

网络空间安全学科系列教材

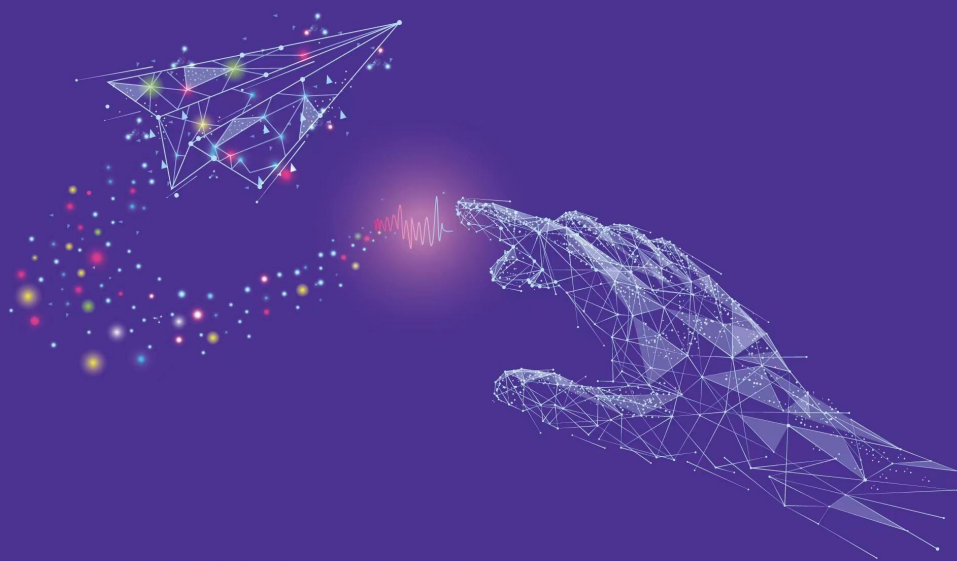
教育部高等学校网络空间安全专业教学指导委员会
中国计算机学会教育专业委员会

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 熊翹楚 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

清华大学出版社

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、熊翹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

目 录	4
第 1 章 数字取证实验教学环境	15
实验 1.1 登录数字取证教训平台	15
(1) 实验目的	15
(2) 实验环境	15
(3) 实验步骤	15
实验 1.2 数字取证教训平台作业与考试系统	16
(1) 实验目的	16
(2) 实验环境	17
(3) 实验步骤	17
实验 1.3 数字取证教训平台取证软件	17
(1) 实验目的	17
(2) 实验环境	17
(3) 实验步骤	17
第 2 章 数字取证基础	19
实验 2.1 加载镜像文件，熟悉不同视图模式	19
(1) 预备知识	19
1. Winhex 与 X-Ways Forensics 的关系	19
2. Winhex 软件配置	20
3. 创建案件	21
4. 视图模式	23
(2) 实验目的	26
(3) 实验环境	26
(4) 实验步骤	26
实验 1 使用 Winhex 创建案件	26
实验 2.2 展开镜像文件目录和文件	26
(1) 预备知识	26
(2) 实验目的	27
(3) 实验环境	27
(4) 实验步骤	27
实验 1 使用 Winhex 练习分区和目录的管理	27
实验 2 使用 Winhex 练习浏览设置	28
实验 2.3 文件过滤与组合过滤	29
(1) 预备知识	29
1. 文件扩展名	29
2. 文件名	29
3. 模糊过滤	29
4. 注意检查过滤条件	29
5. 组合过滤	30
(2) 实验目的	32
(3) 实验环境	32
(4) 实验步骤	32

