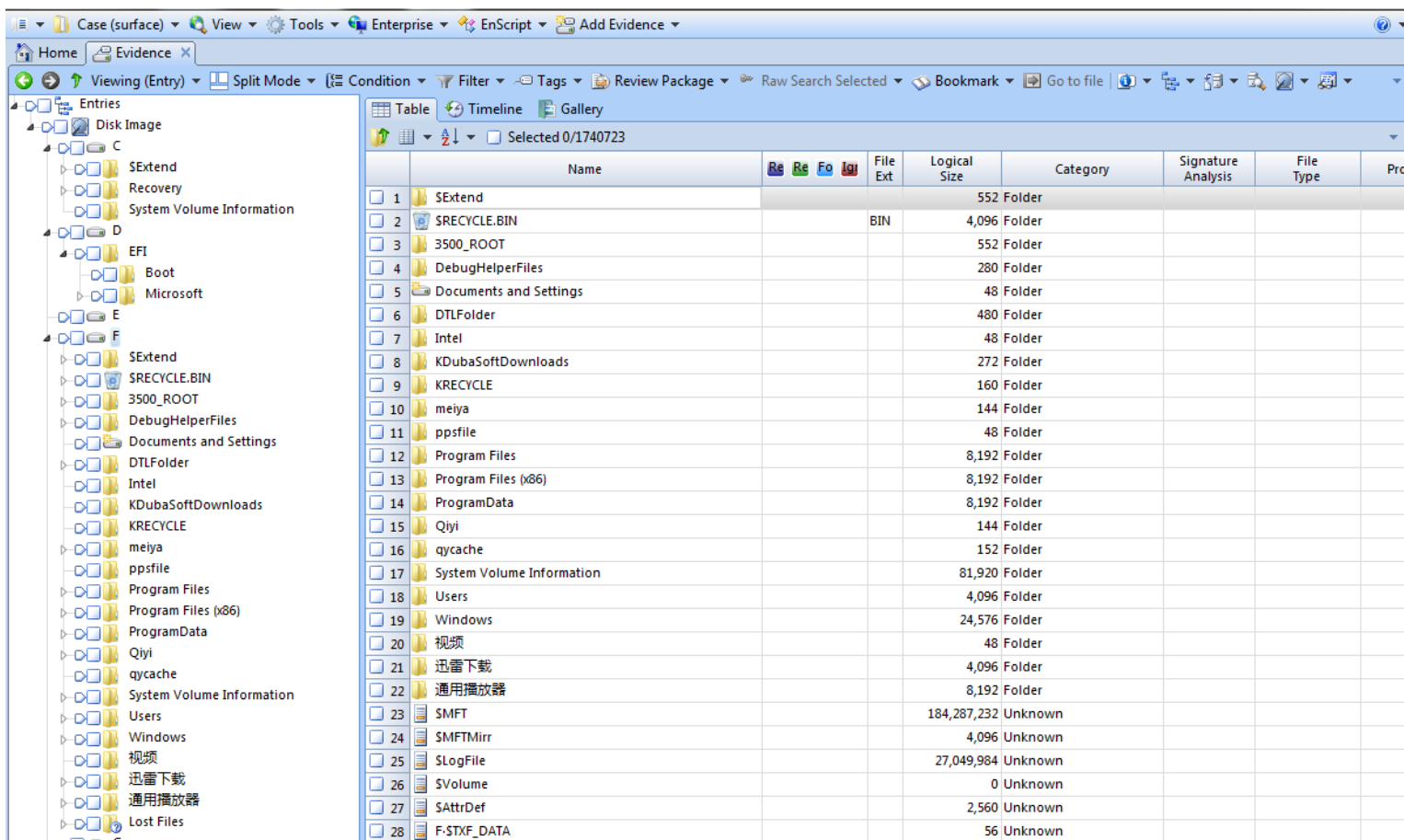
- 通过搜索移动存储介质及云平台中的加密密钥或用户帐户密码等信息进行磁盘解密。
 - BitLocker (密码、本地密钥文件、OneDrive保存的密钥文件)
 - FileVault (密码、iCloud保存的密钥文件)
 - SafeBoot (企业内部服务器获得解密密钥)





