辽宁职业技术大学

教 案

（2025-2026 学年 第 1 学期）

课程名称： 数字取证与司法鉴定

课程类别（总学时）： 考试（48 学时）

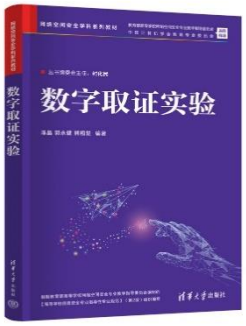
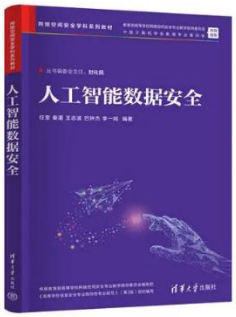
主讲教师： 郭睿思

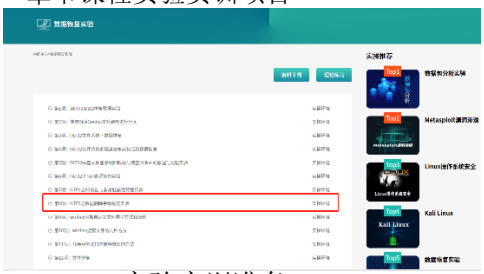
开课单位： 信息工程学院

授课班级： 2023 级信息安全与管理（本）一班

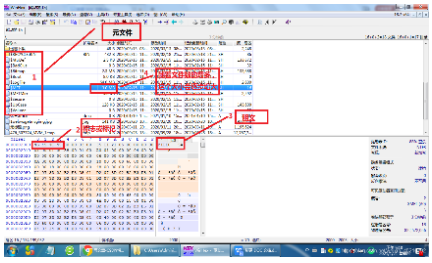
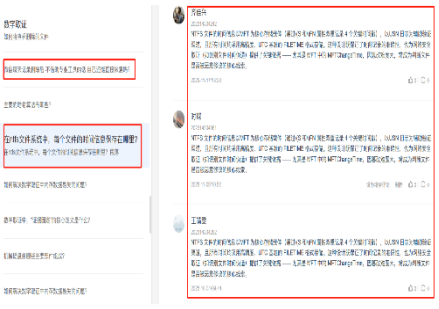
2023 级信息安全与管理（本）四班

2023 级信息安全与管理（本）五班

<table>
<tr><td>授课题目</td><td colspan="3">项目四：文件系统与数据恢复—任务二：NTFS 文件系统</td></tr>
<tr><td>学时</td><td>2</td><td>授课顺序</td><td>14</td></tr>
<tr><td>授课地点</td><td>信息工程学院网络安全攻防实训室</td><td>授课形式</td><td>理实一体化</td></tr>
<tr><td>参考文献</td><td colspan="3">本课程选用教育部高等学校网络空间安全专业规划教材《数字取证》 作为核心理论教材，严格对接专业人才培养方案与课程标准。课程以《数字取证实验》为实训指导教材，对数字取证课程进行了模块重构，突出实践技能培养，更适合职业本科专业学生的学习和理解；辅以《人工智能数据安全》拓展前沿领域知识。三者共同构建“理论—实验—拓展”三位一体的教学资源体系，效支撑职业本科学生实现从基础到综合、从技术到应的阶梯式能力成长。
    </td></tr>
<tr><td>数字教学资源</td><td colspan="3">● 雨课堂平台（发布课前导学任务）
● 国家职业教育智慧教育平台（课前导学）
● 项目实训平台（课中实战）
● DIDCTF-电子数据取证综合平台网站（拓展训练）
● Deepseek、KIMI、百度网站（行业典型案例、提供脱敏练习数据）
● 中国司法鉴定网站（职业理念融入）
● 党史学习教育网站（课程思政案例）</td></tr>
<tr><td rowspan="3">教学目标</td><td>知识目标</td><td colspan="2">● 理解 NTFS 文件系统的逻辑结构与数据组织方式
● 识别 NTFS 核心元文件的功能与作用
● 掌握主文件表（MFT）的条目结构和取证属性【难点】</td></tr>
<tr><td>能力目标</td><td colspan="2">● 能使用 Winhex 工具打开 MFT 样本并进行相关操作与分析【重点】
● 能基于文件系统进行磁盘数据恢复的能力。【重点】</td></tr>
<tr><td>素质目标</td><td colspan="2">● 了解我国数字取证主流技术与成就，增强民族自豪感；
● 牢固法律意识和证据思维，强化学生的保密意识与隐私保护观念
● 秉持工匠精神，追求客观精准，养成严谨、细致的职业习惯。</td></tr>
</table>

