高等院校网络空间安全专业实战化人才培养系列教材

郭启全　丛书主编

数字勘查与取证技术

王新猛　郭启全　吴育宝　吴玉强　杨一涛　田素诚　刘云恒　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书共 13 章，围绕“数字勘查与取证技术”这一主题，系统介绍数字勘查取证的基础知识和相关技术。其中，第 1 章概括性介绍电子数据取证技术，包括电子数据等基本概念，电子数据取证技术在维护网络空间安全中的作用、应用领域以及发展趋势等。第 2 章介绍数字现场勘查相关法律法规与现场勘查方法，包括数字现场勘查相关法律、取证技术标准化发展现状、本地现场勘查、在线提取以及远程勘验。第 3 章介绍数字取证技术基础知识，包括常用软硬件工具、字符编码、文件签名、文件过滤、数据搜索和系统仿真。第 4 章介绍文件系统与数据恢复技术，包括存储介质基础知识、数据恢复原理、磁盘分区模式、文件系统基础以及 RAID 重组。第 5 章介绍检材固定，包括制作固定的形式、制作镜像文件过程、哈希和哈希库以及其他固定方法。第 6 章介绍 Windows 系统的调查取证，包括 Windows 系统常规检验、注册表的调查取证、Windows 系统日志调查取证、内存调查取证、浏览器调查取证，以及回收站调查取证。第 7 章介绍 Linux 系统的勘查取证，包括 Linux 系统简介、Linux 文件分析、Linux 日志取证分析。第 8 章介绍 macOS 的勘查取证，包括 macOS 系统简介、文件分析，以及面向 plist 文件的分析。第 9 章介绍移动终端的勘查取证，包括手机勘查取证的流程、SIM 卡的勘查取证、Android 的勘查取证、iOS 的勘查取证、HarmonyOS 的勘查取证以及其他取证方法。第 10 章介绍物联网取证，包括物联网概述、典型应用、关键技术以及常见物联网设备调查方法。第 11 章介绍汽车车载电子数据取证，包括汽车取证概述、车载自动诊断系统、汽车事件数据记录系统、车载 T-Box，以及汽车车载电子数据取证基本过程。第 12 章介绍工业互联网环境调查取证，包括工业互联网环境的基本含义、安全风险、典型工业互联网拓扑结构，以及 PLC 与上位机取证分析。第 13 章介绍典型案例调查取证分析，包括某网站被入侵案件的勘查取证、某服务器镜像内数据库的勘查取证、某勒索病毒案件数字取证分析，以及某工控网络入侵案件的勘查取证。

本书是高等院校网络空间安全专业实战化人才培养系列教材之一，可作为网络空间安全专业的专业课教材，适合网络空间安全专业、信息安全专业以及相关专业的大学生、研究生系统学习，也适合各单位各部门从事网络安全工作者、科研机构和网络安全企业的研究人员阅读。

图书在版编目（CIP）数据

数字勘查与取证技术 / 王新猛等编著. -- 北京 : 电子工业出版社, 2025. 7. -- ISBN 978-7-121-50322-1

Ⅰ. D918.4

中国国家版本馆 CIP 数据核字第 2025X3K279 号

责任编辑：刘御廷　　文字编辑：叶文涛

印　　刷：

装　　订：

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱　　邮编：100036

开　　本：787 × 1 092　1/16　印张：15.75　字数：378 千字

版　　次：2025 年 7 月第 1 版

印　　次：2025 年 7 月第 1 次印刷

定　　价：69.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：lyt@phei.com.cn。

高等院校网络空间安全专业
实战化人才培养系列教材

编委会

序 FOREWORD

在数字化智慧化高速发展的今天，网络和数据安全的重要性愈发凸显，直接关系到国家政治、经济、国防、文化、社会等各个领域的安全和发展。网络空间技术对抗能力是国家整体实力的重要方面，面对日益复杂的网络安全威胁和挑战，按照“打造一支攻防兼备的队伍，开展一组实战行动，建设一批网络与数据安全基地”的思路，培养具有实战化能力的网络安全人才队伍，已成为国家重大战略需求。