实验 1 查找所有扩展名为 DOC 和文件名为 Index.dat 的文件	32
实验 2 查找“峰会简版.BAK”的保存位置	33
实验 3 查找所有包含字符 mail 的文件夹	33
实验 4 排除无用文件夹中的 txt 文档	34
实验 5 查找 2011 年 5 月 27 日 13 时之后创建的 doc 文件	34
实验 6 查找所有被删除的 DOC 文件	35
实验 2.4 文件签名	35
(1) 预备知识	36
1. 文件签名	36
2. 文件签名库	36
3. 签名状态	38
(2) 实验目的	38
(3) 实验环境	39
(4) 实验步骤	39
实验 1 判断文件“FILE1”的真实类型	39
实验 2 判断“峰会简版.BAK”文件的真实类型	40
实验 3 发现签名不匹配的文件	40
实验 4 发现签名不匹配的图片	42
实验 5 发现被修改扩展名的压缩文件	44
实验 2.5 文件搜索	45
(1) 预备知识	45
1. 同步搜索	45
2. GREP 搜索	47
3. 文件元数据	47
(2) 实验目的	47
(3) 实验环境	48
(4) 实验步骤	48
实验 1 搜索并恢复镜像中的 JPG 图片文件	48
实验 2 搜索镜像未分区空间中的手机号码	50
实验 3 搜索并提取图片中的缩略图	51
实验 4 搜索内存页面文件中的.cn 域名	52
实验 5 在所有分区中搜索包含关键词“峰会”和“CCFC”的文档	52
实验 6 在搜索结果中搜索	54
实验 7 搜索特定型号手机拍摄的照片	54
实验 8 GREP 搜索	55
实验 9 在缓存文件中搜索曾经查看过的网页邮件	56
实验 10 在内存页面文件 Pagefile.sys 中搜索聊天记录	56
实验 11 分析 DOC 文件的编辑历史	57
实验 12 查找所有 Sprite 编辑过的 Office 文件	58
参考文献	58
第 3 章 证据固定和哈希校验	60
实验 3.1 证据固定	60
(1) 预备知识	60
1. 镜像格式	60

2. 虚拟磁盘文件	62
3. 物理磁盘和逻辑磁盘	63
4. 磁盘快照	63
(2) 实验目的	64
(3) 实验环境	65
(4) 实验内容	65
实验 1 使用 Windows 磁盘管理工具创建一个 VHD 虚拟磁盘	65
实验 2 创建物理磁盘镜像文件	67
实验 3 挂载 Bitlocker 加密磁盘镜像并根据密钥解密	69
实验 4 获取 Bitlocker 解密分区 E01 格式镜像	71
实验 3.2 文件哈希和哈希校验	72
(1) 预备知识	72
1. 哈希值	72
2. 哈希库	73
3. 哈希分类	73
4. 哈希对比	74
(2) 实验目的	74
(3) 实验环境	74
(4) 实验内容	74
实验 1 创建磁盘镜像，并计算哈希值	74
实验 2 校验 E01 文件的哈希值	75
实验 3 计算某个文件的哈希值	76
实验 4 计算所有 DOC 文件的哈希值，并隐藏掉重复的文件	77
实验 5 导入 NSRL 哈希库，创建 NSRL 哈希集	78
实验 6 创建“CDF 关注图片”哈希集	79
实验 7 通过哈希集查找相同的文件	80
参考文献	82
第 4 章 文件系统与数据恢复	83
实验 4.1 文件系统基本属性	83
(1) 预备知识	83
1. MBR 分区	83
2. DBR 分区	84
(2) 实验目的	84
(3) 实验环境	85
(4) 实验内容	85
实验 1 理解 MBR 分区信息	85
实验 2 查看被删除的分区信息	86
实验 3 重新分区后恢复丢失的分区	86
实验 4.2 FAT 文件系统与数据恢复	87
(1) 预备知识	87
1. FAT 文件系统的版本号	88
2. FAT 根目录的位置	88
3. 卷松弛	88
4. 地址转换	88

5. 字节顺序	89
6. FAT 分区引导扇区的数据结构	89
(2) 实验目的	90
(3) 实验环境	90
(4) 实验内容	90
实验 1 分析 FAT 文件系统下删除和格式化后的数据状态	90
实验 2 提取镜像中的图片	92
实验 4.3 NTFS 文件系统与数据分析	93
(1) 预备知识	93
1. NTFS 元数据文件类型	93
2. 主文件表 \$MFT (Master File Table)	94
3. 日志文件 \$LogFile	94
4. 日志文件 \$USNJournal	94
(2) 实验目的	95
(3) 实验环境	95
(4) 实验内容	95
实验 1 在 \$LogFile 中分析指定文件的编辑痕迹	95
实验 2 在 \$LogFile 中分析百度云盘上传或下载文件的痕迹	97
实验 3 在 \$LogFile 中分析文件的删除时间	97
实验 4 通过 \$UsnJournal 日志分析文件造假行为和存储劫持	98
实验 5 NTFS 文件系统格式化后的数据恢复	98
参考文献	100
第 5 章 Windows 取证	101
实验 5.1 卷影复制	101
(1) 预备知识	101
(2) 实验目的	102
(3) 实验环境	102
(4) 实验内容	102
实验 5.2 回收站	103
(1) 预备知识	103
1. Windows XP 下回收站格式分析	103
2. Windows 7 及以后操作系统回收站格式分析	104
(2) 实验目的	105
(3) 实验环境	105
(4) 实验内容	105
实验 1 Windows XP 回收站日志分析	105
实验 2 Windows 10 下被删除的文件夹	106
实验 5.3 缩略图	106
(1) 预备知识	106
1. 不同版本 Windows 操作系统下的缩略图存储方式	107
2. 缩略图文件内容	107
3. 缩略图文件查看方式	108
(2) 实验目的	108
(3) 实验环境	108

