



“上网本”对计算机法证技术的新挑战

北京天宇宁企业技术秘密保护咨询服务中心

电子证据调查文摘汇编

2009年9月

“上网本”对计算机法证技术的新挑战

概述

基于过去一年的销售状况来看，作为最小的便携式电脑设备--上网本却很具讽刺性地占有着最大的市场销售份额。它们体积较小，价格便宜，被设计成专门处理那些有限的依赖网络的任务项目的轻便电脑。从使用该设备的庞大用户群来看，上网本难以避免地会被用到不法之途上。这只是众多的科学技术成为社会活动的一部分之后的所带来的科技犯罪的一个缩影。这篇文章将帮助我们更好的理解世界上最著名的上网本——Acer Aspire One，对于法证工作的意义。本文，将从法证获取和分析两方面对该电脑进行阐述。

介绍

计算机取证技术是计算机安全领域中必要的的一个部分。随着电子元件大小的变化，新的文件格式、软件系统和技术种类数量的不断增长和价格不断下降的趋势，加上对存储数据的管理方案上的不足，取证分析的工作变得越加困难复杂。计算机法证是一个比较新的领域，对于寻找隐藏在 PDA、移动电话和上网本等设备中的犯罪证据具有更大的挑战。这些设备可以用于直接从事网络犯罪，也可以间接地从事于计算机技术没有直接联系的犯罪行为。由此可见，私人用户和消费者们的电子产品，都有可能是任何形式的犯罪调查的证据来源。

在这篇文章中对上网本，特别是基于 Acer Aspire One，的取证分析方法进行初步探讨。文中调查者做了一项关于传统台式计算机环境和上网本之间的差别的调查，并分析了有可能会影响取证调查者搜集证据和分析数字证据的现有的限制性因素。文中还记载了取证的完整的程序和怎样解决这些搜集证据的难题。

第二章节提供了一个关于上网本或者亚笔记本电脑的背景情况的介绍。

第三章节阐述了一个对尚在研究中的软件产品的简要的技术性概述。

第四、五章节是该篇文章的核心，是对实际取证调查的重点描述。

第六、七章节则总结了该文所涉及的全部内容。

相关背景

上网本（Netbook）的名字来自于网络（Internet）和笔记本（notebook）。它被设计成价格低廉，超便携式，易于使用的移动电脑。这项设备重量较轻，使用简单，结实，并且相对于其他便携式设备而言更便宜。上网本的基本功能是提供给使用者日常所需的电脑功能，如浏览网页，收发邮件，聊天功能和一些基础的数据储存。这类设备不被推荐用来处理那些较复杂的任务，比如图像处理。

华硕易 PC（Asus EEE PC）于 2007 年开始发行带来的巨大成功，导致几乎所有的台式机制造商们都加入了上网本的生产行业。宏基本身在 2008 年第三季度占据了 38% 的市场份额，并使自己成为了上网本的最大品牌之一。由此我们可以看出上网本的受欢迎程度正在增长。

无论如何，这种受欢迎程度带来了电脑使用上的第二个增长高峰。当越来越多的人开始

使用这些上网本时，取证调查者也将会在调查任务中遇到类似的系统。但是没有前期的关于设备环境和法证状况的相关知识的话，调查者可能无法完全处理调查这些设备所遇到的技术上的阻碍和限制。本文说明了对宏基 **Aspire One** 中数据的提取方法，并描述了哪些相关数据信息可以通过分析过程来得到。

技术概述

宏基制造了两种不同的上网本系列，它们的主要不同之处在于分别使用了 10.1 寸和 8.9 寸的液晶屏。此外，不同的系列中所采用的操作系统类型、存储设备的大小和类型、RAM 的数量都有所不同。但这些系统都使用了相同的中央处理器和微处理器。

为了实现调查目的，调查者使用了宏基 **Aspire One AOA 110-1295**。这是一款 8.9 寸屏幕大小、三个 USB 接口，一个 SD 读卡器，一个 VGA 接口，一个摄像头和一个麦克风的上网本。作为一款典型的上网本，该设备不带有光驱或者软驱，有一个以太网络接口和便于上网的无线网卡。该设备被选择的部分原因在于它的存储设备：**Aspire One** 使用了固态硬盘支持 8 和 16GB 大小的数据存储。