一、培养网络安全实战化人才的根本目的

在网络安全“三化六防”（实战化、体系化、常态化；动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控）理念的指引下，网络安全业务越来越贴近实战。实战行动和实战措施都离不开实战化人才队伍的支撑。培养网络安全实战化人才的根本目的，在于培养一批既具备扎实的理论基础，又掌握高新技术和前沿技术、具备攻防技术对抗能力，还能灵活运用各种技术措施和手段，应对各种网络安全威胁的高素质实战化人才，打造“攻防兼备”和具有网络安全新质战斗力的队伍，支撑国家网络安全整体实战能力的提升。

二、培养网络安全实战化人才的重大意义

习近平总书记强调：“网络空间的竞争，归根结底是人才竞争”，“网络安全的本质在对抗，对抗的本质在攻防两端能力较量”。要建设网络强国，必须打造一支高素质的网络安全实战化人才队伍。我国网络安全人才特别是实战化人才严重缺乏，因此，破解难题，从网络安全保卫、保护、保障三个方面加强实战化人才教育训练，已成为国家重大战略需求。

当前，国家在加快推进数字化智慧化建设，本质是打造数字化生态，而数字化建设面临的最大威胁是网络攻击。与此同时，国家网络安全进入新时代，新时代网络安全最显著的特征是技术对抗。因此，新时代要求我们要树立新理念、采取新举措，从网络安全、数据安全、人工智能安全等方面，大力培养实战化人才队伍，加强“网络备战”，提升队伍的技术对抗和应急处突能力，有效应对新威胁和新技术带来的新挑战，为国家经济发展保驾护航。

三、构建新型网络安全实战化人才教育训练体系

为全面提升我国网络安全领域的实战化人才培养能力和水平，按照“理论支撑技术、技术支撑实战”的理念，创新高等院校及社会差异化实战人才培养的思路和方法，建立新型实战化人才教育训练体系。遵循“问题导向、实战引领、体系化设计、督办落实”四项原则，认真落实“制定实战型教育训练体系规划、建设实战型课程体系、建设实战型师资队伍、建设实战型系列教材、建设实战型实训环境、以实战行动提升实战能力、创新实战

型教育训练模式、加强指导和督办落实”八项重大措施，形成实战化人才培养的“四梁八柱”，有力提升网络安全人才队伍的新质战斗力。

四、精心打造高等院校网络空间安全专业实战化人才培养系列教材

在有关部门的大力支持下，具有 20 多年网络安全实战经验的资深专家统筹规划和整体设计，会同 20 多位部委、高等院校、科研机构、大型企业具有丰富实战经验和教学经验的专家学者，共同打造了 14 部技术先进、案例鲜活、贴近实战的高等院校网络空间安全专业实战化人才培养系列教材，由电子工业出版社出版，以期贡献给读者最高水平、最强实战的网络安全重要知识、核心技术和能力，满足高等院校和社会培养实战化人才的迫切需要。

网络安全实战化人才队伍培养是一项长期而艰巨的任务，按照教、训、战一体化原则，以国家战略为引领，以法规政策标准为遵循，以系统化措施为抓手，政府、高校、企业和社会各界应共同努力，加快推进我国网络安全实战化人才培养，为筑梦网络强国、护航中国式现代化贡献我们的智慧和力量！

郭启全

前言 PREFACE

随着移动互联网、物联网、大数据、云计算等技术的广泛应用，人类社会进入了数据化时代，数据规模呈指数级增长。这些数据不仅记录了人类活动，也成为各类社会活动、经济行为，以及司法诉讼中不可或缺的信息载体。因此，对于电子数据收集、提取、分析及展示等技术的研究与应用就显得尤为必要。实践证明，数字勘查与取证技术在打击网络违法犯罪、防范网络攻击、维护网络空间秩序和安全等方面作用凸显，成为构建网络空间安全保障体系不可或缺的重要组成部分。