<table>
<tr><td>教学重点</td><td colspan="3">● 主文件表（MFT）的取证属性：重点讲解$DATA、$FILENAME
● 训练学生使用 WinHex 工具定位、解析 NTFS 条目
● 完成对文件的创建、访问、修改等行为</td></tr>
<tr><td>教学难点</td><td colspan="3">● MFT 中常驻属性与非常驻属性的存储差异及对取证的影响
● NTFS 文件系统中的磁盘破坏和恢复</td></tr>
<tr><td>教法</td><td>项目驱动法、案例分析法
讨论法、讲授法、演示法</td><td>学法</td><td>自主学习、小组讨论、实践操作</td></tr>
<tr><td>教学准备</td><td colspan="3">本课程内容依据《数字取证》教材第五部分，并结合《数字取证实验（NTFS 文件系统与数据分析）》教材中项目 4 的相关实践环节，进行教学设计。课程聚焦于数字取证核心技能中的文件系统痕迹分析，同时融入网络安全工程师认证相关能力要求，提炼出重点教学内容：NTFS 文件系统元数据分析。在教学过程中，重点围绕 MFT 条目结构解析这一子模块展开。授课内容紧扣技术关键点，既涵盖 NTFS 文件系统的关键元数据结构与属性分析，也为后续深入学习文件恢复、日志分析等模块奠定扎实基础。
● 课前雨课堂讨论发布 ● 理论讲授可视化漫画 ● 模拟测试的教具 u 盘
    </td></tr>
<tr><td>教材处理及数字化资源情况</td><td colspan="3">●章节内容数字化思维导图
 
●网络攻防实战项目平台
 
●章节课程实验实训项目
 
●Winhex 实验实训准备
  </td></tr>
</table>

<table>
<tr><td colspan="5">教学实施</td></tr>
<tr><td colspan="5">课前活动</td></tr>
<tr><td>教学环节</td><td>教学内容</td><td>教师活动</td><td>学生活动</td><td>设计意图（含课程思政元素）</td></tr>
<tr><td rowspan="4">自主学测、反馈学情（5 分钟）</td><td>登陆雨课堂教学平台，发布 NTFS 解析预习资源包：包含一个以数据窃取调查为背景的微案例（约 150 字）、一段核心知识精讲视频，并明确教材中“NTFS-MFT 条目结构与属性”章节。更新操作的学习任务单，明确学习目
标及具体要求：

●观看学习：观看视频，精读教材中 MFT 条目与属性章节。
 
●初步理解 MFT 的核心作用与基本结构，为课堂解析实操奠定基础。
 
●完成思考题：结合微案例，思考并简要记录定位已删除文件时需重点分析的 MFT 属性与标志位
  </td><td>●任务发布
雨课堂发布微案例、一段核心知识精讲视频，并明确教材中本章节对应位置。要求学生基于案例与视频，自主探究文件系统痕迹分析方法，并回答引导性问题。

●学情分析
校企教师查看和分析学生学习情况，明确学习兴趣点、普遍的知识盲区和教学侧重点。

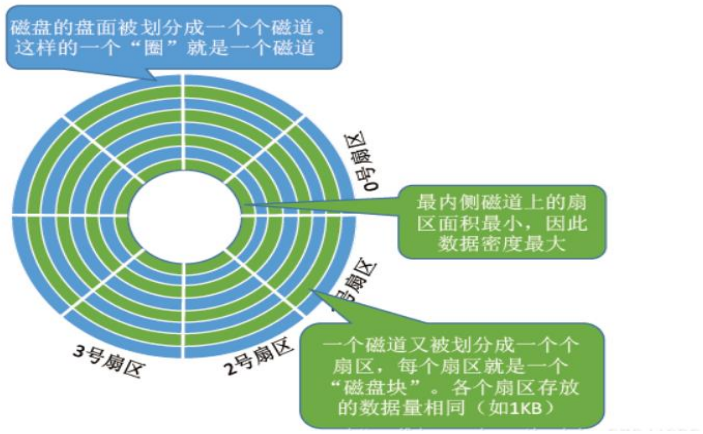
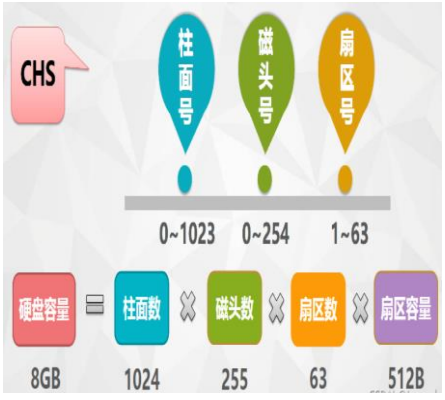
●策略制定
根据学情分析制定本节课的教学策略，进行精细化教学准备（实训样本、应用工具等）</td><td>●自主学习
根据任务清单学生到雨课堂平台完成对应知识点的学习。完成教师发布的视频及导学任务。