宏基 **Aspire One** 支持同时安装两套操作系统：**Linpus Linux Lite** 和 **Windows XP** 家庭版。其默认安装 **Linpus Linux Lite** 操作系统。这套操作系统被专门设计为满足那些对设备要求消耗较低和使用最低硬件的需求。

使用者可以在简洁和高级这两种模式中进行选择使用。简洁模式时，桌面只有四项内容：链接、工作、娱乐和文件。实际上它已经包含了所有操作系统必须带有的软件应用程序。这种模式被设计给那些只有网上冲浪、收发邮件、办公应用和娱乐等需求的普通使用者。当使用简洁模式时，文件系统和高级的外观形式将从使用者的文档中自动被提取出来。

高级模式使用了版本为 4.4.2 的 **Xfce 4** 桌面环境，以便于对 **Linpus Lite** 桌面环境较为熟悉的用户使用。基于高级模式对系统的强大操控能力，用户可以自行增加或者卸载程序，并为打印机、键盘和显示器设置不同类型的配置。而且，高级模式可以提供一个完全的 **Linux** 操作环境。

取证注意事项

对于上网本的证据获取和分析两方面都存在艰巨的任务，关于类似的介绍早已出现。虽然，在获取证据方面的问题已经随着这些设备的发展而有所解决了。

相当数量的设备已经放弃使用传统硬盘而改为使用板载闪存式固态硬盘。这对于上网本来说有很多好处（如节省空间、造价和减少可移动组件等），但这些设备与主板焊接在一起，使得取证更加困难。

在本例中，宏基 **Aspire One** 也无法例外的使用了板载焊接的闪存式硬盘而不是可拆卸的传统硬盘装置。其结果是，取证调查者很难取出硬盘设备并从取证意义上将其复制并用于分析。强行拆卸只会损坏其中的数据存储情况。但有一些属于系统嵌入的技术，通过该技术我们可以获取硬盘上的数据或者将其从电子板上脱焊。但是，任意一种方法都太过费时费钱或者不能够完整地提供充足的获取结果。

因此，取证调查者必须找到一个合适的方法来获取数据而不是从物理上强行损坏硬盘和其中的数据。具有讽刺意味的是，对于上网本的取证分析面对的最大的难题是其可用空间的不足。即使这听起来与取证分析面临的另一大特点（数据存储的增长）完全相反。

小型的自定义操作系统意味着没有任何希望能够像在完整的计算机环境里那样轻易地找到证据。这些证据包括上网记录和日志文件，还有关于用户编辑文件的简洁概况。

比如说, 宏基 Aspire One 上网本能够安装两种不同的操作系统, 从该特点来看, 这款电脑并不只是一款娱乐电脑。这两种操作系统在许多方面都不尽相同, 如文件结构, 磁盘格式, 用户特权, 储存位置, 以及可安装的应用程序等。因此, 当取证调查者并不确定分析中需要安装哪一类操作系统时, 为了能够最大量的提取相关信息, 必须对每一系统都有着深厚的相关知识。

除了默认的系统, 还有一些其他可供选择的系统也被设计成适用于上网本。但在该文中, 调查者集中在对于默认的 Linpus Linux Lite 操作系统的分析。

调查计划

这篇文章介绍并描述了一个总体的框架, 可以用来帮助取证调查者调查宏基 Aspire One 上网本。关于这项工作的许多环节也同样适用于其它的上网本, 但其重点是针对宏基 Aspire One。

分析工作的进程可以分为三个阶段: 镜像获取, 镜像完整性检测和镜像分析。其中每一项都将在此得到具体分析。

i) 镜像获取

如上所述, 从物理意义上获取硬盘是不可行的。因此, 通过提取内存和只读锁设备克隆来对磁盘镜像并不是一个切实可行的方法。更进一步说, 在一个现实的取证环境下进入系统是一个具有法证意义的可选择实施的探索。