(4) 实验内容	108
实验 1 查询图片中的缩略图	108
实验 2 用 WFA 解析 Windows 缩略图	109
实验 5.4 快捷方式	111
(1) 预备知识	111
(2) 实验目的	111
(3) 实验环境	111
(4) 实验内容	111
实验 1 分析一个 LNK 文件的创建时间	111
实验 2 查看目标文件的创建、访问和修改时间	112
实验 5.5 跳转列表	113
(1) 预备知识	113
(2) 实验目的	115
(3) 实验环境	115
(4) 实验内容	115
实验 1 解析跳转列表	115
实验 5.6 预读取	116
(1) 预备知识	116
(2) 实验目的	117
(3) 实验环境	117
(4) 实验内容	117
实验 1 通过 Prefetch 分析安装 QQ 浏览器的时间	117
实验 2 利用 WinPrefetch View 分析预读取文件	118
实验 5.7 远程桌面	119
(1) 预备知识	119
(2) 实验目的	120
(3) 实验环境	120
(4) 实验内容	120
实验 1 远程登录痕迹分析	120
实验 5.8 活动历史记录	121
(1) 预备知识	121
(2) 实验目的	121
(3) 实验环境	122
(4) 实验内容	122
实验 1 分析 Windows 活动历史记录	122
实验 5.9 注册表	122
(1) 预备知识	122
1. 注册表存储位置	123
2. 注册表结构	123
3. CurrentControlSet 控件组	124
4. Shellbag	126
(2) 实验目的	126
(3) 实验环境	126
(4) 实验内容	126

实验 1 注册表配置单元	126
实验 2 注册表分析模板	128
实验 3 系统信息	129
实验 4 应用程序信息	130
实验 5 用户信息	130
实验 6 分析注册表中的 USB 使用痕迹	131
实验 7 USB 设备的连接时间	132
实验 8 分析 USB 设备的连接时间	133
实验 9 查看 USB 设备的最后使用时间	134
实验 10 查看 USB 设备分配的盘符	135
实验 11 分析最近使用过的文件	137
实验 12 Shellbag 中的最近访问文件夹	138
实验 5.10 Windows 事件日志	139
(1) 预备知识	139
(2) 实验目的	141
(3) 实验环境	142
(4) 实验内容	142
实验 1 分析远程登录事件	142
实验 2 USB 设备和分区诊断日志	144
实验 5.11 内存数据取证	145
(1) 预备知识	145
(2) 实验目的	146
(3) 实验环境	146
(4) 实验内容	147
实验 1 获取内存镜像	147
实验 2 使用 Volatility 分析内存镜像	147
实验 3 内存中的注册表	151
参考文献	153
第 6 章 Linux 取证	154
实验 6.1 Linux 痕迹分析	154
(1) 预备知识	154
1.文件系统	154
2.FHS 标准	154
3.Linux 常用命令	155
4.bash_history	156
5.Linux 日志分析	156
6.定时任务	156
(2) 实验目的	157
(3) 实验环境	157
(4) 实验内容	158
实验 1 解析 Linux 系统信息	158
实验 2 Bash_History 痕迹分析	159
实验 3 Linux 日志文件分析	160
实验 6.2 网站取证	161

