

**MacOS文件移动**

**译者：丶来年花落   
原文链接：**[**https://forensic4cast.com/2016/10/macos-file-movements/**](https://forensic4cast.com/2016/10/macos-file-movements/)

**原文作者：Lee Whitfield**

** **

**微信公众号：看雪iOS安全小组 我们的微博：weibo.com/pediyiosteam**

**我们的知乎：zhihu.com/people/pediyiosteam**

**加入我们：看雪iOS安全小组成员募集中：http://bbs.pediy.com/showthread.php?t=212949  
[看雪iOS安全小组]置顶向导集合贴： http://bbs.pediy.com/showthread.php?t=212685**

**MacOS文件移动**

在数字化探索的环境下我们将不断见到越来越多的Apple设备。因此，我将定

期尽我所能在这方面增长我的知识。我经常向 Sarah Edwards 寻求帮助。与

那些所谓的在 Apple store 的不同，她确实是一个天才。不管怎样...

我们最倾向于调查的工作类型是知识产权盗窃。通常情况下，这些案例集中发

生在前员工使用外部 USB 设备从他们的工作用计算机上传输数据时。无论数

据属于公司还是个人都由法院决定，我的重点在于这些是什么数据。

我一直在做一些测试来试图说明 MacOS 系统上的文件移动将如何影响目的地

主机的元数据。我想我应分享我的发现。这是一项正在进行的工作，因为似乎

还有一些我还没有想明白的不同情况。

HFS+ 有五个不同的日期和时间戳。 如下：

* 创建
* 修改（最后写入）
* 访问
* 记录更改
* 添加日期

创建，修改和访问非常直接。记录更改是指在目录中更改文件的元数据（类似

于 NTFS 中的 $ MFT ）。

“添加日期”是一个相对较新的发现。这是指一个文件被复制或移动到其当前位置。如果一个文件存在于 HFS+ 卷上，并且它被移动到该卷上的另一个文件夹，则该元数据值被更新以反映该移动。如果您使用 X­Ways Forensic ，此值将填充在“ Created² ”字段下。在HFS+上创建文件

**在HFS+上创建文件**

在HFS+卷上创建新文件时，日期和时间如下：

* 创建 ­ 创建时间
* 修改 ­ 创建时间
* 访问 ­ 创建时间
* 记录更改 ­ 创建时间
* 添加日期­ 未填充

**在HFS+上创建文件副本**

在 HFS+ 卷上创建文件副本（右键点击文件并在选项菜单中选择“创建文件副

本”）时，日期和时间如下：

* 创建 ­ 从源文件继承
* 修改 ­ 从源文件继承
* 访问 ­ 创建副本时间
* 记录更改 ­ 创建副本时间
* 添加日期­ 创建副本时间

**在HFS+上修改文件**

当在 HFS+ 卷上修改（编辑）文件时，日期和时间将受到如下影响：

* 创建 ­ 不变
* 修改 ­ 修改时间
* 访问 ­ 修改时间
* 记录更改 ­ 修改时间
* 添加日期­ 不变

这里要指出的是“添加日期”值。 如果复制文件，然后编辑该重复文件的内

容，“添加日期”字段仍将显示创建副本的日期和时间。所以这里你将有同一个

文件的原始创建时间，副本创建时间和修改时间。

**HFS+到HFS+**

如果用户将文件从一个 HFS+ 卷复制或移动到另一个 HFS+ 卷，则在目标文

件上日期和时间将受到以下方式的影响：

* 创建 ­ 从源文件继承
* 修改 ­ 从源文件继承
* 访问 ­ 更新为复制时间
* 记录更改 ­ 更新为复制时间
* 添加日期­ 更新为复制时间

归属于文件的所有其他元数据都存储在存储在 HFS+ 文件系统中。

**HFS+到ExFAT**

ExFAT 只有3个时间戳。 如果用户将文件从 HFS+ 卷复制或移动

到 ExFAT ，则在目标文件上日期和时间将受到以下方式的影响：

* 创建 ­ 从源文件继承
* 修改 ­ 从源文件继承
* 访问 ­ 更新为复制时间

有更多的行为而不是简单地更新文件的时间戳。 这将在稍后的元数据部分中

讨论。

**HFS+到FAT32**

像 ExFAT 一样有3个时间戳，但访问时间只能归属于一天。 如果用户将文件

从 HFS+ 卷复制或移动到 FAT32 ，则在目标文件上日期和时间将受到以下方

式的影响：

* 创建 ­ 从源文件继承
* 修改 ­ 从源文件继承
* 访问 ­ 更新为复制时间

有更多的行为而不是简单地更新文件的时间戳。 这将在稍后的元数据部分中

讨论。

**ExFAT或FAT32到HFS+**

如果用户将文件从 ExFAT 或 FAT32 卷复制或移动到 HFS+ ，则在目标文件

上日期和时间将受到以下方式的影响：

* 创建 ­ 从源文件继承
* 修改 ­ 从源文件继承
* 访问 ­ 更新为复制时间
* 记录更改 ­ 更新为复制时间
* 添加日期­ 更新为复制时间

**原数据和“.\_”文件**

因为存储在 HFS+ 卷中的文件通常比其他卷（扩展属性等）拥有大得多的元

数据，因此从 HFS+ 卷复制到 ExFAT 或 FAT32 卷的任何文件也将具有

由 MacOS 创建的匹配隐藏文件 。例如，如果我将一个名为“ me.jpg ”的文

件从 HFS+ 卷复制到 ExFAT 或 FAT32 卷，也会创建一个隐藏文件。 这个隐

藏的元文件将命名为“ .\_me.jpg ”。 这样的文件的时间戳将如下：

* 创建 ­ 创建时间
* 修改 ­ 创建时间
* 访问 ­ 创建时间

这意味着即使通过编辑或访问文件来更改其他时间戳元数据字段，我们仍然可

以通过查看关联元文件的的创建日期来知道文件被复制到 ExFAT 或 FAT32

卷的确切日期和时间。

**关于Mac OS访问时间的注释**

HFS+ 卷上访问时间有点奇怪。显然，如果您选择一个文件并从选项菜单中

单击“获取信息”，访问时间字段将被更新。但是，打开文件且还未保存（？）

时，访问时间不会更新。

然而，如果您使用“获取信息”或打开一个 ExFAT 或 FAT 文件（且暂不保

存），访问的元数据字段会更新。

相关元文件也更新了其访问日期和时间。