虽然宏基 Aspire One 没有板载光驱, 但是它可以通过 USB 外接光驱或者优盘来启动, 这是在 BIOS 中默认的启动方法。

在这项调查工作中, 调查人员选择了版本 2 的 Helix-3 作为一个实际的取证调查环境来运行系统。

上一版本的实际环境是基于 SLAX 的, 最新的版本已经改为 Ubuntu 系统。它可以在宏基上网本中启动运行。

一旦程序启动运行后, 取证调查者必须给外接的 USB 硬盘配上读写许可以便在法证意义上拷贝镜像, 或者可选择性的配上外接网络驱动器。

为了能在本机上配备一个驱动器, 需要遵循以下步骤:

```
mkdir /mnt/destination  
sudo mount /dev/sdb1 /mnt/destination
```

假定外接硬盘路径设置于 /dev/sdb1, 使用 NTFS 格式的硬盘也同样可行, 但是在这里使用超出了 NTFS 系统的工作范围。更多相关信息可从 Helix3 使用手册上查阅。

一旦一个目标磁盘被配备了一个读写许可, 此时镜像可能被获取。Helix3 提供了一些可供选择的如 Linen、DD 等对磁盘进行镜像获取的方案。

调查者在 Helix3 系统中采用 Adepto 2.1 镜像软件来对硬盘创建镜像。

相对于 DCFLDD 的命令行界面来说, Adepto 2.1 是一个图文并茂的软件。

我们使用的一些关于镜像的步骤有:

```
dcfldd if=/dev/sda1 of=/media/destination/sda1-img.dd.  
dcfldd if=/dev/sda2 of=/mnt/destination/sda2-img.dd.  
dcfldd if=/dev/sda of=/mnt/destination/sda-img.dd.
```

这些指令的实施是在上述外接目标磁盘已经被正确配备的情况下。

Adepto 2.1 还提供了创建数据区的法证拷贝和创建对全部硬盘获取镜像两种选项。

宏基 Aspire One 的分区默认状况如以下表格中所总结的：

| | | |
|------------------|----------|-------------------------|
| /dev/sda | 31.5 KB | Unallocated Data |
| /dev/sda1 | 6.511 GB | ext2 (operating system) |
| /dev/sda2 | 1.004 GB | ext3 (swap partition) |
| /dev/sda | 661.5 KB | Boot Partition |

表格1 –宏基Aspire One上网本的默认分区

分区sda1包含了简化的Linpus Lite操作系统，并是法证分析的主要重点。

在调查中，sda2 也会对工作产生帮助，因为它是共享分区。它可能对记忆系统分析技术和更高级的分析产生帮助。

ii)镜像完整性检测

使用 DCFLDD 指令获取的潜在益处的其中一点是获取镜像是通过对比哈希值进行的。保证镜像完整获取的方法是根据某个特征来将镜像进行分段的指令。这是一个在许多法证获取工具里都有的特点。

iii)镜像分析

这是在任何法证分析过程中都是最重要的一个步骤，法证工作者可以使用各种各样的方法来提取相关数据。

我们遵循的是由华硕 Eee PC 界定的法证调查工序。在实际操作中，为了达到最终的目的，所实施的工作步骤则依据于调查者制定的特定的方式。一种方式是指向各分区，另一种方式是根据安装在系统里的每一个程序来获取数据的。

我们使用 Encase v6.11.2 来分析获取的镜像并将关注的证据分为两部分。系统生成的日志数据和用户创建的数据。在下文中两部分将分开论述。

1)用户创建的数据

根据上文，用户所创建数据是纯粹由用户直接创建的，或者与使用者有直接关系的那些数据。包括：上网浏览记录，聊天记录，RSS Feeds，邮件，个人文档文件，日程表和通讯录。

关于这些文件大多数的作用，是它们是提供数据的来源，宏基 Aspire One 上网本已经预先安装了上述项目。而且，这其中的每一项都在下文中有一系列的详细说明。

a)上网浏览记录：

对绝大多数人来说，因特网或者上网交流是必不可少的日常活动的一部分。这项技术对我们日常生活的影响可以从消费者花费在网络上的时间几乎是看电视的两倍的情况来判断。因而，我们可以预见根据网络进行犯罪或者计划犯罪的可能性是相当高的。