(1) 预备知识	161
1.服务器镜像文件	161
2.网站重建	162
3.网站的数据库配置文件	162
4. Hosts 文件	162
5. 网站访问日志	163
6. 网站后台密码加密	163
(2) 实验目的	163
(3) 实验环境	163
(4) 实验内容	164
实验 1 校验网站的数据库配置文件, 绑定 Hosts 文件, 访问网站	164
实验 2 获取网站后台地址, 绕过网站后台密码加密	167
实验 3 从数据库中访问后台登录的用户名, 绕过网站后台密码加密	168
参考文献	170
第 7 章 macOS 取证分析	172
实验 7.1 macOS 操作系统痕迹分析	172
(1) 预备知识	172
1.SQLite 数据库	172
2.PList 属性列表文件	174
3.macOS 自动登录和密码	175
(2) 实验目的	175
(3) 实验环境	175
(4) 实验内容	176
实验 1 解析 macOS 系统信息	176
实验 2 解析 macOS 用户信息	179
实验 7.2 分析最近的行为	185
(1) 预备知识	185
(2) 实验目的	186
(3) 实验环境	186
(4) 实验内容	186
实验 1 解析用户最近运行的程序	186
实验 2 分析用户最近打开过哪些图片	187
实验 3 分析 macOS 系统行为痕迹	188
参考文献	189
第 8 章 Android 取证	191
实验 8.1 Android 取证基础	191
(1) 预备知识	191
1. Android 安全与加密	191
2. Android 系统的 ADB	193
(2) 实验目的	194
(3) 实验环境	194
(4) 实验内容	195
实验 1 开启 USB 调试准备联机取证	195
实验 2 通过 ADB 指令查看和修改权限	195

实验 3 通过 ADB 指令判断设备的加密类型	196
实验 8.2 Root 权限的获取与锁屏密码的破解	197
(1) 预备知识	197
1. 获取 Root 权限的方法	197
2. Android 的工作模式	199
3. Android 的 Bootloader	199
4. Android 的屏幕锁	200
(2) 实验目的	201
(3) 实验环境	201
(4) 实验内容	201
实验 1 手机工作模式的切换方法	201
实验 2 通过刷入 TWRP 获取 Root 权限	202
实验 3 突破 Android 设备的锁屏密码	204
实验 8.3 Android 设备数据的获取与分析	205
(1) 预备知识	205
1. 数据提取方法	205
2. Android 数据的分区结构和数据	207
(2) 实验目的	210
(3) 实验环境	210
(4) 实验内容	210
实验 1 使用 Android Backup 获取数据	210
实验 2 解析 Android Backup 备份数据	211
实验 3 使用小米手机内置备份工具备份数据	212
实验 4 小米手机备份数据解析	213
参考文献	215
第 9 章 高级取证	216
实验 9.1 iTunes 备份解析	216
(1) 预备知识	216
1. iTunes 备份	216
2. 备份中的重要文件	216
(2) 实验目的	217
(3) 实验环境	217
(4) 实验内容	217
实验 1 查看 iTunes 备份基本信息	217
实验 2 查看 Status.plist 基本信息	218
实验 3 查看 Manifest.db 中的文件信息	219
实验 4 查看 Manifest.plist 中的文件信息和配合解密	219
实验 9.2 解析系统内置 APP 的信息	220
(1) 预备知识	220
(2) 实验目的	221
(3) 实验环境	221
(4) 实验内容	221
实验 1 解析通讯录	221
实验 2 解析通话记录	222

实验 3 解析 WIFI 连接记录	222
参考文献	223
第 10 章 应用程序取证分析	224
实验 10.1 云数据分析	224
(1) 预备知识	224
1.BaiduYunCacheFileV0.db	225
2.BaiduYunGuanjia.db	225
3.BaiduYunRecentV0.db	225
4.BaiduYunMBoxV0.db	225
5.上传和下载的痕迹	225
(2) 实验目的	226
(3) 实验环境	226
(4) 实验内容	226
实验 1 利用 Myhex 分析百度云盘传输痕迹	226
实验 2 分析百度云盘上传下载过程中的残留痕迹	227
实验 10.2 即时通讯痕迹分析	229
(1) 预备知识	229
1. 微信数据库解析	230
2. 微信数据恢复	230
(2) 实验目的	231
(3) 实验环境	231
(4) 实验内容	231
实验 1 利用 Myhex 分析安卓端微信数据库	231
实验 10.3 电子邮件取证分析	234
(1) 预备知识	234
1. Outlook 客户端	235
2.Foxmail 客户端	235
3.邮件头格式	235
4.邮件附件	236
5.邮件传输过程	236
(2) 实验目的	236
(3) 实验环境	237
(4) 实验内容	237
实验 1 分析电子邮件来自哪个邮箱	237
实验 2 解析 Thunderbird 邮箱	238
实验 10.4 浏览器历史记录分析	239
(1) 预备知识	239
1. Index.DAT 和 WebCacheV01.dat	239
2.Index.dat 数据列解析	240
(2) 实验目的	241
(3) 实验环境	241
(4) 实验内容	241
实验 1 根据浏览器历史记录分析用户行为痕迹	241
参考文献	243