进入新时代，网络安全最显著的特征是技术对抗，应树立新理念，采取新举措，立足有效应对大规模网络攻击，认真落实“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施，按照“打造一支攻防兼备的队伍，开展一组实战演习行动，建设一批网络与数据安全基地”这条主线，加强战略谋划和战术设计，建立完善的网络安全综合防御体系，大力提升综合防御能力和技术对抗能力。从创新角度出发，按照“理论支撑技术、技术支撑实战”的理念，加强理论创新和技术突破，实施“挂图作战”；从“打造一支攻防兼备的队伍”出发，创新高等院校和企业差异化网络安全人才培养思路和方法，建立实战化人才教育训练体系，加强教育训练体系规划，强化课程体系、师资队伍、系列教材、实训环境建设和培养模式创新，培养网络安全实战化人才。

为了满足培养网络安全实战化人才的需要，郭启全组织成立编委会，共同编著高等院校网络空间安全专业实战化人才培养系列教材，包括《网络安全保护制度与实施》《网络安全建设与运营》《网络空间安全技术》《商用密码应用技术》《数据安全管理与技术》《人工智能安全治理与技术》《网络安全事件处置与追踪溯源技术》《网络安全检测评估技术与方法》《网络安全威胁情报分析与挖掘技术》《数字勘查与取证技术》《恶意代码分析与检测技术》《恶意代码分析与检测技术实验指导书》《漏洞挖掘与渗透测试技术》《网络空间安全导论》。郭启全统筹规划和整体设计全套教材，组织具有丰富的网络安全实战经验和教学经验的专家学者撰写这套高等院校网络空间安全专业教材，并对内容严格把关，以期贡献给读者最高水平、最强实战的网络安全、数据安全、人工智能安全等方面的重要知识。

本书共分 13 章，由王新猛、郭启全等编著。具体编写情况如下：第 1 章网络空间安全概述，由王新猛编写；第 2 章数字现场勘查，由吴育宝、刘云恒编写；第 3 章数字取证技术基础知识，由刘云恒编写。第 4 章文件系统与数据恢复技术，由田素诚编写；第 5 章检材固定，由吴玉强编写；第 6 章 Windows 系统的调查取证，由吴玉强编写；第 7 章 Linux 系统的勘查取证，由杨一涛编写；第 8 章 macOS 的勘查取证，由杨一涛编写；第

9 章移动终端的勘查取证，由钱珺编写；第 10 章物联网取证，由钱珺编写；第 11 章汽车车载电子数据取证，由邹柏林编写；第 12 章工业互联网环境调查取证，由邹柏林编写；第 13 章典型案例调查取证分析，由吴育宝、高宇编写。全书由郭启全统稿。本书内容翔实，展现了作者丰富的实战经验，通过对典型案例的分析，全方位、多层次展示数字勘查与取证的完整过程，旨在为广大学习者、研究者和从业者提供一本系统性、实用性强的教材。

感谢所有为本书提供宝贵资料、建议和指导的专家们。我们将持续关注数字取证领域的最新动态和发展趋势，适时对教材进行更新和完善，以期更好地满足教学科研需求，服务于国家法治建设和网络安全事业发展。

书中不足之处，敬请指正。

作者

目录 CONTENTS

第 3 章

数字取证技术基础知识

第 4 章

文件系统与数据恢复技术

第 1 章 网络空间安全概述

本章主要介绍数字勘查与取证技术的相关概念解析、电子数据取证技术在维护网络空间安全中的重要作用、电子数据取证技术的在其他领域中的应用、电子数据取证技术的发展趋势，为深入学习数字勘查与取证技术奠定基础。

1.1 相关概念解析

数字勘查与取证的对象是电子数据，电子数据的由来与计算机和信息技术的发展密切相关。电子数据可以追溯到 20 世纪中叶，第一台电子计算机 ENIAC 于 1946 年在美国宾夕法尼亚大学诞生，这标志着数据开始以电子形式进行创建、处理和存储。数据不再仅限于在物理介质上表示的文字、数字等，而是转变为二进制代码在电子元件中流动和存储。电子数据出现之初，并不受重视，仅被理解为电子数据在生成、存储、传输、修改过程中产生的相关记录，供技术人员发现与分析问题使用。随着现代信息技术的发展与普及，人们慢慢注意到电子数据的存在和价值，并不断拓展应用领域，尤其在涉及计算机、网络、通信等现代信息技术的相关事件调查中，作用更为显著。因此，电子数据从没有一个统一的称谓，到被称作电子证据，最终固化为电子数据并成为特定法律术语，逐渐在司法实践、网络安全以及许多行业管理中被广泛应用。

