网络空间安全学科系列教材

教育部高等学校网络空间安全专业教学指导委员会
中国计算机学会教育专业委员会
共同指导

丛书顾问委员会主任：沈昌祥 | 丛书编委会主任：封化民

数字取证实验

陈晶 郭永健 熊翘楚 编著

根据教育部高等学校网络空间安全专业教学指导委员会编制的
《高等学校信息安全专业指导性专业规范（第2版）》组织编写

清華大學出版社

内 容 简 介

受高科技的冲击，利用信息技术进行的犯罪急剧增长，为了适应打击新型犯罪的需要，提升司法人员的电子数据取证能力势在必行。随着“电子数据”时代的到来，电子数据已经在新修订的刑事诉讼法、民事诉讼法、行政诉讼法中被明确列为一种独立的证据类型，被誉为新的“证据之王”。这凸显了电子数据，尤其是在数字取证技术的帮助下，对于打击网络犯罪、获取犯罪证据的重要性。

本书作者总结五年的实验教学思路和经验，编写出这本《数字取证实验》。实验紧密结合电子数据证据取证工作实际，既考虑了数字取证的知识体系，又尊重了理论学习和取证实践的规律，按照理论和技术并重的编写思路，深入浅出地讲解数字取证的基本原理。并结合电子数据取证实践性强的特点，通过实际的案例分析和实践练习将理论与现实世界联系起来，帮助学生更好地学习和掌握取证知识。该书适合国内网络空间安全方向的本科生以及公安院校网络安全与执法方向的学生使用。

《数字取证实验》一书共设计了十二个章节，每个章节围绕一个具体的数字取证主题设计若干个小实验，包括电子证据的获取、哈希计算、文件过滤、关键字搜索、元数据提取、数据恢复等核心知识点，并基于 Windows、Linux 和 macOS 桌面操作系统取证，Android 和 iOS 移动终端操作系统的基本原理、安全架构和痕迹特点进行详细讲解并开展实验。

该书配套的实验系统提供了丰富的实验案例、实验工具和习题，在武汉大学国家网络安全学院进行了五年的实践优化，确保读者能够获得最佳的教学效果。

前 言

随着大数据、互联网、人工智能时代的到来，以数字化、网络化、智能化为主要特征的创新浪潮一浪高过一浪，现代科技正在推动社会变革和进步，同时也深刻影响着司法办案的模式、证据类型和证据规则。

随着数字化进程的推进，数字证据和数字取证技术在各类案件中的重要性日益凸显。数字取证作为一门新兴的交叉学科，旨在通过科学的方法和技术手段，从海量的数字信息中提取、分析和鉴定与案件相关的电子证据，为案件的侦破和审判提供有力支撑。

《数字取证实验》作为《数字取证》的配套实践教材，强调理论与实践相结合，通过实验的方式让学生亲自动手，掌握数字取证的基本技能和方法。全书在实验内容的安排上，既注重系统性，又强调实用性。在结构编排上，全书分为十二个章节，每个章节围绕一个具体的数字取证主题设计若干个小实验。通过实验步骤的详细讲解和实际操作案例的展示，使读者能够循序渐进地掌握数字取证的核心技术。在内容上，本书既包含了数字取证的基本理论和方法，也涵盖了当前数字取证领域的最新技术和研究成果，旨在为读者提供一本既全面又前沿的学习参考资料。全书的具体内容介绍如下。

第一章至第四章节主要介绍数字取证实验教学环境以及取证的基础操作，包括电子证据的获取、哈希计算、文件过滤、关键字搜索、元数据提取、数据恢复等核心技术。随着内容的深入，第五章至第十章则聚焦于操作系统和痕迹分析。这些章节基于国际主流的 Windows、Linux 和 macOS 桌面操作系统，以及 Android 和 iOS 移动终端操作系统的基本原理、安全架构和痕迹特点，介绍不同操作系统中如何获取数据、回收站和废纸篓、最近执行的程序、最近打开的文件、注册表分析、日志分析和内存分析等核心取证知识点。第十一章和第十二章涵盖了智能穿戴设备取证、无人机取证、物联网设备取证等新兴领域的知识，并对数据加解密、隐藏和反取证技术等进行实践操作。

