第5章 Windows取证

Windows是由微软公司开发的图形化操作系统，常见的Windows操作系统主要包括Windows XP/7/8/8.1/10/11以及Windows Server 2003/2008/2012/2016/2019/2022，前者主要应用在PC和平板计算机上，后者则主要应用在服务器设备上。截至2022年10月，适用于桌面设备的Windows的最新版本号是Windows 11，版本号是21H2。

目前，随着Windows的更新迭代，Windows 10/11已经占据了Windows系列主要的市场份额，本章的内容也主要是基于这两者。同时，旧版本的Windows系统和新版本的Windows系统也会有一些不同点。以回收站为例，在Windows XP及以前的版本中，其名称为Recycler；在Windows 7中，其名称为Recycled；而在Windows 10及以上的版本中，其名称则为$Recycle.Bin。本章内容主要包括Windows系统重要的痕迹文件、注册表、事件日志以及内存取证。

5.1 重要的痕迹文件

在很多英文文献中，经常会使用Artifacts表示数字取证中最具有价值的、值得调查人员关注的数据。通常此类数据是由操作系统或应用程序本身自动创建的，有些是人为操作之后遗留下来的，还有些会随着用户的活动而不断更新。例如，当用户在Windows中安装一个应用程序时，操作系统会创建该程序的快捷方式(lnk文件)；当用户运行该应用程序时，操作系统会创建该应用程序所对应的预读取文件(prefetch文件)。此外，操作系统和文件系统也会生成其他的记录和数据。

在中文环境中，由于并没有一个精确的词汇对应Artifacts，因此，业界通常会使用“痕迹文件”一词表示Artifacts，用来指代取证中值得关注的重要数据。上述快捷方式和预读取文件便是重要的痕迹文件，因为这些数据能够揭示程序或者文件的被打开或运行的痕迹，也能够揭示一定时间内用户的行为。因此，在实际的取证工作中，取证调查人员应重点关注Windows系统中的这些痕迹文件。

5.1.1 卷影复制

卷影复制(Volume Shadow Copy，VSC)是微软公司提供的一个自动或手动备份服务，是一种对卷中文件创建快照的方法。

还原点是在某些时刻操作系统所创建的快照，这些快照能够帮助操作系统恢复特定时刻的工作状态，以解决计算机运行缓慢或停止响应的问题。当 Windows 操作系统出现问题损坏时，操作系统可能会提示用户通过系统还原点进行恢复。还原点可以由用户手动创建，也可以由系统在重大系统事件（如系统更新、安装程序）之前自动创建。默认情况下还原点功能处于启用状态，并且每天自动生成一个快照。

当用户创建还原点时，操作系统会触发卷影复制服务，卷影复制服务是 Windows XP 及以后的操作系统具备的一项功能，操作系统通过它为还原点创建数据快照；或者说，卷影复制服务为还原点提供源数据，这些源数据便是卷影副本，并且每个还原点都有其对应的卷影副本。卷影复制服务只支持 NTFS 格式的分区或卷。

在数字取证中，通过分析卷影副本，取证调查人员能够发现大量有价值的取证信息，因为卷影副本中可能包含着很多已删除文件的副本，如已删除的 BitLocker 密钥等信息。但是，卷影副本中不会包含未分配簇、松弛扇区和休眠文件等内容。取证调查人员可以使用 X-Ways Forensics、猎痕鉴证大师或 ShadowExplorer 等工具实现对卷影副本的解析。

5.1.2 回收站

回收站是 Windows 操作系统中用来暂时保存已删除数据的一个文件夹，默认是系统和隐含属性。当用户删除一个文件后，该文件会默认被放入并一直保存在回收站中。用户可以通过“还原”命令将回收站中的文件放回原处，或选择“清空回收站”命令将数据彻底删除。在一些涉及企业内部调查的案件中，经常出现离职员工窃取并故意删除公司数据的情况。那么，是否能知道一个人在什么时间删除了哪些数据呢？通过对回收站进行细致的分析，取证调查人员有机会发现被删除的数据以及删除时间。

