Mac OS X 取证训练营

课程时长: 5 天/级

开课时间: 应团队客户要求

授课地点: 应团队客户要求

授课语言: 英语

学员人数: 应团队客户要求 (建议每班不超过 12 人)

学习目标:

苹果电脑取证训练营的课程内容涵盖了苹果操作系统取证的整个逻辑流程。整个流程中完全没有用到昂贵的自动取证工具，仅需使用一部苹果电脑。学员会惊奇地发现，原来他们可以在非常短暂的时间内提取到比以往更多的证据。

适用学员:

初级至高级苹果电脑取证人员。

深圳市顺安特科技有限公司
中国广东省深圳市罗湖区人民南路 2008 号嘉里中心 13 楼 1308 室　　邮编 518001
网址: www.dataexpert.com.hk　　电子邮箱: info@dataexpert.com.hk　　服务热线: +86 755 22905810

Data Expert™ Technology Makes Possibility

初级课程

为何使用以 Windows 为依托的取证工具会遗漏证据？

怎样使用苹果电脑对苹果电脑进行取证？

编号	主 题	内 容
1	**非 Intel 苹果电脑的常见问题 (PowerPC 与经典 OS)**	侦查人员在工作时可能会遇到比较早期的技术问题，课程将讲解早期的苹果技术及如何应对相关问题。另外，通过回顾经典 OS，有助于学员了解技术与系统革新、操作系统痕迹和特征。
2	**Mac OS X 版本概述**	了解不同 Mac OS 的取证重点和特征，并知悉这些特征是从哪一版本开始出现的。
3	**Mac 文件系统**	了解 Mac OS 支持的文件系统。
4	**Intel Mac 技术及 Bootcamp**	Mac Intel 技术在取证中的重要性。
5	**Mac 安全问题及 FileVault 攻击**	时下最新的 Mac 安全保护措施。
6	**苹果电脑的数据搜索与获取**	了解获取 Mac 及 iOS 硬件的最佳方式。
7	**安全获取系统信息**	如何在不损害证据的情况下安全获取系统信息？
8	**固件密码绕过**	OFP 概述及移除方法。
9	**易失性数据收集**	如何创建可信的实用硬盘(Utilities Disk) 并将其用于捕捉易失性信息。
10	**镜像与数据获取的手动操作和自动操作方法**	使用苹果电脑安全地对硬盘进行镜像，可手动操作也可使用 PALANDIN 进行自动操作。
11	**苹果电脑 RAM 镜像**	练习制作苹果电脑 RAM 镜像、密码恢复。
12	**验证与安全挂载(Mount)取证镜像**	安全挂载镜像，为后续操作做准备。
13	**取证镜像索引**	如何使用 Mac OS 进行取证镜像索引。
14	**搜索在使用 Mac OS X 的技术**	从命令行和 GUI 中创建自定义搜索表达式。
15	**证据定位（电子邮件、图表、上网痕迹、文档、系统痕迹、即时通讯、日志等）**	在文件系统中识别 Mac 痕迹。
16	**已删除文件恢复**	练习手动恢复已删除文件，了解 Mac 优化存在的风险。
17	**检查 SQLite 数据库及 PLIST 文件**	检查 Mac 数据存储的核心。
18	**利用 OS X 进行取证**	如何使用 Mac OS 内置技术进行取证。

深圳市顺安特科技有限公司
中国广东省深圳市罗湖区人民南路 2008 号嘉里中心 13 楼 1308 室 邮编 518001
网址: www.dataexpert.com.hk 电子邮箱: info@dataexpert.com.hk 服务热线: +86 755 22905810

编号	主 题	内 容
19	**制作报告**	如何创建本地报告并使用 Mac 妥善查看数据。
20	**检查 iOS 设备痕迹**	识别与侦察 Mac iOS 痕迹。
21	**NTFS 系统**	在以 Windows 为核心的取证实验室中进行 Mac 综合取证。
22	**应用程序推荐**	介绍常见的商业/非商业 Mac 取证辅助工具。
23	**自动取证工具**	简介当前自动 Mac 取证工具。
24	**用作取证用途的苹果电脑之硬件要求**	Mac 取证硬件简介。

高级课程

苹果硬件、技术及应用程序的使用及解析。

编号	主 题	内 容
1	**高级文件系统分析**	简介 Mac OS X 环境下域名的概念，学生可掌握证据痕迹的定位方法。此外，我们还会教授如何手动解析已安装的应用程序。
2	**高级命令行**	存在于 Mac OS X 界面和桌面下的是 Unix Shell,其中含有一个终端，可以令用户从命令行中获取操作的原动力与控制力。学员将会学到“命令行”的高级应用知识，以便更加得心应手地进行 Mac 取证。
3	**AppleScript 与 Automator**	Mac OS X 中含有两个本地应用程序，用户可运用它们开发专属程序、设计自动工作流程。学员将会学到如何创建他们自己的 AppleScript 与 Automator，从而简化 Mac 取证操作、提升侦察实力。

编号	主 题	内 容
4	**虚拟机的认识与使用**	学生会学到 Mac OS X 虚拟机的识别和必要的分析流程。此外，本课程还将教授 Mac 环境下如何利用虚拟机辅助取证查验。
5	**Mac OS X 服务器取证**	Mac OS X 服务器技术，包括服务和用户账户。我们会介绍安全进行动态取证的最佳方案和受损系统的应急响应。
6	**苹果电脑时间线解析**	创建文件系统时间线可追溯疑犯逐分甚至逐秒的历史记录。此课程将带领学员认识 Mac 时间戳，并运用时间戳进行解析。
7	**iCloud 取证**	分析与 Apple iCloud 账户同步的文档及其他数据。
8	**苹果独家技术**	我们将会提供绝佳的解决方案和资源，帮助学员应对一些较为麻烦和独特的苹果技术。
9	**高级搜索技巧**	掌握高级索引的使用方法，学会运用即时搜索找出所需数据。
10	**应用程序解析**	找出应用程序留下的痕迹。