宏基 Aspire One 中已经设置了 Mozilla Firefox 作为默认浏览器。路径文件 /home/user/.mozilla/firefox 中包含了 cookie 程序，上网记录和书签。

以下表格 2 对出现在文件夹里的相关文件进行了详细的说明。

| Use of file | Full Path |
|--|---|
| Cookies information | /home/user/Mozilla/firefox/uc1c3f23.default/cookies.txt |
| History of URLs visited | /home/user/Mozilla/firefox/uc1c3f23.default/history.dat |
| List of bookmarked websites | /home/user/Mozilla/firefox/uc1c3f23.default/bookmarks.html |
| Information saved in the browser for auto complete | /home/user/Mozilla/firefox/uc1c3f23.default/formhistory.dat |
| Username and password saved in the browser | /home/user/Mozilla/firefox/uc1c3f23.default/signons2.txt |
| Security module database | /home/user/Mozilla/firefox/uc1c3f23.default/secmod.db |
| Key database | /home/user/Mozilla/firefox/uc1c3f23.default/key3.db |
| Client Certificate database | /home/user/Mozilla/firefox/uc1c3f23.default/cert7.db |
| History of the downloaded files by the browser | /home/user/Mozilla/firefox/uc1c3f23.default/downloads.rdf |
| Temporary Internet files | /home/user/Mozilla/firefox/uc1c3f23.default/cache |

表格2 某用户上网行为后涉及的相关文件列表

b) 聊天工具

上网本已经预先安装了Acer通讯工具应用程序，它支持时下流行的所有即时聊天工具：Yahoo, Google Talk, AOL以及ICQ。这项应用程序已经被作为Acer通讯套装的一部分，并且它带有是否安装聊天工具的选项和注册名以及密码。关于此可从/home/user/.ACS directory. 中查阅。

c) 邮件客户端：

当今社会，邮件绝对是电子交流最普通常见的方式，也是一个当犯罪行为不止一个嫌疑人时的极其重要的证据信息来源。

宏基通讯套装里面的邮件客户端是 Aspire One Mail。可从路径文件/home/user/.AME/Message.里查阅所有邮件客户及其历史内容、附件以及日志信息。

d) RSS Feeds:

RSS 是一个允许用户订阅‘feeds’的系统，支持开放下载工作的快速自动分类。

在宏基 Aspire One 的 Linpus 操作系统里简易模式的联系栏里有一个 RSS feed 图标，它可以通过从任何网站加入 XML 文件来设定。

RSS feeds 相关信息可在目录文件夹/home/user/.AME/RSS 下了解。它允许调查者提取订阅的 feeds 以及相关的日期时间。

e) 日程表和通讯录:

日程表应用程序中建立了一个记载用户登记的所有信息的数据库。可从目录文件 `/home/user/.PIMDS/Calendar/PimDS_Calendar.db` 中查询具体信息。

同样的，关于通讯录程序中记载的所有信息也可从目录文件 `/home/user/.PIMDS/Contact/PimDS_Contact.db` 中查看细节。

在法证调查中，有许多明显有益的环节能够帮助找到这类信息并提供类似时间线索分析和可能与所调查案件有关的其它信息。

f) 个人文件

所有通过 OpenOffice.org 应用程序（比如说，文档、电子制表软件和报告）保存过的文档（不管是临时保存过还是永久保存着的）都保存在目录文件夹 `/home/user/Documents folder`。

同样的，用户创建的照片和内置摄像头拍摄的照片都被存储在 `/home/user/Pictures` 文件夹里。

依此类推，所有的音乐、视频和下载的文件都各自存放在对应名称的目录文件里 `/home/user/`。

g) My SQL 数据管理库:

My SQL 是已安装在 Aspire One 里的默认程序，配合 OpenOffice.org 的通讯录和日程表程序使用。该程序只能在高级程序里使用并将相关信息存放在目录文件夹：`/home/user/.openoffice.org2.0/user/database` 中

h) gFTP

gFTP 是一个配合上网本使用的默认的 FTP 客户端，是一项在高级模式里应用的程序。

用来记录信息的书签和记录会话连接和数据传输的日志在取证分析中也有很大作用。可以从目录文件 `/home/user/.gftp` 中查看。

2) 系统生成日志

系统生成日志是用于记录操作命令，结构文件，安装程序、配置设备等的信息。用户对这类文件的生成创建控制权有限，因为需要相当的技术能力才能对系统生成数据进行改变，所以它也是一个极好的证据信息的来源。