在 Windows XP 操作系统中，回收站的路径为 X:\RECYCLER，X 代表驱动器的盘符。在 RECYCLER 文件夹下包含多个以 SID 命名的子文件夹，这些不同的子文件夹分别存放着不同的用户删除的内容。一旦文件被移入回收站，这些文件的名字就会被修改为 DC1.*、DC2.*、DC3.* 等，或者被修改为 D*、* 并保留原始扩展名。在 RECYCLER 文件夹中，存在一个名为 INFO2 的文件，该文件中记录了被删除文件的原始路径、删除时间以及文件大小等信息。

从 Windows Vista 开始直至 Windows 11 操作系统，回收站的路径均为 X:\$Recycle.Bin，X 代表驱动器的盘符。在 $Recycle.Bin 文件夹下包含多个以 SID 命名的子文件夹，存放着不同用户删除的不同数据。不同于 Windows XP 回收站的文件命名规则，在 $Recycle.Bin 文件夹下，每一个被单独删除的文件都会对应两个文件。当 Windows 删除一个文件时，会首先创建一个文件，用于记录被删除文件的原始名称、大小、路径和删除时间。该文件名的命名规则为“$I+6 位由字母和数字组合的随机数+原始文件扩展名”。然后，回收站中原始文件的文件名会被更改，改名规则为“$R+相同的 6 位随机数+原始扩展名”。因此，$I* 文件中记录的是被删除文件的原始信息，$R* 文件则是被删除的原始文件。两个文件的后 6 位随机数相同。$I* 文件需要使用专业的工具解析，取证调查人员可以使用 WinHex、RBCmd、$I_Parse 等工具实现对 $I* 文件的解析。

5.1.3　缩略图

Windows 操作系统为了方便用户能够更加快速地浏览如 JPG、PNG、AVI 等多媒体文件的内容，从 Windows XP 开始新增了缩略图功能。Windows XP 将缩略图固定存储于每个文件夹中的 thumbs.db 文件中。Windows 7 则取消了 thumbs.db 方式，而将缩略图文件存储在 C:\Users\<UserName>\AppData\Local\Microsoft\Windows\Explorer 文件夹下的 thumbcache_*.db 文件中，其中 * 表示缩略图的尺寸，分别为 32、96、256、1024 等，即用户在文件资源管理器中浏览文件时选择大图标、小图标等不同查看模式的结果。Windows 10 及以后的版本依然采取同样的缩略图存储规则，但增加了 16、48、768、1280、1920 等更多的缩略图尺寸。

不同版本的 thumbcache_*.db 文件的文件签名稍有不同。Windows 10 中缩略图文件的头部特征字节的值为 0x20，如图 5-1 所示。Windows 8.1 中该值为 0x1F，Windows 7 中该值则为 0x15。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	43	4D	4D	4D	20	00	00	00	06	00	00	00	00	00	00	00	CMMM
00000010	18	00	00	00	9C	C6	9D	01	43	4D	4D	4D	6A	62	01	00	œÆ CMMMjb
00000020	0F	07	36	EC	C8	67	C3	EE	20	00	00	00	00	00	00	00	6ìÈgÃî

图 5-1　Windows 10 中缩略图文件的文件头

Windows 缩略图的特性在于其不会随着原文件的丢失而被删除，即一旦操作系统中产生了一个图片文件的缩略图信息，那么即使该图片的原文件被删除了，或者存储该图片的外置存储设备被移除了，该图片的缩略图信息仍然可能存在于 thumbcache_*.db 文件中。这一特性对数字取证的作用是不言而喻的，尤其是在调查涉及恐怖主义或者淫秽色情的案件时，通过分析缩略图或许能够更有效地获取案件线索。2020 年，某检察院司法鉴定中心在对一起案件中的手机检材进行分析时，获取了 20 余张图片的缩略图。虽然没有在涉案手机中获取这些缩略图所对应的原始图片，但取证调查人员仍怀疑这些原始图片是犯罪嫌疑人在性侵女童时拍摄的。随后，在对台式计算机的取证调查中，取证调查人员发现并解密了一个 EFS 加密的文件夹，该文件夹中包含 20 余张图片和一段性侵视频，这些图片便是上述缩略图所对应的原始图片文件。取证调查人员通过进一步检验这些图片的元数据信息，确定了这些图片的拍摄设备和拍摄时间等信息，并最终证明了检材手机为最初拍摄设备以及原始图片和视频被复制到台式计算机后在手机上被删除的事实。