1.1.1 电子数据

电子数据这一概念最早出现在我国的法律规定中，是在 2012 年我国刑事诉讼法第二次修正时，电子数据作为新的证据类型列入刑事诉讼证据。之后，2012 年我国民事诉讼法第二次修正、2014 年行政诉讼法第一次修正时，也分别将电子数据列入诉讼证据。

2016 年，为规范电子数据的收集提取和审查判断，提高刑事案件办理质量，最高人民法院、最高人民检察院、公安部根据《中华人民共和国刑事诉讼法》等有关法律规定，结合司法实际，制定了《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》（以下简称《规定》）。这是最高人民法院、最高人民检察院、公安部首次就电子数据制定的针对性规定。

《规定》采用“概括＋例举＋排除”的方式，对电子数据作了界定。

1. 概括规定

《规定》的第一条第一款将电子数据概括为，“电子数据是案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据。”需要注意的是，对“案件发生过程中”不应作狭义的理解，除了案件中形成的电子数据，还应当包含案件前和案件后的行为形成的电子数据，比如电信网络诈骗实施前行为人架设的钓鱼网站，实施后的诈骗资金处置等环节，都是勘查和取证的重点。

2. 例举规定

《规定》的第一条第二款对电子数据作了列举，即电子数据包括但不限于下列信息、电子文件：（一）网页、博客、微博客、朋友圈、贴吧、网盘等网络平台发布的信息；（二）手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信信息；（三）用户注册信息、身份认证信息、电子交易记录、通信记录、登录日志等信息；（四）文档、图片、音视频、数字证书、计算机程序等电子文件。

3. 排除规定

《规定》的第一条第三款对具有相似性却不作为电子数据的几种情形作了排除，即以数字化形式记载的证人证言、被害人陈述以及犯罪嫌疑人、被告人供述和辩解等证据，不属于电子数据。

1.1.2 数字勘查

传统的现场勘查主要是对物理空间的勘查，在发生事故、违法、灾害等事件后，由政府及其执法部门相关人员前往现场进行调查、勘验、测量、拍照等一系列工作，以获取事件发生的相关证据和信息。本教材中涉及的数字勘查特指对存储、处理、传输电子数据的存储介质进行搜查、提取、扣押或查封和冻结等工作。

1.1.3 数字取证

数字取证，又称电子数据取证，是指使用合法、合理、规范的技术或方法，从存储介质中提取、固定、分析和展示电子数据的过程。

数字勘查和数字取证是不同的两个概念，数字勘查侧重于电子数据及其存储介质的收集过程；数字取证则侧重于电子数据的提取与解析过程。但实践中，数字勘查与数字取证没有截然分开，毕竟勘查重要的任务之一就是获取证据。所以，在后续的章节表述中，不再强调二者的联系与区别，主要用“电子数据取证”来指代。

数字勘查与取证主要针对两类数据存储介质：一是对电子数据的永久性存储介质进行勘验检查；二是针对临时存放数据或在网络之间传输数据等非永久性存储介质进行勘

验检查。

1. 永久性存储介质

永久性存储介质是指一种数据存储设备或技术，即使在没有外部电源供应的情况下，也能保持其中储存的数据不会丢失。这些存储介质的物理特性使其能够在断电后长期保存信息，适合用于需要长期、稳定存储数据的应用场景。

常见的永久性存储介质包括：（1）硬盘驱动器（HDD）。HDD 利用磁性材料记录数据，即使电脑关机后，磁盘上的数据依然得以保留。（2）固态硬盘（SSD）。SDD 虽然基于闪存而非磁性原理，但同样具备断电后数据不丢失的特性。（3）光盘（CD、DVD、蓝光光盘等）。通过激光蚀刻在光盘上的凹坑和空白区域来编码二进制数据，除非物理损坏，否则其所存储的信息能够长期保存。（4）闪存设备（如 U 盘、SD 卡、CF 卡等）。采用闪存芯片作为存储媒介，即使断电也能够持久地存储数据。另外，ROM（Read-Only Memory）和 EEPROM（Electrically Erasable Programmable Read-Only Memory）等半导体存储器在制造时写入或在特定条件下可擦写的固件数据，在无电情况下数据也能保持稳定。