《数字取证实验》是一本兼具理论性和实践性的教材，书中所有实验案例均已集成到虚拟仿真实验教学环境中。通过本书的学习，不仅可以帮助读者提升个人的专业技能和素养，更可以推动数字取证技术在我国的普及和发展，为我国司法公正和社会安全贡献一份力量。

本书由武汉大学陈晶、郭永健、熊翘楚三位老师精心编写。在撰稿和校对过程中得到了欧季成、皮浩、许伟、谢明聪、魏智煌、胡力和的大力支持，他们为本书第六章、第七章、第八章、第九章、第十一章提供了初稿、素材和修改意见。 限于作者水平，本书难免存在各种错误和不足，殷切希望广大读者批评指正，也希望读者能够就图书内容和编排方式提出宝贵意见和建议。

联系作者：sprite@cflab.net

编者

目 录

第 1 章 数字取证实验教学环境

数字取证是一项涉及法律规范和科学技术的学科，主要研究如何对数字化存储的数据信息进行获取、保存、分析和出示。其过程包括从存储设备及网络等媒介中收集数据，通过对媒介进行恢复和检查，获取与案件相关的电子数据。随后，对电子数据进行解释和分析，发掘其中的信息，并最终通过报告等形式形成证据，以证明或证伪某种假设。

《数字取证实验》教材与《数字取证》课程相结合，设计了涵盖十二章的系列实验环节，逐步引导读者掌握不同取证工具的基础操作。通过将背景知识、操作方法与取证思路融为一体，最终培养解决数字取证实际问题的能力。在本课程所使用的数字取证教学平台中，整合了实验工具、教学课件、教学视频以及实验指导手册等资源。通过阅读本章内容，读者可对课程实验环境、实验方法及实验资源有所了解。

实验 1.1 登录数字取证教训平台

（1）实验目的

通过本实验，使读者了解数字取证教训平台的基本功能模块，掌握教学课件、教学视频和实验手册的使用方法。

（2）实验环境

浏览器，推荐使用谷歌浏览器。

（3）实验步骤

步骤 1：请打开浏览器，输入数字取证教训平台的网址，进入登录页面。在此页面中，请使用个人账户和密码登录教训平台首页，如图 1-1 所示。

图 1-1 数字取证教训平台首页

步骤 2：登录后，选择“数字取证概述”模块，点击“开始学习”，以进入本次课程。在课程目录大纲中，依次点击各小节右侧的“开始学习”按钮，进入虚拟机学习界面。平台为每位用户分配一台用于训练的虚拟机，并将课程资源整合其中，如图 1-2 所示。

图 1-2 课程页面示意图

步骤 3：点击桌面的“CDF 实训系统”图标，打开取证软件和课间集成入口菜单页面。选择左侧菜单栏中的“课件”，在右侧查看对应章节的实验指导、教学课件、教学视频、实验手册以及参考资料，如图 1-3 所示。