Thumbcache_*.db 文件需要借助专业的取证工具才能查看，取证调查人员可以使用 X-Ways Forensics 或 Thumbcache Viewer 等工具分析缩略图文件。图 5-2 为使用 Thumbcache Viewer 查看 Thumbcache_*.db 获取的信息。

如图 5-2 所示，通过查看 Thumbcache_*.db，取证调查人员只能获取缩略图的文件名（一串哈希值）等信息，却无法获取缩略图所对应的原始文件的路径信息。如果需要进一步分析缩略图所对应的原始路径等信息，则需要结合 Windows.edb 文件一同分析。Windows.edb 是 Windows 搜索服务的数据库文件，可以提供内容索引、属性缓存以及文件、电子邮件和其他内容的搜索结果，该文件位于 C:\ProgramData\Microsoft\Search\Data\Applications\Windows 文件夹中。在分析过程中，在 Thumbcache Viewer 中选择

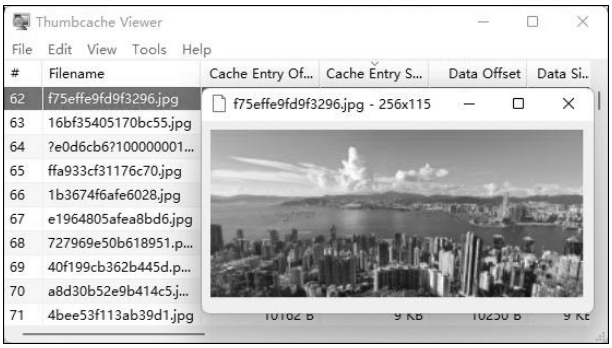

图 5-2　使用 Thumbcache Viewer 查看 Thumbcache_*.db 获取的信息

Tools→Map File Paths 命令，然后选择相应的 Windows.edb 文件，单击 Scan 按钮开始扫描。扫描结束后，程序便会列出各个缩略图的原始路径信息。

5.1.4　快捷方式

快捷方式文件的扩展名为 lnk(或 LNK)，其主要作用是方便用户快速调用不同位置的其他资源。在普通用户看来，快捷方式文件只是一种普通的文件，可有可无；但在数字取证中通过对快捷方式的分析能够获得极有价值的线索。快捷方式中包含所指向的目标文件的位置和大小等信息。大部分快捷方式文件是用户在打开文件时操作系统产生的，这些 LNK 文件通常存储在下列位置：

C:\Documents and Settings\%USERNAME%\Recent(Windows XP)

C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent(Windows 7-10)

上述位置的快捷方式文件不会被自动删除。如果人为删除某个文件的快捷方式，在当前计算机运行期间，即使再次打开原来的文件也不会再产生该文件所对应的 LNK 文件，除非将该文件重命名或者在下一次计算机运行期间重新打开该文件。

有些快捷文件是由用户或者应用程序生成的，通常位于桌面或者 Windows 启动菜单中，这些快捷方式通常保存在下列位置：

C:\Users\<UserName>\Desktop\

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\

这些 LNK 文件不会被自动删除，只能在用户不需要的时候主动删除。

最近打开的 Office 文档也会产生相应的 LNK 文件。这些文件主要存储在下列位置：

C:\Users\<UserName>\AppData\Roaming\Microsoft\Office\Recent(Windows 7-10)

快捷方式文件的特性在于，不会因为它指向的目标文件丢失而丢失。例如，如果用户曾经在计算机中连接过一个 USB 硬盘，并打开过这个硬盘中的某个文件，那么通过分析与这个文件关联的 LNK 文件，取证调查人员便能够获取该文件的路径和时间等基本信

息。此外，通过对快捷方式文件的解析，能够获取下列信息：

- 目标文件的属性、大小。
- 目标文件的创建时间、修改时间和访问时间。
- 目标文件所在的卷的名字、序列号、类型、ID。
- 目标文件的原始路径、相对路径。
- 目标文件所在的主机名、MAC 地址、时间戳信息。
- NetBios 名称(存在于部分 LNK 文件中)。

