doi 10.3969/j.issn.1671-1122.2014.09.049

FileVault2 加密分区离线解密技术及其取证应用

蓝朝祥，沈长达，钱镜洁

（厦门市美亚柏科信息股份有限公司，福建厦门 361008）

摘　要：苹果公司推出 OS X 10.3（Panther）系统时，引入了 FileVault 磁盘加密功能。在最新发布的 OS X Lion 系统中，引入了全新加密方式 FileVault2。FileVault2 使用全磁盘、AES-XTS 128 加密来帮助保护数据安全。针对当前大部分的取证软件都不支持对经过 FileVault2 加密的磁盘进行数据解析问题，文章首先讨论了 FileVault2 的加密原理，接着提出了离线解密的方法，并在此基础上设计了 FileVault2 取证工具，使得加密磁盘摆脱了目标数据源对 Mac OS 系统的依赖，能够在没有 Mac OS 系统的环境下对经过 FileVault2 加密的磁盘进行取证。实践表明此离线解密方法丰富了加密数据的取证项。

关键词：加密磁盘；加密；解密

中图分类号：TP309　　文献标识码：A　　文章编号：1671-1122（2014）09-0211-03

The Method of Decrypting FileVault2 Offline and Applications in Forensics

LAN Chao-xiang, SHEN Chang-da, QIAN Jing-jie

(*Xiamen Meiya Pico Information Co.,Ltd., Xiamen Fujian* 361008, *China*)

Abstract: Apple launched OS X 10.3 (Panther) system, the introduction of a FileVault disk encryption feature. In the latest release of OS X Lion system, the introduction of a new encryption FileVault2. FileVault2 uses full disk, AES-XTS 128 encryption to help keep data secure. Given that most of forensic soft can't achieve forensics quickly on FileVault2 encrypting disk. This paper first discusser encrypting principles of the FileVault2, then puts the FileVault2 decryption method offline. And on this basis, designs the decrypting FileVault2 tools, which works independent of the operating system on the target data source and able to in the absence of Mac OS system environment through FileVault2 encrypted disk forensics. Practice shows that offline decryption method enriches the evidence items.

Key words: encrypting disk; encrypt; decrypt

0 引言

随着各种信息安全事件曝光，大家对使用的数据安全保护意识越来越强。各种对应的数据保护技术应运而生，如 Windows 的 BitLocker 加密技术。本文主要研究了苹果产品 Mac OS X 中的 FileVault2 加密技术。在 OS X Lion 中的 FileVault2 加密技术采用全磁盘加密技术，支持实时加解密，并且还可以指定用户可见。用户只需记住登录密码即可访问加密数据，免去了记忆复杂的加密密码的烦恼，同时也达到对数据加密强度的需求。但是苹果公司并没有公布 FileVault2 相关的源码和文档，所以目前加密的数据在离开 Mac 系统后，不能通过恢复密钥或者用户登录密码来解密加密数据，这些特性极大影响了电子数据取证的进行。因此，研究如何在脱离了 Mac OS 系统情况下，通过对 FileVault2 加密卷进行解密并设计出对应的取证工具，对加密数据取证具有重大意义。

收稿日期：2014-08-06

作者简介：蓝朝祥（1987-），男，福建，工程师，本科，主要研究方向：文件系统解析；沈长达（1989-），男，福建，工程师，本科，主要研究方向：文件系统解析及数据恢复；钱镜洁（1984-），女，江苏，工程师，硕士，主要研究方向：数据存储和恢复。

1 基本概念

FileVault2 是 Mac OS X 10.7 引入用来加密 Macintosh 磁盘卷的一种方法，加密和解密都可以实时进行。FileVault2 通过系统偏好设置中的安全性与隐私进行管理。单击安全性与隐私面板中的 FileVault 标签，便可以启用或停用 FileVault2。在启动 FileVault2 时，系统会生成一个 24 字符的恢复密钥，此密钥是备用的解锁方式，即使用户密码丢失，也可以使用此恢复密钥访问加密卷。在设置中，还可指定其他用户可见。

2 FileVault2 加密机制

在系统启用 FileVault2 后，根据命令查看系统磁盘信息可知主卷的文件系统由本机的 HFSPlus 转换为 CoreStorage[2]（加密）类型。采用 AES-XTS 128[1] 位加密算法来加密全磁盘。