2. 非永久性存储介质

非永久性存储介质，又称易失性存储器或临时存储器，是指在断电后不能保持其存储内容的电子设备或技术。这类存储器依赖持续的电源供应来维持数据的存在状态，一旦失去电力供给，其中存储的信息将迅速消失。

常见的非永久性存储介质包括：（1）随机存取存储器（RAM）。RAM 是计算机系统中用于临时存放运行时数据的主要内存类型，如动态随机存取存储器（DRAM）和静态随机存取存储器（SRAM）。当计算机关机或遭遇意外断电时，RAM 中的所有数据都将丢失。（2）CPU 缓存（L1、L2、L3 Cache）。这些高速小容量存储区域位于 CPU 内部，用于提高数据读取速度，同样不具备断电保存数据的能力。（3）显示缓冲区（Display Buffer）和其他硬件电路内的临时寄存器。这些存储单元仅在设备工作期间保留信息。（4）CMOS RAM（Complementary Metal-Oxide-Semiconductor RAM）。尽管名为 RAM，但 CMOS RAM 通常用来存储 BIOS 设置等少量重要信息，它通过主板上的电池供电，在正常情况下也能保持数据不丢失，但如果电池耗尽，则所存储的数据也会消失。

非永久性存储介质主要用于处理和暂存正在使用或即将使用的数据，具有较高的读写速度，但无法实现长期可靠的数据存储。因此，对此类易失性电子数据，应当特别注意取证时机和取证方法。

1.2 电子数据取证技术在维护网络空间安全中的重要作用

电子数据取证技术尽管主要是为了支持侦查打击网络犯罪和解决事后追责问题，但也被作为构建网络空间安全保障体系的重要组成部分。随着取证技术逐步向智能化方向发展与应用，在预防网络安全风险、提高应急响应能力、打击网络犯罪，以及维护网络空间秩

序等方面发挥的作用更加明显。

1. 实时监控与预警

电子数据取证技术在实时监控与预警方面的应用，是现代网络安全防御体系中至关重要的环节，有效增强了对网络威胁的预见性和反应力，提高了整体的安全防护水平。一方面，智能取证技术可以自动检测异常行为。通过持续的网络流量分析、日志审计和用户行为模式识别，电子数据取证工具可以实时监测并发现潜在的非法侵入或其他异常操作。例如，自动识别出不符合常规的登录尝试、大规模的数据传输或未经授权的系统访问等。另一方面，其可以自动整合威胁情报。利用智能取证技术收集到的实时数据可与全球威胁情报数据库自动比对，快速识别已知攻击特征、恶意软件签名等信息，一旦匹配成功即可发出预警，从而降低未知威胁转化为实际损失的可能性。

2. 应急响应与恢复

在应急响应与恢复环节中，电子数据取证技术是保障网络安全的关键支撑之一，不仅有助于快速有效地应对突发网络安全事件，还有助于最大限度地减少损失，并为后续的法律程序和安全策略升级奠定基础。当发生网络攻击、数据泄露或其他安全事件时，取证工作作为需要第一时间响应的核心环节，通过电子数据取证技术快速定位受损系统、确定损失范围，同时协助恢复被破坏或篡改的数据，降低安全事故的影响程度，控制事态进一步恶化。

3. 网络犯罪案件侦查调查

电子数据取证技术在网络犯罪案件侦查中承担着线索识别、侦查导引、证据固定以及罪责认定等关键任务，从证据的发现、收集、分析到展示，覆盖网络犯罪案件侦查及诉讼的全过程，使打击网络犯罪更加有力且高效。一方面，其可以帮助侦查人员准确判断网络犯罪性质和程度，并从网络攻击事件中提取并分析 IP 地址、恶意软件样本、操作记录等电子数据，从而追踪攻击行为的源头，揭示攻击路径、攻击手段和技术细节，为攻击溯源和识别攻击者身份提供方向。另一方面，在合法授权范围内，其能够使用专业工具解锁被加密保护的设备或文件，或对已删除、隐藏、加密或损坏的数据进行恢复，提取电子邮件、文档、聊天记录、图片、音频视频文件等可能涉及犯罪活动的信息。