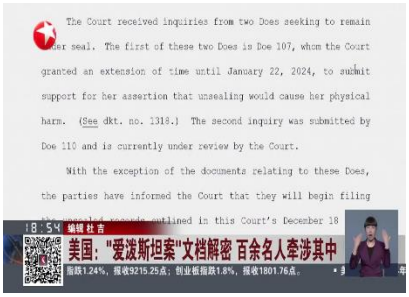
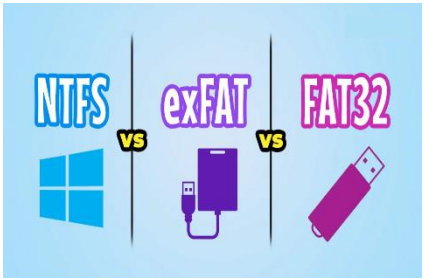
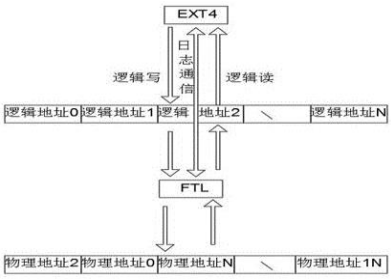
●自主探究
学习完成课程后，学生要自主查看课程项目，回答思考题并尝试给出具体的实施步骤。

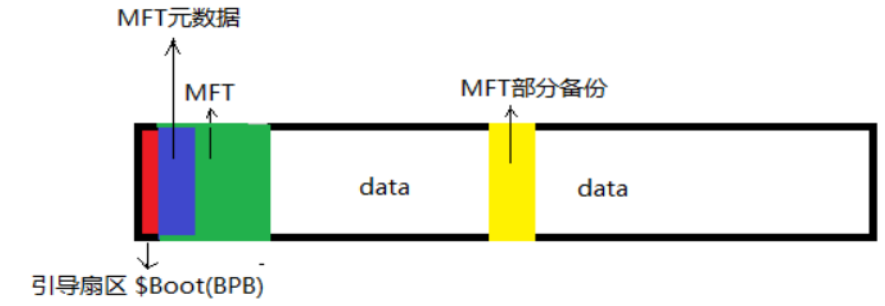
●课前反馈
完成教师发布的讨论与测试；
提出问题和重点想了解的领域等。</td><td>●民族自信
通过官网真实取证案例，展示数字取证技术在打击违法犯罪中的实际应用，让学生感受技术的社会价值，增强国家技术自信与民族自豪感；