图 1-3 平台内课件等教学资源

实验 1.2 数字取证教训平台作业与考试系统

（1）实验目的

通过本实验，使读者掌握作业系统和考试系统（教师）的使用方法。

（2）实验环境

浏览器，推荐使用谷歌浏览器。

（3）实验步骤

进入个人虚拟机环境后，将鼠标移动至左侧，呼出小弹窗，点击“实验习题”，即可进行本章习题测试，如图 1-4 所示。本书为每个章节均设计了不同的实验习题。

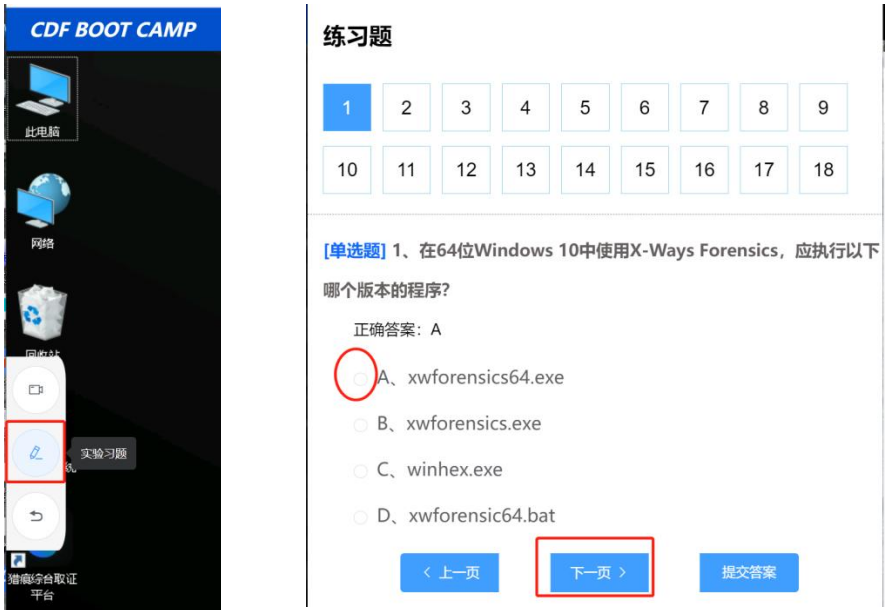

图 1-4 作业系统

实验 1.3 数字取证教训平台取证软件

（1）实验目的

通过本实验，使读者熟悉平台内集成的数字取证常用软件的基本功能。

（2）实验环境

浏览器，推荐使用谷歌浏览器。

（3）实验步骤

步骤 1：在进入个人虚拟机环境后，点击桌面上的“CDF 实训系统”图标，打开取证软件与课间集成入口菜单页面。在左侧菜单栏中选择“应用”，即可查看平台内整合的多款数字取证常用软件，如图 1-5 所示。这些软件包括 Myhex、WinHex、猎痕鉴证大师、猎痕分析软件以及哈希计算工具等。

图 1-5 数字取证平台取证软件

步骤 2：根据实验内容要求，点击对应取证软件下方的“启动软件”按钮，可以打开取证软件，进行案例分析。具体分析过程将在第 2 章进行介绍。

第 2 章 数字取证基础

在应对海量数据的海量数字取证过程中，调查人员需运用适当的过滤搜索策略对数据进行筛选。过滤是指根据现有属性查找符合特定条件的数据，而搜索则是基于关键词在检材中快速定位数据。将这两种方法相结合，可助力调查人员找到案件调查的关键线索。本章将借助数字取证领域常用软件 Myhex、Winhex 和 X-Ways Forensics，结合文件过滤、关键词搜索、文件签名等内容，帮助读者掌握数字取证基础知识及取证分析工具的基本使用方法。

实验 2.1 加载镜像文件，熟悉不同视图模式

（1）预备知识

1. Winhex 与 X-Ways Forensics 的关系

Winhex 是 X-Ways 公司的 CEO Stefan 在学生时代开发的一个十六进制编辑器，其主要应用于磁盘和内存十六进制编辑，常被用于数据恢复和磁盘编辑，如图 2-1 所示。