4. 证据保全与合法化

电子数据取证技术不仅可以帮助实现证据的有效保全，还能通过科学分析和规范化处理，提升电子数据的合法性，从而有力支持司法、管理等活动。电子数据取证首先要求对存储介质进行完整、无损的镜像复制，确保原始数据不丢失、不受破坏，这是证据保全的基础。取证过程中，应严格遵守流程及规范，确保每一步操作都可追溯和重现，建立完整的证据链。通过电子签名、可信时间戳、Hash 值校验、区块链等技术手段收集和固定证据，并实现防篡改；或者通过电子取证存证平台认证，确保电子数据的真实性、完整性和不可篡改性，从而提升电子数据的证明能力和法律效力。

5. 威慑违规违法行为

任何通过电子设备或网络系统进行的活动都有可能留下电子痕迹，这些痕迹可以作为

追责时的有力证据。电子数据中包含时间戳等元数据，使得违法行为的时间线非常清晰，另外可以通过 IP 地址追踪到行为发生的具体位置，极大提高了对违规违法者的定位能力。比如电子邮件、聊天记录、交易信息、网络浏览历史，都可以被用于证明行为的发生和责任归属。还可以利用大数据技术，开发预警模型，从海量电子数据中发现异常行为模式，及时预警潜在的违规违法行为。因此，电子数据取证技术的存在增强了网络安全监管能力，提高了违规违法行为被发现、查处的概率，从而起到威慑作用。

6. 预防未来攻击

通过对已发生的网络攻击事件进行电子数据的搜集和深入分析，可以发现攻击者的工具、技术和行为模式，从而用于预测未来的攻击趋势，并制定针对性的防御策略。另外，利用电子数据取证技术对历史安全事件的数据进行挖掘，可以帮助识别系统的薄弱环节，提前进行风险评估并发出预警，防止类似攻击再次发生。随着电子数据取证技术的不断发展，先进的取证工具和方法能更有效地追踪、定位网络攻击源头，从而推动新的防御技术的研发和部署，提高整体网络安全防护水平。

1.3 电子数据取证技术在其他领域中的应用

电子数据取证技术应用广泛，不仅用于网络安全事件调查，还用于各类诉讼、行政执法、内部管理，以及知识产权保护等领域。

1. 用于各类诉讼

由于电子数据已经成为刑事、民事和行政诉讼中法定的证据类型之一，因此，电子数据取证技术被广泛应用于这些司法领域，作为查明案件事实的重要手段。在刑事诉讼中，通过收集到的犯罪嫌疑人的电子邮件、通信信息、电子交易记录等电子数据，可能直接揭示犯罪动机、犯罪过程和犯罪结果。在民事诉讼中，通过收集到的通信信息或者图片、音视频等电子数据，可能直接还原纠纷产生过程。在行政诉讼中，通过收集到的网页、文档、计算机程序等电子数据，可能直接回溯行政主体的决策及其具体的行为。

2. 用于行政执法

电子数据取证技术有助于提高行政执法效率，使得行政案件查处工作更加精准、快捷。当公安、市场监管、税务、环保等具有行政执法权的部门，在执行法律法规和监管政策时，可利用电子数据取证技术来发现、获取、分析并验证与违法行为相关的证据。如通过电子数据取证技术，深入调查行政行为的相对人或其他利害关系人的内部管理系统、交易记录、通信记录、网络行为等，以揭示可能存在的网络违法、市场欺诈、不正当竞争、偷税漏税或环境监测数据造假等违法行为。这些部门甚至还可对收集到的数据进行挖掘和分析，找出隐藏的违法线索，形成完整的证据链，为行政处罚提供依据。

3. 用于纪检监察

电子数据取证技术为纪检监察机关提供了强有力的技术手段，不仅增强了反腐败斗争

的技术力量，也极大地提升了执纪执法工作的科学性和准确性。对于党政机关、企事业单位的内部纪检监察工作而言，电子数据取证技术能够加强对权力运行的制约和监督，预防和惩治滥用职权、玩忽职守等违纪违法行为的发生。对于党的纪律检查机关和政府的监察部门而言，利用电子数据取证技术可以帮助纪检监察人员及时发现违法违纪线索，快速锁定违法违纪人员，揭示和惩治腐败行为、利益输送等职务犯罪问题。

