

硬盘数据恢复课程

以电子取证实验室为基础的硬盘数据恢复课程



课程时长: 3 天

授课地点: 应团队客户要求

学员人数: 应团队客户要求 (建议每班不超过 12 人)

授课语言: 英语/中文

讲师: 计算机法证顾问, 美国科技犯罪调查协会(HTCIA)成员

顺安特硬盘数据恢复课程为一门综合性课程, 内容包含了硬盘的全部常见问题及相应的数据恢复方法。学员可从中学到中级至高级水平的硬盘数据恢复理论及技术, 还可掌握计算机法证科学中的基本技能——电子证据固定, 为未来发展奠定基础。

学习目标

- 了解硬盘固件组成及工作原理
- 了解硬盘数据恢复工具工作原理
- 区分不同品牌与型号的硬盘, 学会阅读分析报告并依据报告制定数据恢复方案
- 掌握 100 级无尘室标准作业流程, 学会在无尘室中处理硬盘物理损坏问题

顺安特电子取证实验室, 包括:

- 100 级无尘室
- 盘片与磁头更换工作台
- 数据恢复工作台, 配备多种连接线及常用零部件
- 数据恢复工具及设备: 写保护工具、取证级镜像工具 (复制机)、综合密码破解系统、智能分析工具, 消磁机及介质粉碎机等

本课程适用于以下人群:

- 警察及执法部门工作人员

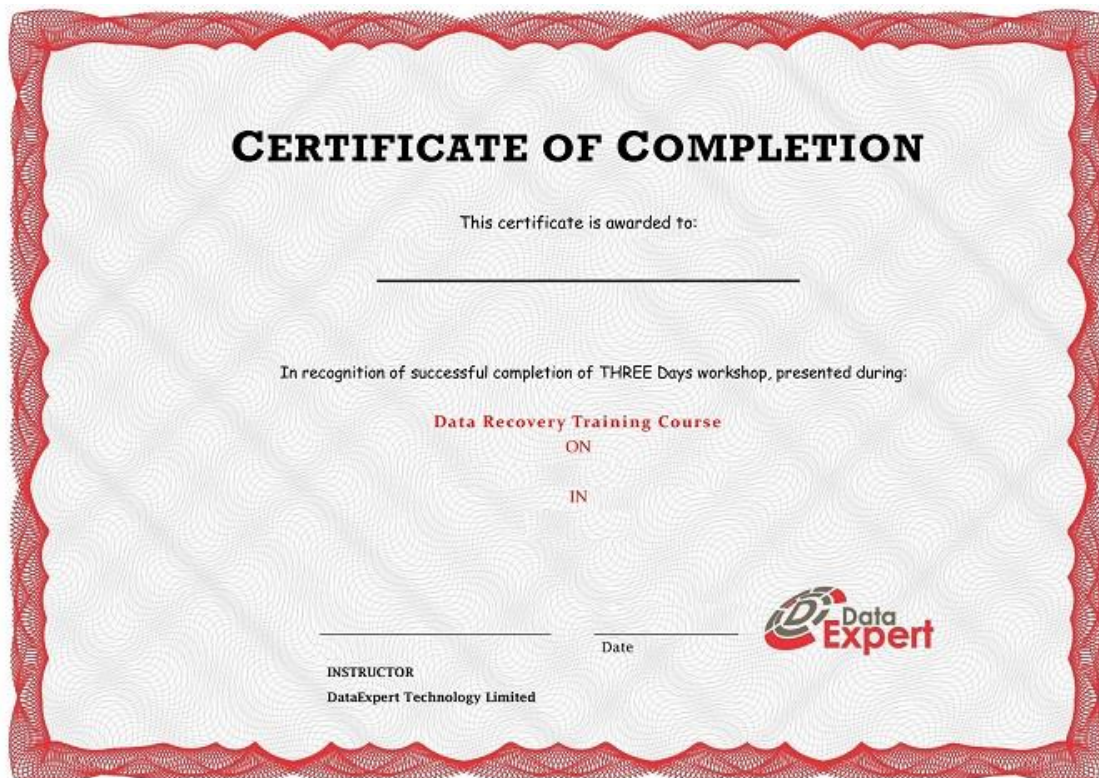
- 国防及军队工作人员
- 法律工作者
- 企业系统管理人员及 IT 部门工作人员
- 信息安全部门工作人员
- 数据恢复从业者及爱好者等