第 11 章 高级取证	245
实验 11.1 小米手环日志分析	245
(2) 预备知识	245
(2) 实验目的	245
(3) 实验环境	245
(4) 实验内容	245
实验 1 解析小米手环日志	245
实验 11.2 树莓派家庭娱乐中心镜像分析	248
(1) 预备知识	248
(2) 实验目的	248
(3) 实验环境	248
(4) 实验内容	248
实验 1 解析树莓派镜像系统信息	248
实验 2 分析 Raspberry Pi 中 Kodi 的使用痕迹	251
实验 11.3 无线路由器痕迹分析	253
(1) 预备知识	253
(2) 实验目的	253
(3) 实验环境	253
(4) 实验内容	254
实验 1 解析 OnHub 无线路由器诊断报告	254
实验 11.4 无人机飞行记录	256
(1) 预备知识	256
(2) 实验目的	256
(3) 实验环境	257
(4) 实验内容	257
实验 1 解析无人机历史记录	257
参考文献	261
第 12 章 取证的挑战	262
实验 12.1 加密文件破解	262
(1) 预备知识	262
(2) 实验目的	263
(3) 实验环境	263
(4) 实验内容	263
实验 1 利用 Winhex 查找加密文件	263
实验 2 利用 Passware 查找加密文件	264
实验 3 破解 VC 加密容器	265
实验 12.2 数据隐藏	267
(1) 预备知识	267
1. ADS 数据流	267
2. OOXML 文件	268
3. 松弛空间	270
(2) 实验目的	270
(3) 实验环境	270

(4) 实验内容	270
实验 1 创建 ADS 数据流	270
实验 2 查找 ADS 数据流	271
实验 3 查看文件松弛空间中存在的密码	272
实验 4 修复被修改的文件头	273
实验 12.3 数据擦除	274
(1) 预备知识	274
(2) 实验目的	275
(3) 实验环境	275
(4) 实验内容	275
实验 1 利用 Winhex 擦除文件	275
实验 2 擦除痕迹分析	277
参考文献	278