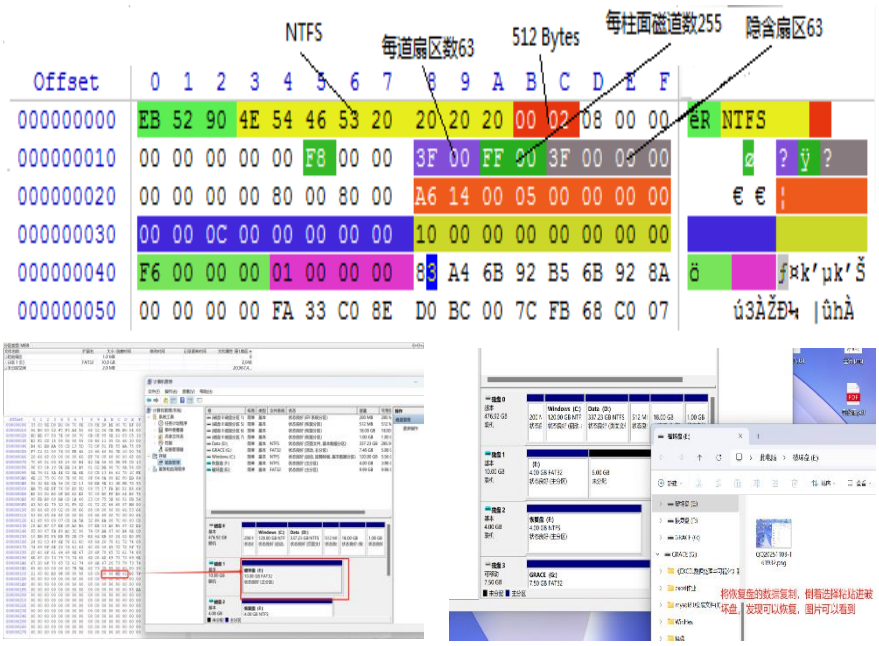
●工匠精神
将企业项目验收标准作为评价考核依据，塑造学生精益求精的工匠精神；

●职业精神
教师全方位监，督检查学生学习状态，培养科学严谨的学习态度和工作作风；</td></tr>
</table>

课堂实施		
教学环节	教学内容	
一、复习回顾 （3分钟）	**复习内容：** 1. **硬盘中常见的术语：** ■ 柱面：同一磁道构成的圆柱面 ■ 磁道：磁头旋转形成的轨迹 ■ 扇区：硬盘读写的基本单位，通常大小为 512 字节 ■ 块：Linux 操作系统中硬盘管理的最小单位 ■ 分区：操作系统中对硬盘进行逻辑管理的区域 ■ 卷：操作系统或应用程序用来存储数据可寻址的扇区集合  **2. 寻址方式** ■ CHS 寻址：C(柱面号)；H(磁头号)；S(扇区号) ■ LBA 寻址：逻辑块寻址，所有扇区从 0 开始编号   ■ 复习后提问：之前学习的 MBR 和 GPT 分区系统中，哪种更适合搭配 NTFS 文件系统？（GPT 支持大容量，适配 NTFS 的大分区需求）； ■ 追问：若取证时发现 windows 操作系统某分区的文件被删除，想追溯删除时间，依赖什么功能可实现追溯？（引出 NTFS 文件系统-日志功能）	通过提问+可视化图片讲解，帮助学生快速回忆上节课涉及的知识技能，以用于本节项目实战的基础知识实现衔接。

二、案例导入 （5分钟）	**案例新课导入：**情境案例，引发思考（2 分钟） 通过葫芦岛征信案、爱泼斯坦案中的电子证据提取工程案例，引入课程驱动项目：NTFS 文件系统结构解析与元文件 MFT 核心属性分析，进而导入本节 “NTFS 文件系统与数据恢复核心技术” 课程内容 **1. 爱泼斯坦案：** http://m.toutiao.com/group/7586883105315701282/?upstream_biz=doubao **2. 辽宁葫芦岛帮信案：** https://m.gmw.cn/2025-12/03/content_1304248721.htm   **学习目标：** 1. 掌握 NTFS、ext4、FAT32 三种主流文件系统的核心特性 2. 掌握 NTFS 文件系统结构及各类重要元文件 3. 掌握 MFT（主文件表）的三类核心取证属性(10H\30H\80H) 4. 能够独立运用 WinHex 软件完成虚拟磁盘的指定区域破坏操作，并基于文件系统原理实现虚拟磁盘数据的有效恢复	创设案例情景，师生交流引导思考 分析完成项目方法引出教学内容 同时思政方面引导学生关注时事，提升法律意识
三、新知学习 （15分钟）	**核心理论知识点讲解：** **1. 三种主流文件系统的核心特性** （1）Windows 系统——NTFS （2）Linux 系统——EXT4 （3）移动存储设备——FAT(FAT32、EXFAT)   **2. NTFS 文件系统的结构** （1）概念：是微软设计的一种高性能、高可靠性的日志型文件系统 （2）结构构成：NTFS 文件系统的结构采用分区域分层存储的设计，核心围绕**引导区、主文件表（MFT）、数据区**三大模块构建，同时包含元文件、位图等关键组件，确保文件管理的高效性与可靠性。 ■ 引导区：位于 NTFS 分区的第 0 个扇区，是分区的起始标识区域 ■ 主文件表：核心管理组件，相当于文件系统的“数据库索引” ■ 数据区：是存储用户文件实际数据的区域 ■ 元文件：责维护文件系统的结构、状态和运行逻辑	通过项目驱动式学习引导学生构建符合工程实践标准的文件系统分析与应用体系； 结合文件系统在数据安全领域应用，讲述科研工作者攻克技术难题的事迹，帮助学生树立国家自信、民族自信；