入读条件

- 具备计算机操作系统基本知识
- 对计算机硬件具备基本认识

课程定制

为满足客户的多样化需求，令学员高效达成学习目标，顺安特可为团队客户安排定制化课程，包括时间安排、授课地点、语言选择、内部培训等。



课程安排

第一天 0845 - 1800

硬盘相关理论介绍及结构部件知识，是初学者必备的知识基础，同时也令有经验者温故知新。

硬盘构造——设计原理与概念

- 硬盘的历史
- 操作原理
- 基本元件
- 接口概览 (ST506 至 SATA, SAS)
- 磁性介质类型
- 数据恢复的成功率
- 盘片上的数据结构
- 伺服信息：磁道位置、磁头精确位置、伺服数据结构
- 磁头类型、悬空高度及与位元密度的关系

常见文件系统

- DOS
- FAT 16 及 FAT 32
- HTFS/Ext2/HFS+

硬盘的几何结构

- 磁道、扇区数据格式
- 物理、逻辑结构: PCHS/LCHS/LBA 寻址、硬盘系统区域 (SA)、区域(Zone)结构、BIOS 结构、Negative 柱面
- 扇区、磁道、柱面、区域、磁头列表
- 坏扇区映射类型、G-List/ P-List/ U-List、LBA 对齐
- 转换: LBA 寻址(LBA 28/ LBA 48); 静态、动态转换类型

硬盘固件结构

- 嵌入式 ROM
- 外置闪存 ROM/NV-ROM
- SA 原始叠加 (Raw Overlay)
- 区域表

第二天 0845 - 1800

硬盘子系统

- 管理员、用户密码
- 高安全性及最大安全性
- 解锁、删除、清除指令
- 解锁 ATA 硬盘的步骤
- 具有 FDE (全盘加密) 功能的硬盘原理

不同存储设备的查验

- 硬盘 (2.5" & 3.5", ATA, SATA, SCSI, SAS)
- 极碟(Zip disk) 与 LS120
- 磁光盘
- 移动硬盘
- 闪存盘 (U 盘, SD 卡)

印刷电路板

- 不同品牌硬盘的 PCB 结构概述
- PCB 层次及功能
- PCB 结构及成分
- 元件类型与功能

硬盘物理损坏诊断

- 外部感官判断
- 主要元件及存储设备的识别
- 示波器的基本应用
- 确定设备功能情况

元件表面贴装技术简介

- 表面贴装热风工作台操作
- IC 表面贴装去除操作
- IC 表面贴装去除练习

常见硬盘数据恢复工具简介

- **硬件**
 - 安特拉数据恢复及电子取证系统
- **软件**
 - R-Studio

第三天 0845 - 1800

理论与实践相结合，学习处理硬盘物理损坏故障和无尘室的使用方法。

物理数据恢复工作流程

- 硬盘诊断
- 更换碟片
- ATA 密码移除
- PCB 修复
- 磁头故障
- 硬盘固件恢复
- 更换 PCB
- 前置放大器故障
- 发动机故障
- 故障防范

逻辑恢复案例

- MBR 与 EBR 恢复
- GPT 盘简介
- 硬盘备份及复制
- 文件提取

无尘室操作演示与实践

- 无尘室操作流程与 HEPA 微滤简介
- 磁头拆卸技术
- 硬盘部件重组

实践操作

- 1.8", 2.5", 3.5" ATA/ SATA 硬盘
- 2.5" SAS 硬盘