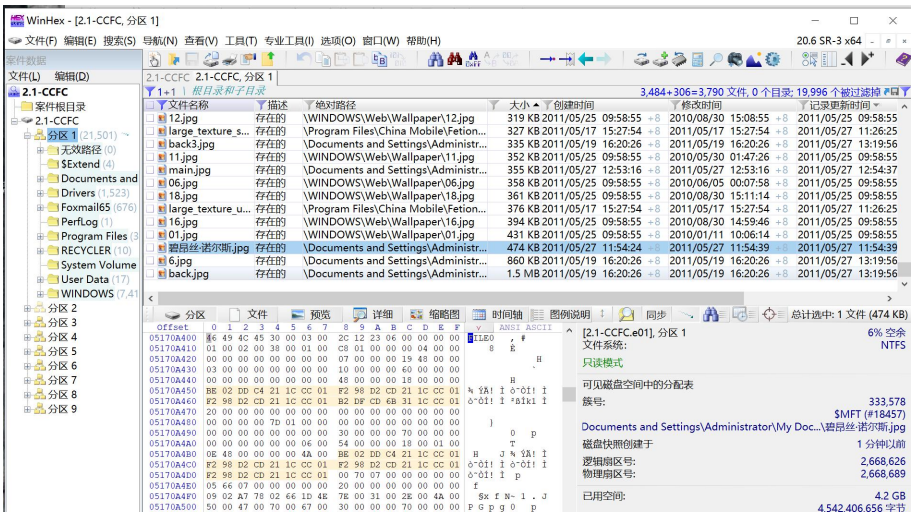

图 2-1 Winhex 20.6 界面

Winhex 功能主要有四个：

- 磁盘克隆、数据镜像
- RAM 内存编辑：对内存信息直接编辑，如调试内存、编译程序等；
- 文件分析：分析文件格式、判断文件类型和数据格式；
- 擦除数据：可对磁盘填充 0 或随机数，是保证数据安全的最佳方式。

X-Ways Forensics 是为计算机取证分析人员提供的一个功能强大的综合取证平台，与 Winhex 紧密结合，使得其能够发现很多其他分析工具无法找到的数据和文件，如图 2-2 所

示。

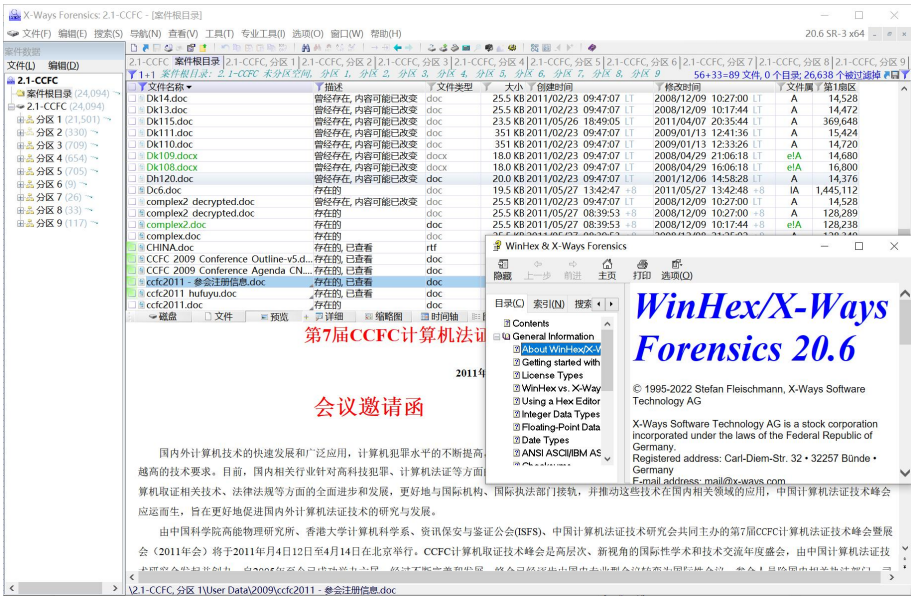

图 2-2 X-Ways Forensics 启动界面

X-Ways Forensics 与 Winhex 是包含关系，X-Ways 软件中含有 Winhex 工具，具备 Winhex 所有的基本功能。X-Ways Forensics 和 Winhex 的主要区别如图 2-3 所示：

	代码	显示界面	下载安装	使用
Winhex	相同的代码基础	名称为Winhex	Winhex需要单独下载作为插件使用，且要放到X-Ways安装目录下	编辑磁盘、镜像
X-Ways		名称为X-Ways		只读模式严格写保护

图 2-3 Winhex 与 X-Ways Forensics 的区别

2. Winhex 软件配置

在启动 Winhex 软件后，首次运行时会呈现英文界面，展示 Winhex 的版权信息提示。关闭 Winhex 帮助文件后，将呈现“General Options”（常规设置）窗口。通过点击菜单中的“Help”，然后选择“Setup”-“中文”，可将软件语言切换至中文。为确保查看便捷，教学环境中的 Winhex 界面已预设为中文，如图 2-4 所示。

常规设置的目标是为取证软件营造一个优越的运行环境，并将个人操作习惯固定化。关键步骤包括勾选“以管理员身份运行”，以及设定临时目录和案件保存目录，从而使用户能够从固定且熟悉的位置获取案件产生的数据。