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。

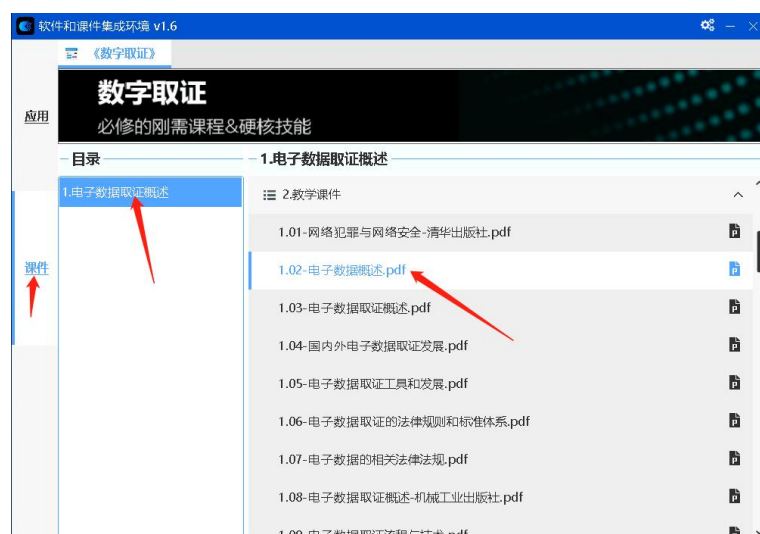


图 1-3 平台内课件等教学资源

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。

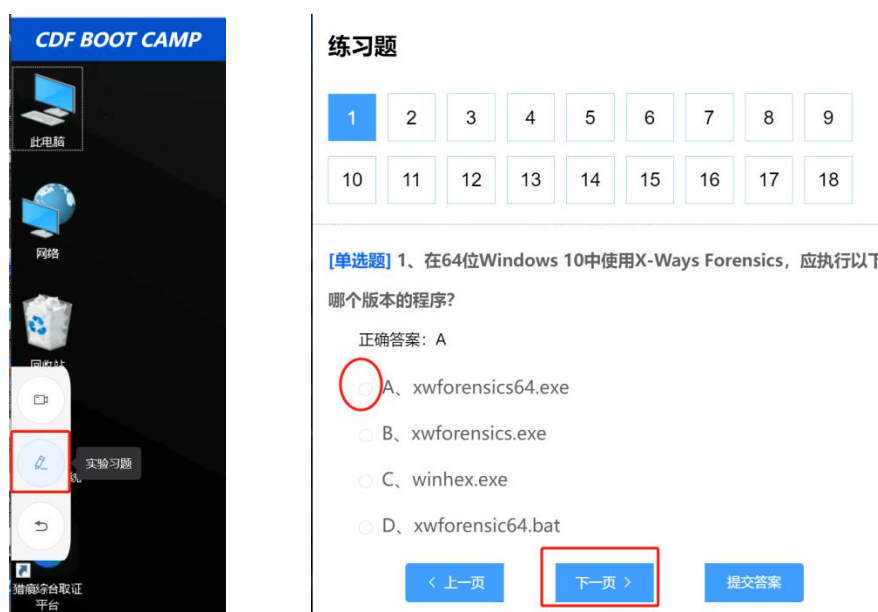


图 1-4 作业系统

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。

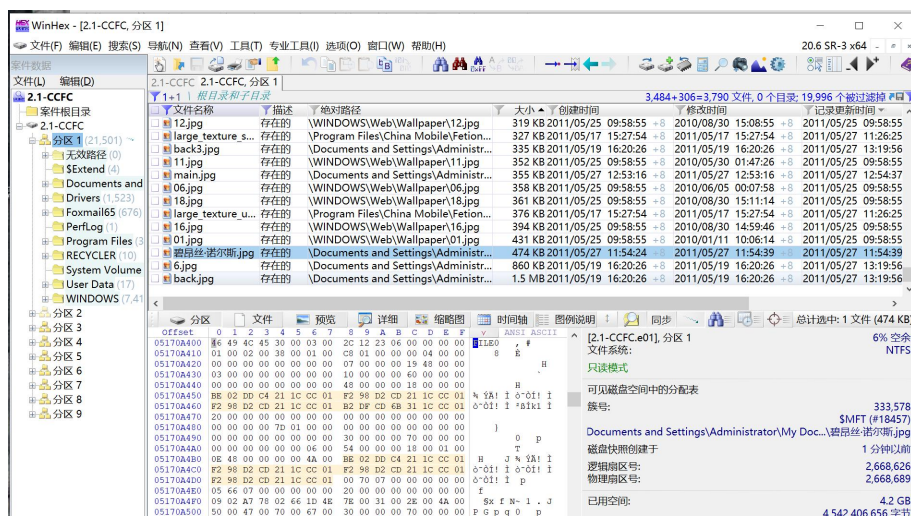


图 2-1 Winhex 20.6 界面

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。

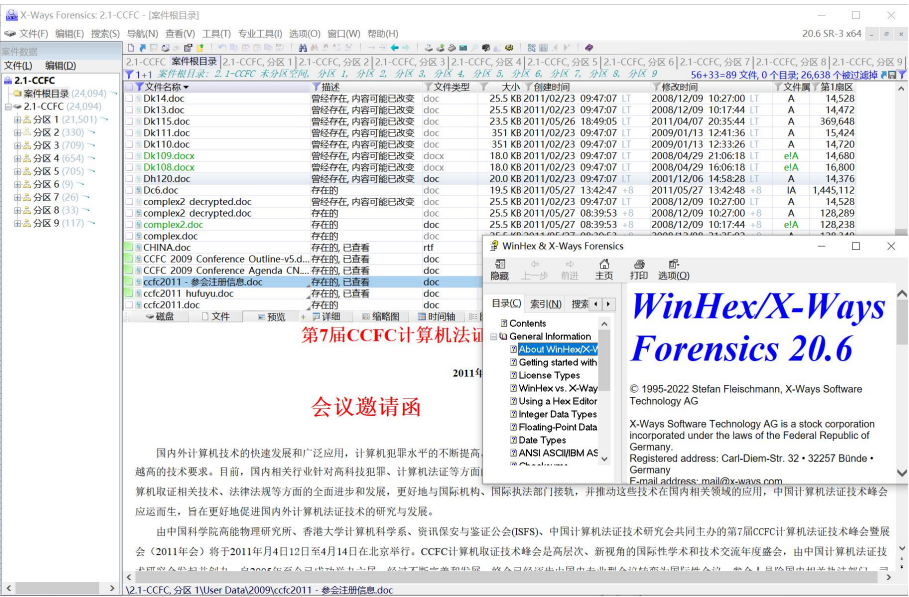


图 2-2 X-Ways Forensics 启动界面

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。