2.1 AES-XTS加密算法简介

AES-XTS 是一种使用两个密钥加密的加密方法[3]。key1（master key 主密钥）和 key2（tweak 密钥）AES-XTS 加密算法结构如图 1 所示。

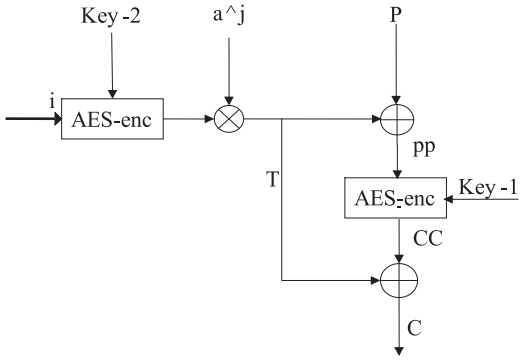

图1 AES-XTS加密算法

AES-XTS 加密算法特点如下：

1）磁盘块（如一个扇区）分成多个密文块（如 AES-128[1] 的 128bit）；

2）各个密文块之间独立（没有 CBC 那样的依赖关系）；

3）密文块的加密输入包含了 index 信息（扇区号和块号）。

2.2 加密机制简析

除了生成一个加密的主卷，加密的同时还会生成一个新的逻辑卷，通常被称为 Recovery HD。这个新的逻辑卷中存储了加密卷的主密钥（master key）。在这个新生成的逻辑卷中有一个 AES-XTS 加密的文件 EncryptedRoot.plist..wipekey。其中 KEY1 在主卷头（加密的主卷）中，KEY2 为 128 位为零的加密字段（即 16 个零字节），加密使用的主密钥就存储在此文件中。Tweak key 也是由这个主密钥推导出来的，故解密此文件获取主密钥是解密整个卷的关键步骤[3]。

新的 Recovery HD 卷包含了一系列的新文件，包括新的启动加密卷的 EFI 启动代码。

3 FileVault2 离线解密技术分析

在了解了 FileVault2 加密的流程之后，可以根据具体方法得到相对应的解密流程。将加密后的磁盘用外部工具加载观察，从磁盘结构来看，加密后的硬盘与加密前硬盘发生了重大的变化。主卷的分区由 HFSPlus 文件系统变为一个 CoreStorage 管理的加密卷，并增加了一个 Recovery HD 分区卷。通过对加密数据研究和相关资料文献的阅读，得知加密卷的卷头存储了解密所需的各种相关参数[4]。图 2 为 FileVault2 解密流程。

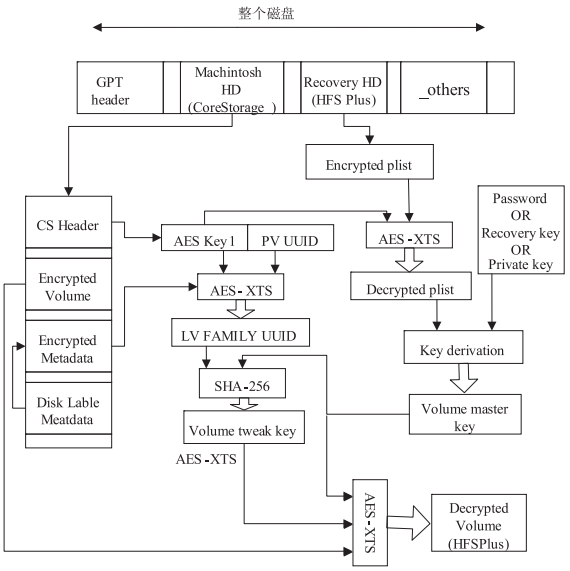

图2 FileVault2解密流程

根据对加密卷数据分析可得加密卷的头部主要包含有如下信息：

卷头部签名、块大小、卷大小、元数据大小、第一个元数据块块号、第二个元数据块块号、第三个元数据块块号、第四个元数据块块号、加密方法、逻辑卷 ID（用于解密加密的密钥文件）、物理卷 ID[5]。

解密步骤如下：

1）识别到 FileVault2 加密卷和存储的需要提取的用户密码生成的主密钥信息或者恢复令牌的 EncryptedRoot.plist.wipekey 文件 ；