	3. MFT（主文件表）   ■ 10H 属性(标准信息属性)：$Standard Information ■ 30H 属性（文件名称属性）：$File Name ■ 80H 属性（数据属性）：$Data	在辨析不同文件系统特性、解析 NTFS 复杂结构的过程中，培养学生科学严谨的学习态度和工作作风，塑造其精益求精的工匠精神。
四、翻转课堂（12分钟）	1. 提问：针对项目工作任务清单中的难点问题，结合课前导入案例，讨论分析“**如何把 NTFS 文件系统中已经被删除的数据进行恢复？或发现相关的删除时间、文件大小等线索？**”  2. 学生分组讨论、实践试错、总结实施方案，并以小组为单位进行项目方案汇报。 3. 教师归纳点评，以将 NTFS 文件系统比作 “一间藏着数据线索的密室”，删除文件的恢复任务就是 “密室解谜”游戏的生动比喻进行讲解，帮助学生更好记忆。	增强沟通协作能力，培养自创新思维和自主探究精神

五、示范操作（15 分钟）	使用 Winhex 软件操作示范如何利用 NTFS 的结构特点，查看关键的取证信息，帮助学生完成任务清单中的难点问题，掌握项目实战实操的技能要点。  	构成理论知识转化为实践应用的思维闭环，使学生深刻意识到一切应实际出发，理论联系实际
六、项目实践（25分钟）	**实践课堂：** 教师明确项目任务要求、验收标准以及规范编码，学生分组进行项目实践 **项目实施步骤：** 1 请按要求创建 2 个指定参数的虚拟硬盘（VHD），命名分别为 “破坏盘”和“恢复盘”；其中破坏盘容量 10GB、文件系统为 FAT32。恢复盘容量 4GB、文件系统为 NTFS，请配置相关的参数。 2. 使用 WinHex 工具对 FAT32 格式的 “破坏盘” 执行全量 0 覆盖操作模拟数据损坏 3. 借助 NTFS 格式的 “恢复盘” 完成数据恢复， 要求恢复位置 1：更改文件系统的类型 要求恢复位置 2：更改文件的大小 （注意：物理格式的对齐操作否则影响恢复结果，全程需记录关键操作步骤并截图展示。	教师全方位监督检查学生学习状态，培养科学严谨的学习态度和工作作风
七、评价总结（15 分钟）	1. 学生进行项目成果汇报、答辩路演； 2. 教师依据项目规范和职业标准进行成果点评； 3. 总结课程内容，并布置课后作业。	提升团队协作及沟通能力
八、拓展与作业	1. 下发指导意见及建议； 2. 学生复盘课程内容，自我评价，优化项目，并撰写实验报告； 3. 参与相关双创竞赛，考取职业技能等级证	将企业级标准和竞赛内容融入于课堂之中

<table>
<tr><td>板书设计</td><td colspan="2"> 
</td></tr>
<tr><td rowspan="4">教学与评价（重点关注：教学效果、教学不足、整改措施、教学评价等要素</td><td>教学效果</td><td>课前提前下发工作任务清单的方式，可以有效提升学生对于本节课讲授的知识技能以及实战项目的知识储备，教学环节推进流畅，学生听课注意力集中，项目实践效果显著，应全面推广。</td></tr>
<tr><td>教学不足</td><td>1.课堂使用 AIGC 应用不足，应训练学生检测使用 AI 脱敏数据；借助大模型辅助复杂案件分析
2.过程性考核评价体系有待完善，实操和翻转课堂进行过程中的学生报告与实操评价，应继续精进可量化指标，减少教师主观评价。</td></tr>
<tr><td>整改措施</td><td>1.每月更新脱敏案例库，引入 AIGC 深度伪造取证、物联网取证等前沿案例
2.减少主观评价，增加“随堂技能小测”和“阶段性实验报告”等量化指标</td></tr>
<tr><td>教学评价</td><td>细化课前任务、课堂表现、上机测验、团队协作、完成时间、项目成果、职业规范、编码能力、汇报路演、拓展作业十个考核评价指标，全过程多元化考核学生的理论运用、实践技能、职业素养、思创意识四个维度的达成度。</td></tr>
</table>