……

在数字取证中，除了使用 X-Ways Forensics 解析快捷方式文件以外，还可以使用 LECmd 和 LinkParser 等工具。

5.1.5　跳转列表

跳转列表(jump list)是从 Windows 7 开始引入的一项新功能。当用户打开应用程序，并右击该应用程序在任务栏上的图标后，会显示出一个动态的列表，这便是跳转列表。

图 5-3　Google Chrome 浏览器的跳转列表

跳转列表包含的数据类似于快捷方式，能够直接跳转到经常使用的文件或目录中。相较于普通的快捷方式文件，跳转列表中存储着更多的信息，这一特性或许能够更好地帮助取证调查人员分析用户的行为习惯等。例如，在图 5-3 所示的 Google Chrome 浏览器的跳转列表中，记录着用户最近访问的记录和最频繁访问的记录。同样，在文件资源管理器和 WPS 等应用程序的跳转列表中也记录着用户最近访问的文件等信息。

Windows 中存在两种类型的跳转列表文件：一种跳转列表文件的扩展名是 automaticDestinations-ms，此类跳转列表文件是用户打开文件或者应用程序时自动创建的，存储位置为 C:\Users\<UserName>\AppData\Roaming\Microsoft\Office\Recent\AutomaticDestinations；另一种跳转列表文件的扩展名为 customDestinations-ms，是用户固定文件或者应用程序时创建的，存储位置为 C:\Users\<UserName>\AppData\Roaming\Microsoft\Office\Recent\CustomDestinations。

跳转列表文件的命名规则是“App ID(应用程序 ID)＋扩展名”。每一个应用程序都有固定的 App ID，且不同版本应用程序的 App ID 可能会不同。表 5-1 为常见的 App ID。

表 5-1　常见的 App ID

App ID	描　　述
fb3b0dbfee58fac8	Microsoft Office Word 365 x86
d00655d2aa12ff6d	Microsoft Office PowerPoint x64

续表

App ID	描　　述
b8ab77100df80ab2	Microsoft Office Excel x64
69639df789022856	Google Chrome 86.0.4240.111
6824f4a902c78fbd	Mozilla Firefox 64.0
ccba5a5986c77e43	Microsoft Edge(Chromium)
8eafbd04ec8631ce	VMware Workstation x64
ae6df75df512bd06	Windows Media Player

在数字取证中，取证调查人员可以使用 X-Ways Forensics 或 JumpList Explorer 分析跳转列表文件。图 5-4 是使用 JumpList Explorer 查看 8eafbd04ec8631ce.automaticDestinations-ms 的结果。从中可以看出，每个跳转列表文件中可能包含多个条目，这些条目中主要存储着下列信息：

- 关联文件的路径、主机名、MAC 地址。
- DestList 的创建时间、上次修改时间。
- 目标文件的创建时间、修改时间、上次访问时间。
- 目标文件的头部属性信息。