2）解密通过文件系统解析获得的 EncryptedRoot.plist.wipekey 文件后，提取存储的密钥信息 ；

3）输入用户登录密码或者恢复密钥，验证步骤 2）中提取到的密钥信息是否正确 ；

4）验证正确后根据用户密码或者恢复密钥及加密的 EncryptedRoot.plist.wipekey 文件中存储的密钥信息生成主密钥和 tweak key ；

5）用生成的两个解密密钥信息（key1 和 key2）及加密卷数据进行解密，生成解密数据即完成解密。

用取证工具或其他可以解析 HFSPlus 文件系统的工具对解密数据进行解析，可以验证解密结果是否正确。

4 FileVault2 取证工具设计与实现

在了解了 FileVault2 的离线解密方法的基础上设计实现对 FileVault2 加密卷解密的取证工具 [6]。此工具主要包括以下几个模块，模块交互如图 3 所示。

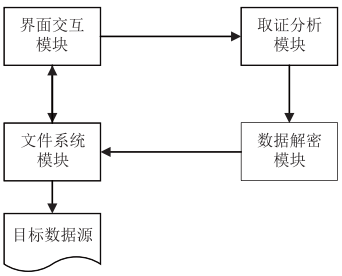

图3 模块交互

1）文件系统模块。负责加载数据源，读取数据源。该模块能够识别加载数据源是否为 FileVault2 加密分区 ；能够识别出 Recovery HD 分区，并且能在 Recovery HD 分区识别出存储密钥的加密文件。

2）数据解密模块。负责数据解密，在文件系统模块的基础上，根据对加密机制的研究，得出对加密卷的解密方法实现。

3）取证分析模块。负责对解密后的数据进行相关信息（如系统信息、最近访问记录）的取证分析和证据提取工作。

4）界面交互模块。负责接收用户输入用户登录密码或者加密卷恢复密钥以及解密成功与否的相关提示，并对解密后的数据进行相关展示，方便用户进行取证分析。

图 4 为 FileVault2 加密后取证工具加载后的数据信息 ；通过新的解密工具加载解密后数据信息如图 5 所示 ；图 6 为解密后的加密卷中的图片视图信息。

图4 解密前数据

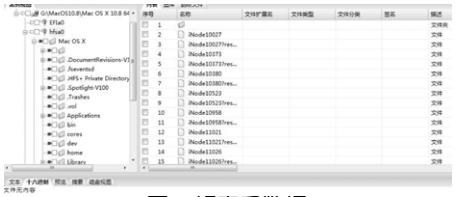

图5 解密后数据

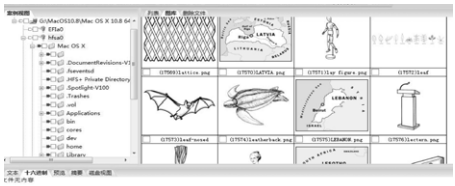

图6 解密后图片视图

5 结束语

本文从分析 FileVault2 的加密原理出发，结合对 AES-XTS 解密算法的了解和实际加密数据的特征分析及实际解析数据的实践情况下，设计实现了 FileVault2 的离线解密功能，使得在 Windows下分析 Mac 加密卷信息成为可能。经测试，此工具支持 Mac OS X 10.7 及其以上版本中的 FileVault2 加密卷的解密。但此方法需要在已知用户登录密码或者恢复密钥的情况下才能解析，目前还尚未达到能够自动搜索检测加密密码或者密钥，自动识别并解密的情况，这一情况有待继续研究完善。（责编 潘海洋）

参考文献

[1] RFC3394, Advanced Encrypttion Standard (AES) Key Wrap Algorithm[S], Network Working Group, J.Schaad, September 2002.

[2] STEPHEN.Mac OS X Lion Adds CoreStorage, a Volume Manager[EB/OL] http://blog.fosketts.net/2011/08/04/mac-osx-lion-corestorage-volume-manager/.html, 2011-8.

[3] RFC2104，HMAC:Keyed-Hashing for Message Authentication[S], IETF Network Working Group, P Jones February 1997.

[4] 杨璞，赵庸，吴鸿伟，等 . 电子数据勘察取证与鉴定（信息加解密技术）[M]. 北京 ：中国人民公安大学出版社，2012.

[5] 韩水玲，马敏，王涛，等 . 数字证书应用系统的设计与实现 [J]. 信息网络安全，2012，(09) ：43-45.

[6] 夏伟，李晖，崔彦平 . 移动网银安全研究 [J]. 信息网络安全，2012，(10) ：64-67.