基于加密密钥或用户密码的解密

- Surface平板电脑的Bitlocker加密比较特殊，可以默认自动加密，然后通过特定取证软件（如EnCase）可以直接解密。



| | Name | Re | Re | Re | Re | File Ext | Logical Size | Category | Signature Analysis | File Type | Pro |
|----|---------------------------|----|----|----|----|----------|--------------|----------|--------------------|-----------|-----|
| 1 | \$Extend | | | | | | 552 | Folder | | | |
| 2 | \$RECYCLE.BIN | | | | | BIN | 4,096 | Folder | | | |
| 3 | 3500_ROOT | | | | | | 552 | Folder | | | |
| 4 | DebugHelperFiles | | | | | | 280 | Folder | | | |
| 5 | Documents and Settings | | | | | | 48 | Folder | | | |
| 6 | DTLFolder | | | | | | 480 | Folder | | | |
| 7 | Intel | | | | | | 48 | Folder | | | |
| 8 | KDubaSoftDownloads | | | | | | 272 | Folder | | | |
| 9 | KRECYCLE | | | | | | 160 | Folder | | | |
| 10 | meiya | | | | | | 144 | Folder | | | |
| 11 | ppsfile | | | | | | 48 | Folder | | | |
| 12 | Program Files | | | | | | 8,192 | Folder | | | |
| 13 | Program Files (x86) | | | | | | 8,192 | Folder | | | |
| 14 | ProgramData | | | | | | 8,192 | Folder | | | |
| 15 | Qiyi | | | | | | 144 | Folder | | | |
| 16 | qycache | | | | | | 152 | Folder | | | |
| 17 | System Volume Information | | | | | | 81,920 | Folder | | | |
| 18 | Users | | | | | | 4,096 | Folder | | | |
| 19 | Windows | | | | | | 24,576 | Folder | | | |
| 20 | 视频 | | | | | | 48 | Folder | | | |
| 21 | 迅雷下载 | | | | | | 4,096 | Folder | | | |
| 22 | 通用播放器 | | | | | | 8,192 | Folder | | | |
| 23 | SMFT | | | | | | 184,287,232 | Unknown | | | |
| 24 | SMFTMirr | | | | | | 4,096 | Unknown | | | |
| 25 | SLogFile | | | | | | 27,049,984 | Unknown | | | |
| 26 | SVolume | | | | | | 0 | Unknown | | | |
| 27 | SAttrDef | | | | | | 2,560 | Unknown | | | |
| 28 | F-STXF_DATA | | | | | | 56 | Unknown | | | |

基于物理内存镜像的解密



文件(F) 设置(S) 视图(V) 取证(P) 工具(T) 帮助(H)

新建案例 保存案例 打开案例 添加设备 数据恢复 自动取证 动态取证 搜索 文件过滤 时间线 云联动 关联分析 关联碰撞 在线帮助

案例视图

TrueCrypt——内存镜像

- E:\培训资料\@Training\Memory Analysis\mydata-decrypt-ed-partition-0.tc
 - \$Extend
 - (Root directory)
 - 丢失的文件

列表 图库 删除文件

| 序号 | 名称 | 文件扩展名 | 文件类型 | 文件分 |
|-----------------------------|----------------------|-------|------------|-----|
| <input type="checkbox"/> 15 | (Root directory) | | | |
| <input type="checkbox"/> 16 | (Root directory)*... | | | |
| <input type="checkbox"/> 17 | 01300015.jpg | jpg | JPEG图片(标准) | 图片 |
| <input type="checkbox"/> 18 | 02170006.jpg | jpg | JPEG图片(标准) | 图片 |
| <input type="checkbox"/> 19 | 02180017.jpg | jpg | JPEG图片(标准) | 图片 |
| <input type="checkbox"/> 20 | 100_0264.JPG | JPG | JPEG图片(标准) | 图片 |
| <input type="checkbox"/> 21 | 100_0303.JPG | JPG | JPEG图片(标准) | 图片 |
| <input type="checkbox"/> 22 | 100_0304 crop.b... | bmp | Windows位图 | 图片 |
| <input type="checkbox"/> 23 | 100_0307.JPG | JPG | JPEG图片(标准) | 图片 |

文本 十六进制 预览 摘要 磁盘视图

电子数据取证技术交流



电子数据取证推荐书籍



清华大学出版社《电子数据取证》- 2015年出版

- 涵盖最新电子数据取证技术及法规；
- 20位国内电子数据取证、信息安全专家联合编写





中国互联网安全大会



360互联网安全中心

谢谢大家