……

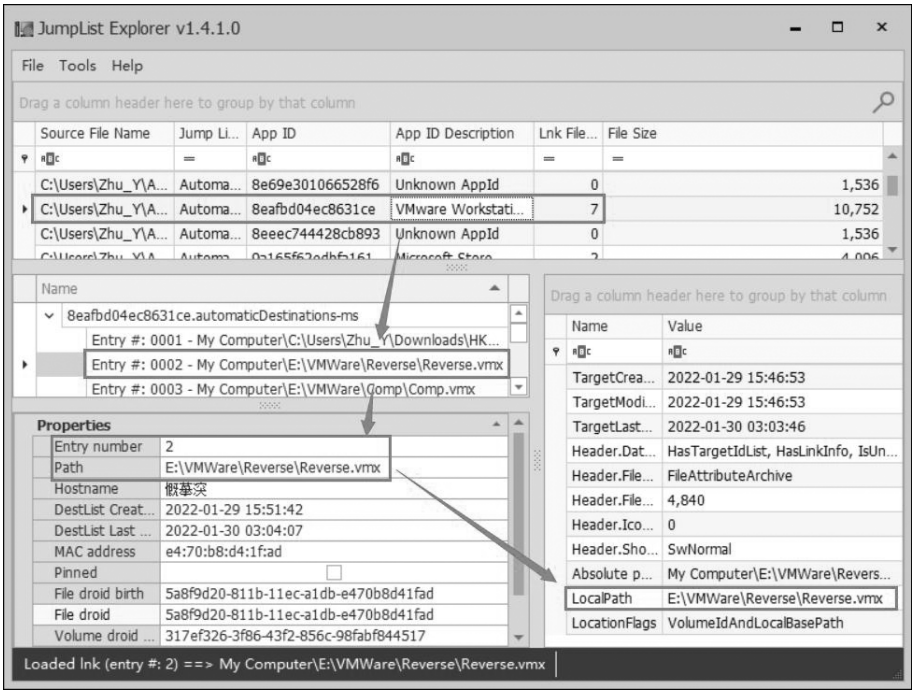

图 5-4　使用 JumpList Explorer 查看跳转列表文件的结果

5.1.6　预读取

预读取是 Windows XP 开始出现的功能，其作用是加速 Windows 的引导过程并缩短程序启动所需的时间。预读取功能通过在启动应用程序时将应用程序所需的文件提前缓存到内存中，从而实现加快程序启动的目的。

在 Windows 系统中，当用户第一次运行某个程序时，系统会创建一个该程序所对应的预读取文件，保存在 C:\Windows\Prefetch 文件夹下。预读取文件的命名规则为“应用程序的名称”＋“-”＋“程序所在路径的哈希值”＋“.pf”。例如，在系统运行 MyHex 程序后，会在预读取文件所在的文件夹中创建该程序所关联的预读取文件，在本例中，预读取文件的名称为 MYHEX.EXE-2C385A27.pf。

表 5-2 和表 5-3 所示为使用 X-Ways Forensics 查看 MYHEX.EXE-2C385A27.pf 所获取的信息。预读取文件中存储着很多有价值的信息，其中主要包括以下信息：

表 5-2　预读取文件包含的与应用程序运行相关的信息

Name(应用程序名称)	MYHEX.EXE
Last Run(最后运行时间)	2022/08/05 15:49:17 ＋8
Last Run(最后运行时间)	2022/08/04 18:02:31 ＋8
Last Run(最后运行时间)	2022/08/04 12:45:13 ＋8
Run Count(运行次数)	3

表 5-3　预读取文件包含的应用程序的调用和关联的卷信息

时间/ms	名　　称	路　　径
0	NTDLL.DLL	\VOLUME{01d804715ba690cd-685bb2b3}\WINDOWS\SYSTEM32\
5	WOW64.DLL	\VOLUME{01d804715ba690cd-685bb2b3}\WINDOWS\SYSTEM32\
⋮	⋮	⋮
173	MYHEX.EXE	\VOLUME{01d823e7c76e2852-48c80d78}\FORENSICS\\MYHEX\
193	LOCALE.NLS	\VOLUME{01d804715ba690cd-685bb2b3}\WINDOWS\SYSTEM32\

- 应用程序的名称、运行的次数。
- 应用程序最近 8 次(如果有)的运行时间。
- 应用程序所关联的卷信息。
- 应用程序所调用的 DLL 文件等。

从 Windows 10 开始，预读取文件的数据结构和存储的数据发生了一些变化。在该版本之前，预读取文件只会记录应用程序最后一次运行的时间；在该版本及以后的版本中，预读取文件能够记录应用程序最近 8 次的运行时间。

在早期的 Windows 系统(Windows XP 到 Windows 7)中，系统最多可以存储 128 个预读取文件；Windows 8 及以后的版本最多能够存储 1024 个预读取文件。一般情况下，

当一个程序的预读取文件生成之后，除非达到系统存储数量的上限，否则即使该程序被卸载，对应的预读取文件也不会被删除。在特殊情况下，某些程序的预读取文件也可能会被自动删除。除使用 X-Ways Forensics 外，取证调查人员还可以使用 PECmd 等工具对预读取文件进行分析。从预读取文件中可以掌握应用程序是否运行过、运行的时间和次数、包含的 DLL 等信息，这些信息有助于对恶意程序的调查分析。