4. 用于审计工作

电子数据取证技术对于现代审计而言不仅是技术工具的升级，更是审计方法论与实践方式的重大变革。传统的审计方法往往依赖于纸质记录和人工检查，而电子数据取证技术能够快速、准确地从海量的电子数据中筛选出关键信息，深入挖掘隐藏的交易记录、修改痕迹以及异常操作行为，有效发现并预防财务报表造假、内部贪污、挪用公款等经济犯罪活动。同时，还能利用电子数据取证技术审查其内部控制的有效性，发现潜在的风险点，并对被审计单位的合规情况进行全面评估。

5. 用于内部管理

单位在对内部的管理中，一方面可以利用电子数据取证技术确保数据的完整性和合法性，为可能出现的法律争议提供证据支持和保障。另一方面可对单位内因职务行为形成的电子记录进行审查，确保本单位员工行为符合法律法规、相关政策、行业规定以及单位内部的管理制度。当单位内部出现员工违规违法行为、知识产权侵权、劳动合同纠纷等情况时，其可以协助人力资源部门、法务部门或审计团队快速准确地定位和收集相关电子证据，以便公正、透明地进行内部调查和处理。还可以利用电子数据取证技术进行日常的数据安全监控，及早发现潜在的网络攻击、数据泄露等风险，提升单位信息安全管理水平。

6. 用于知识产权保护

电子数据取证技术对于知识产权保护也至关重要，它增强了对数字化环境下侵权行为的检测、防范和应对能力。在数字化和网络化日益普及的今天，侵权行为往往通过网络进行，针对软件代码、设计图纸、音视频文件等复杂的数字内容，可以利用电子数据取证技术深入分析其中的元数据、水印等信息，精准比对是否存在抄袭、剽窃行为，确定侵权作品的源头、传播路径以及涉及的相关责任人，并通过记录侵权产品的销售数据来估算损害赔偿金额，为权利人提供有力的追责依据。

未来，电子数据无处不在，电子数据取证技术也必将在更广泛的领域发挥更大的作用。

1.4 电子数据取证技术的发展趋势

电子数据取证技术的发展，必然要顺应信息技术的新发展和取证环境的新变化。随着电子数据的数量呈指数级增长，以及电子数据载体不断向智能化方向迭代更新，未来的电子数据取证技术将更加注重对海量电子数据处理与分析的智能化、标准化、规范化以及跨

平台性。同时，也会更加注重隐私保护和安全性等问题。

1. 自动化和智能化

人工智能技术运用到电子数据取证领域，可以对电子数据进行更准确、全面和深入的分析与解读。比如，利用图像识别技术自动识别各类文件类型，并通过内容分析对其进行智能分类；使用 NLP 技术解析非结构化的文本数据，提取有意义的信息和语义关联，有助于发现线索，揭示事实；应用大数据技术处理海量的电子数据，快速搜索、筛选、发现关键证据，并通过关联分析挖掘潜在的关系网络和行为模式；运用机器学习算法来识别恶意软件、检测异常行为、确定数据的真实性和完整性，以及提高密码破解和数据恢复的成功率。

另外，随着时间和案例经验的增长，通过智能取证与分析，能够不断优化其分析策略，从而为调查人员提供自动化决策支持。

2. 云计算与大数据处理

随着云计算和大数据处理技术的发展，未来必然也会在更高效、更智能、更合规等方面持续赋能电子数据取证。但同时，这也会给取证工作带来难题。一方面，大数据技术将促使数据量呈爆发式增长，取证所面临的电子数据规模远超以往。另一方面，云计算环境下的数据往往是动态变化的，取证工作需要在数据产生的瞬间或尽可能短的时间内完成，以防数据被修改或删除，这就要求取证技术具有更高的实时性和敏捷性，能够及时捕捉并固化证据。此外，云计算使得数据分散存储在多个地理位置的服务器集群中，这就要求电子数据取证技术还需要适应数据冗余备份、虚拟化存储、分布式数据结构等云存储的特点。因此，电子数据取证需要借助云计算、大数据、人工智能等技术，才有可能有效解决这些问题。