调查员可以从查阅 `/var` 目录着手，它包含了管理数据，日志和操作系统创建的临时文件。

这些应用程序是由第三方的程序所安装的，并且在简便模式中并不显示。这些记录的显示可以说明这类软件曾被安装使用，这也可以提供一些使用者使用的状况。

调查者也可以寻找一些应用程序的临时文件，因为它们都是使用者在使用程序时应用和活动的显示来源。目录 `/tmp` 中储存了所有临时文件。所有特殊的信息都被存在 `/etc/hosts` 中。

另外，所有 Mozilla Firefox 浏览器和 Acer Messenger 使用的常规的结构文件和类似文件都存放在目录文件 `/root` 里。

另一项值得研究的项目是命令行记录。

调查者可以在对应位置下找到哈希历史记录并根据时间线索分析，这些信息都有可能产生作用，相关信息在下表中有所说明。

| File Name | Path |
|---------------|--------------------------|
| .bash_history | /home/user/.bash_history |
| .bash_logout | /home/user/.bash_logout |
| .bash_profile | /home/user/.bash_profile |

表格3 –指令文件的概况和Bash历史记录的路径

在许多方面，关于该系统的文件体积和存储状况与 Linux 的其它版本类似，所以也会将数据保存在相同的路径里。这对取证调查者有极大的意义，使得调查者对其他 Linux 系统的分析知识得以横向利用。

未来的调查

关于上文中我们得到的信息可以很好的使用于未来的调查工作中。

首先一点就是如何对取证框架做出适当修改一适应宏基 Aspire One系列的其他上网本。

还可以在Microsoft Windows XP作为操作系统的环境下探索出不同的镜像分析方式。

无论如何，这种分析方法都同任何Microsoft Windows系统的分析极其相似。除非制造商再加入其它的软件，或者由其他制造商创建另一类提取和分析的流程图。

在这里讨论的所有流程都基于从原始硬件设备中导出数据。有可能对我们所遇到的状况并不适用。

在调查中当上网本遭到物理上的损坏不能再运行时可能依然包含有价值的证据数据。尽管如此，当我们讨论的条件合适时，损坏的环境可能意味着硬件的数据提取只有唯一可行的方法。

如使用了 SalvationDATA 软件的系统进行全面恢复后依然可以进行深入调查，此软件有可能将上网本的取证调查带至更高的水平。

关于上网本是对不甚明朗的计算机技术的积极发展的意义已在上文中进行了讨论。如商业信息的外储存、在线语言处理、录像、聊天交流和其他被设计来达到未知目的系统程序对上网本用户来说都是相当有重要意义的，计算机的等级将给予其相应的储存空间和电力能源。

不明朗的计算机业中上网本的使用有着极大的法证含义，特别是在数据分析方面。

主要的问题出现在如何掌握账户和系统的使用情况，尤其是当数据存储在其他地方（甚至其他国家），而设备本身只包含少量信息时。

关于宏基 Aspire one 使用的操作系统和当前数据的需要进一步分析研究。对不同的上网本系统的区别也需要进行强调。

但是对于Linux基础系统的调查分析方法已在本文中提出。

结论

根据制造业的销售图表来看（包括当下销售的数据状况和大体的经济条件），我们有理由相信上网本的销售量会继续增加。上网本凭借它的小巧和有竞争力的价格优势被大众所需要，而且这种需求正日益增大。因此，一个关于这种机器类型的细节研究应当尽快完成，而且也应当设计一个大致的架构来引导取证调查者。本文详述了基于法证意义层面上对宏基 Aspire One –AOA 110-295 上网本的调查方法，虽然这些详述只是针对这一特定对象，但是这些方法和流程也是值得推广的，也可以略加修改来适应宏基 Aspire 的其他系列上网本，或者其他品牌的上网本也可以适用于这套方案。