5.1.7 远程桌面缓存

远程桌面协议(Remote Desktop Protocol，RDP)是微软公司开发的专有协议，它提供了图形界面以帮助用户通过网络连接到另一台计算机。RDP 是目前常用的远程访问 Windows 计算机的协议，用户在使用远程桌面连接程序 mstsc.exe 时，系统会产生相应的 RDP 缓存文件。在 Windows 7 及以后的版本中，RDP 缓存文件存储在 C:\Users\<UserName>\AppData\Local\Microsoft\Terminal Server Client\Cache。

RDP 缓存文件有两种类型：一种是 *.bmc 文件，用于较早的操作系统；另一种是 Cache*.bin 文件，用于 Windows 7 及更高版本的操作系统。Cache*.bin 文件最大可达 100MB。当超过 100MB 时会新增一个文件，文件名中的数值从 0000 开始递增，如 Cache0000.bin、Cache0001.bin、Cache0002.bin。这些缓存文件以图块的形式存储原始位图(bitmap)。各个图块的大小可以不同，常见大小是 64×64 像素。*.bmc 文件中图块的颜色深度通常为每像素 16 位或 32 位。*.bin 文件中图块的颜色深度为每像素 32 位。

.bmc 文件并没有固定的头部标识，它是由一张张位图组成的文件，每个位图都有单独的区块文件头信息，总共 20B，前 8B 是位图的哈希值，接下来的 2B 是位图的宽度，再接下来的 2B 是位图的高度，然后的 4B 表示位图的大小(单位是字节)，最后 4B 表示位图的特定参数(是否压缩)。Cache.bin 文件有固定的头部标识，以字符串 RDP8bmp 开头，占用 8B，后面 4B 为版本号，共 12B。

在数字取证中，这些信息能够更好地帮助取证调查人员进行取证分析。例如攻击者在横向渗透攻击时，如果使用跳板机通过 RDP 远程连接了目标计算机并进行了某些操作，取证调查人员就可以在跳板机上分析缓存文件，同时配合 Windows 日志文件发现入侵行为。

在取证实践中，可以使用 BMC Viewer、RdpCacheStitcher、BMC-Tools 等工具配合解析。图 5-5 是使用 BMC-Tools.py 对远程桌面缓存文件的解析结果。这些缓存文件被分割出的文件非常小，但可识别的内容通常是可见的，包括图片、文件和文件夹名称、图标和桌面壁纸等信息。

5.1.8 活动历史记录

随着 Windows 操作系统的更新，Windows 10/11 已经成为现在主流的操作系统版本。相较于以往的操作系统，Windows 10/11 在性能和功能等各方面都有着更好的用户体验。与此同时，这些在 Windows 10/11 中新增的功能也给数字取证提供了一些痕迹和线索。活动历史记录也被称为时间轴、时间线，是从 Windows 10 开始新增的功能，它跟踪所有类型的用户活动和操作，例如用户使用的应用程序和服务、打开的文件以及浏览的

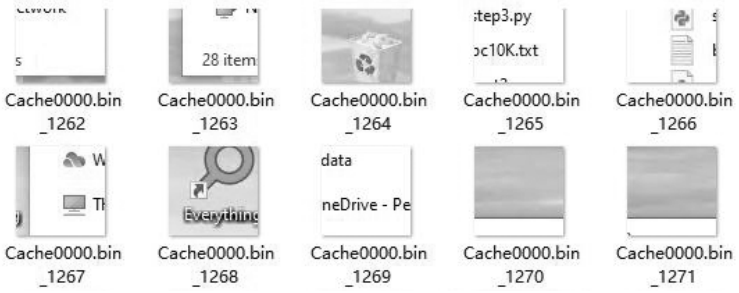

图 5-5　使用 BMC-Tools.py 对远程桌面缓存文件的解析结果

网站、启动和关闭应用程序的时间、用户与应用程序进行主动交互时的时间戳和访问的文件以及用户复制、粘贴的文本和文件等。注意，并不是所有打开的应用程序都会显示在时间轴中。