3. 区块链取证

面对区块链技术的快速发展，未来电子数据取证技术将面临取证方式的革新，特别是针对区块链上发生的交易、数据流转等行为，取证将更加侧重于对区块链网络和智能合约的审计和追踪。同时，利用区块链的不可篡改性和时间戳功能，可以实现证据的实时固化和保全。一旦数据写入区块链，就形成了一个无法更改且带有时间标记的证据链，大大简化了证据收集和验证的过程。因此，未来会出现更多基于区块链技术的自动化取证工具和平台，这些工具能够自动抓取、分析和验证链上数据，提高取证效率，并降低人为操作错误的可能性。

随着司法体系对区块链技术认知的加深和相关法律法规的完善，基于区块链的取证结果比过去更容易获得司法认可。

4. 移动终端和物联网取证

物联网环境下的数据分布在众多终端设备、边缘计算节点以及云端服务器中，这就需要未来的电子数据取证技术能够适应这种分布式数据架构，具有远程取证和分布式取证能力。同时，由于物联网技术的实时特性使得证据可能瞬息即逝，实时取证和早期预警系统

将成为重要的发展方向。通过实时监测网络流量、设备行为等数据，及时发现潜在的违法犯罪行为或安全事件。

对于物联网的取证还需严格遵循日益严格的隐私保护法规，这就要求研发出既能够保障取证效率又要尊重用户隐私权的新技术进行安全取证。并通过建立覆盖物联网全生命周期的取证体系，从设备制造、部署、运行到废弃阶段，全程考虑证据采集、分析和管理的各个环节，形成全方位、立体化的取证策略。

5. 跨平台和多介质兼容

面对不断迭代的硬件和软件，需要及时研发和升级数据取证工具和技术，提升跨平台和兼容各类存储介质的能力。不仅需要支持 Windows、Linux、macOS、Android、iOS 等多种操作系统的取证，还要支持计算机、手机、平板、物联网终端设备等不同设备及其固态硬盘、闪存、内存、移动设备内置存储、云端存储、嵌入式设备存储、其他新型存储等不同存储介质的取证。

6. 加密数据破解与密码学对抗

随着加密技术的不断进步和广泛应用，大量的电子数据尤其是敏感信息被加密存储和传输，这给电子数据取证带来了挑战。加密技术使得存储在设备或网络传输中的数据以密文形式存在，传统取证技术很难直接获取和解析数据内容。如果没有正确的密钥，即使是合法的取证行动也无法解读加密信息。

针对加密数据的取证技术也将持续进步，包括研究先进解密技术、反制恶意加密手段以及加密环境下证据的有效获取和解读。未来取证技术需要有能力破解或绕过不同平台和设备的加密机制，合法地获取和解析加密数据。然而，密码学对抗使得电子数据取证工作面临道德和法律困境，毕竟破解或绕过不同平台和设备的加密机制，可能会同时涉及公民隐私权、网络安全和国家利益，如何确定相互间利益的平衡原则，在做与不做之间进行选择，同样是未来需要面对的问题。

7. 隐私保护和合规性

在收集、存储、传输和处理电子数据的过程中，需要保护个人隐私和商业秘密，防止数据泄露和滥用。因此，未来的电子数据取证技术将更加注重数据加密、隐私保护、访问控制等安全技术的应用，确保电子数据的安全性和隐私性。

随着法律法规对电子数据证据的要求日益严格，电子数据取证将更加注重符合国际和国内法律法规要求的标准流程，保证所获取证据的合法性和法庭可采纳性。

习　题

1. 简述电子数据的由来与演变。
2. 如何理解电子数据的法律含义？

3. 如何理解数字勘查与取证的含义？
4. 如何理解电子数据取证技术在维护网络空间安全中的重要地位？
5. 电子数据取证技术在网络实时监控与预警中具体作用有哪些？
6. 简述电子数据取证技术在网络犯罪案件调查中的作用。
7. 如何理解电子数据取证技术的威慑作用？
8. 电子数据取证技术能够预防未来攻击的原理是什么？
9. 简述面对区块链技术的取证发展方向。
10. 简述为何要重视电子数据取证技术的标准建设。