活动历史记录保存在名为 ActivitiesCache.db 的 SQLite 数据库文件中，存储位置为 C:\Users\<UserName>\AppData\Local\ConnectedDevicesPlatform\L.<UserName>文件夹。ActivitiesCache.db 数据库中包含 Activity、Activity_PackageId、AppSettings、ActivityAssetCache、ActivityOperation、ManualSequence 和 Metadata 7 个表，其中最主要的是 Activity 表。Activity 表中包含多个字段，其中比较重要的是 AppId、LastModifiedTime、Payload、StartTime 和 EndTime 等字段。

图 5-6 是使用 DB Browser for SQLite 查看 ActivitiesCache.db 获取的信息。其中，LastModifiedTime 字段记录的是相关行为的上次修改时间，格式为 UNIX 时间；Payload 则是与该行为相关的动作。参考图 5-6 中的数据可以了解到：在“2022-06-12　10:26:22 (1655000782)”时，系统中运行了 Cisco AnyConnect Secure Mobility Client 程序，或发生了某个与该程序相关联的行为。

图 5-6　使用 DB Browser for SQLite 查看 ActivitiesCache.db 获取的信息

在数字取证中，取证调查人员还可以使用 WxTCmd 等工具实现对 ActivitiesCache.db 的解析，解析结果可以保存为 CSV 格式。

5.1.9　通知中心

类似于手机中的消息推送，Windows 10/11 操作系统也会为用户推送一些消息，如系统的设置信息或应用程序的使用信息等。用户在安装了喜欢的应用程序和游戏后可以为

其设置通知，通常可以在应用程序的设置菜单中设置通知。如果不想看到某个特定应用程序的通知，可以关闭这些通知。通知信息或许能够为取证分析提供一些线索。图 5-7 为 Windows 11 操作系统中来自 Cisco AnyConnect 的一条通知。

图 5-7　Windows 11 操作系统中来自 Cisco AnyConnect 的一条通知

消息通知的内容存储在名为 wpndatabase.db 的数据库中，存储位置为 C:\Users\<UserName>\AppData\Local\Microsoft\Windows\Notifications。该文件中包含 HandlerAssets、HandlerSettings、Metadata、Notification、NotificationData、NotificationHandler、TransientTable 和 WNSPushChannel 8 个表。其中最重要的是 Notification 表。如图 5-8 所示，Notification 表的 ArrivalTime 字段记录的是消息到达的时间，格式为 Windows 时间；Payload 字段记录消息的具体内容。在该表的第二行中，ArrivalTime 中记录的时间为“2022-06-29 19:24:50(UTC+8)”，Payload 字段包含与“Connected:vpn2fa.hku.hk”相关的内容，由此推断，该条记录所记录的正是图 5-7 中显示的 Cisco AnyConnect 推送的通知内容。

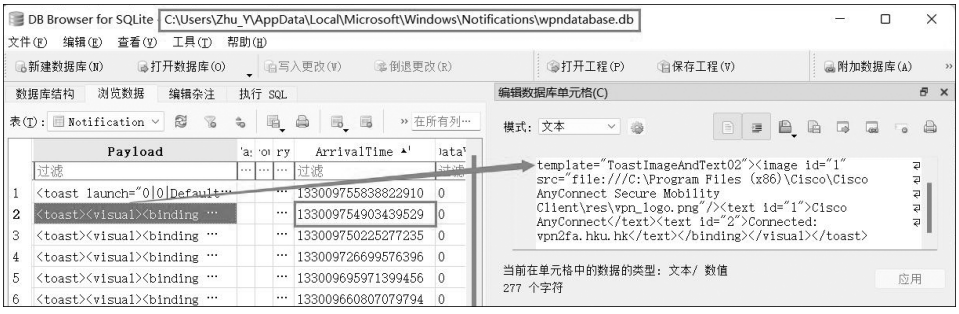

图 5-8　wpndatabase.db 的 Notification 表

5.2　注册表

注册表是 Windows 操作系统中的一个重要的层次数据库，用于操作系统和应用程序存储和检索配置数据。注册表中存储的数据因 Windows 的版本而异。应用程序使用注册表 API 检索、修改或删除注册表数据。在数字取证的过程中，注册表的取证分析是很重要的一个环节。取证调查人员可以从注册表中获取大量有关操作系统、应用程序、网络以及用户的信息。有时候，仅通过分析注册表便能够还原一些事件的原貌。