

GZB

国家职业技能标准

职业编码：4-04-05-08

电子数据取证分析师

(2022 年版)

中华人民共和国人力资源和社会保障部
中华人民共和国公安部 制定

中国劳动社会保障出版社出版发行

(北京市惠新东街1号 邮政编码: 100029)

*

厂印刷装订 新华书店经销

880毫米×1230毫米 32开本 印张 千字
2022年 月第1版 2022年 月第1次印刷

统一书号: 155167·

定价: .00元

读者服务部电话: (010) 64929211/84209101/64921644

营销中心电话: (010) 64962347

出版社网址: <http://www.class.com.cn>

版权专有 侵权必究

如有印装差错, 请与本社联系调换: (010) 81211666

我社将与版权执法机关配合, 大力打击盗印、销售和使用盗版图书活动, 敬请广大读者协助举报, 经查实将给予举报者奖励。

举报电话: (010) 64954652

说 明

为规范从业者的从业行为，引导职业教育培训的方向，为职业技能鉴定提供依据，依据《中华人民共和国劳动法》，适应经济社会发展和科技进步的客观需要，立足培育工匠精神和精益求精的敬业风气，人力资源社会保障部联合公安部组织有关专家，制定了《电子数据取证分析师国家职业技能标准（2022年版）》（以下简称《标准》）。

一、本《标准》以《人力资源社会保障部办公厅 市场监管总局办公厅 统计局办公室 关于发布集成电路工程技术人员等职业信息的通知（人社厅发〔2021〕17号）》为依据，严格按照《国家职业技能标准编制技术规程（2018年版）》有关要求，以“职业活动为导向、职业技能为核心”为指导思想，对电子数据取证分析从业人员的职业活动内容进行规范细致描述，对各等级从业者的技能水平和理论知识水平进行了明确规定。

二、本《标准》依据有关规定将本职业分为四级/中级工、三级/高级工、二级/技师、一级/高级技师四个等级，包括职业概况、基本要求、工作要求和权重表四个方面的内容。

三、本《标准》主要起草单位有：公安部网络安全保卫局、公安部第三研究所、上海市公安局、中国人民公安大学、上海公安学院、广东度才子集团有限公司、上海海盾安全技术培训中心、厦门市美亚柏科信息股份有限公司、广东安证计算机司法鉴定所。主要起草人有：翟晓飞、樊亦胜、张鹤、张厚宝、王艺筱、何晓霞、李蓓、高峰、崔孝晨、蔡文明、林远进、皮浩、江鑫。

四、本《标准》主要审定单位有：公安部网络安全保卫局、公安部第三研究所、上海市公安局、重庆市公安局、中国人民公安大学、最高人民检察院检察技术信息研究中心、司法鉴定科学研究院、上海交通大学网络空间安全学院、同济大学电子与信息工程学院、成都东软学院继续教育学院、广西职业技术学院、上海政法学院警

职业编码：4-04-05-08

务学院。主要审定人员有：赵代江、赵宪伟、郭弘、杨涛、刘毅、田庆宜、李欣、薛质、谭成翔、周政杰、于春鹏、蔡一军、俞雪丽、黎斌、赵志岩、李波。

五、本《标准》在制定过程中，得到了人力资源社会保障部职业技能鉴定中心、上海市职业技能鉴定中心等单位，以及葛恒双、张灵芝、孙兴旺、夏莹、余欢荣等专家的指导与大力支持，在此一并感谢。

六、本《标准》业经人力资源社会保障部、公安部批准，自公布之日^①起施行。

^① 2022年7月18日，本《标准》以《人力资源社会保障部办公厅 公安部办公厅关于颁布电子数据取证分析师国家职业技能标准的通知》（人社厅发〔2022〕36号）公布。

电子数据取证分析师 国家职业技能标准 (2022年版)

1. 职业概况

1.1 职业名称

电子数据取证分析师

1.2 职业编码

4-04-05-08

1.3 职业定义

从事电子数据提取、固定、恢复、分析等工作的人员。

1.4 职业技能等级

本职业共设四个等级，分别为：四级/中级工、三级/高级工、二级/技师、一级/高级技师。

1.5 职业环境条件

室内、外，常温。

1.6 职业能力特征

具有较好的学习、观察、分析、推理和判断、表达、计算、色觉、视觉和行为能力，动作协调，心理健康。

1.7 普通受教育程度

高中毕业（或同等学力）。

1.8 培训参考学时

四级/中级工不少于 80 标准学时；三级/高级工、二级/技师不少于 120 标准学时；一级/高级技师不少于 80 标准学时。

1.9 职业技能鉴定要求

1.9.1 申报条件

具备以下条件之一者，可申报四级/中级工：

(1) 取得相关职业^①五级/初级工职业资格证书（技能等级证书）后，累计从事本职业或相关职业工作 3 年（含）以上。

(2) 累计从事本职业或相关职业工作 5 年（含）以上。

(3) 取得技工学校本专业或相关专业^②毕业证书（含尚未取得毕业证书的在校应届毕业生）；或取得经评估论证、以中级技能为培养目标的中等及以上职业学校本专业或相关专业毕业证书（含尚未

① 相关职业：网络与信息安全管理员、信息安全测试员、密码技术应用员、通信工程技术人员、计算机硬件工程技术人员、计算机软件工程技术人员、计算机网络工程技术人员、信息系统分析工程技术人员、信息系统运行维护工程技术人员、信息管理工程技术人员、物联网工程技术人员、工业互联网工程技术人员、数据分析处理工程技术人员、信息通信网络运行管理员、信息通信信息化系统管理员、计算机程序设计员、计算机软件测试员等，下同。

② 本专业或相关专业：司法鉴定（物证技术）电子数据鉴定、公安技术网络安全执法、刑事技术（公安技术）电子物证检验、信息安全、网络空间安全、网络信息安全、网络与信息安全、信息安全与管理、网络安全与执法、保密技术、大数据技术与应用、电子技术应用、电子商务技术、电子与计算机工程、电子与信息技术、工业互联网技术应用、计算机程序设计、计算机科学与技术、计算机网络技术、计算机网络应用、网络工程、计算机系统与维护、计算机信息管理、计算机应用技术、计算机应用与维修、计算机与数码产品维修、空间信息与数字技术、区块链工程、人工智能技术服务、人工智能技术应用、软件工程、软件技术、软件与信息服务、数据科学与大数据技术、数字媒体技术、数字媒体技术应用、通信技术、通信网络应用、通信系统工程安装与维护、通信运营服务、网络安全防务系统安装与维护、网站建设与管理、物联网工程、物联网技术应用、物联网应用技术、新媒体技术、虚拟现实技术、虚拟现实技术应用、虚拟现实应用技术、移动应用技术与服务、移动应用开发、云计算技术应用、云计算技术与应用、智能科学与技术等，下同。

取得毕业证书的在校应届毕业生)。

具备以下条件之一者，可申报三级/高级工：

(1) 取得本职业或相关职业四级/中级工职业资格证书（技能等级证书）后，累计从事本职业或相关职业工作4年（含）以上。

(2) 取得本职业或相关职业四级/中级工职业资格证书（技能等级证书）后，并具有高级技工学校、技师学院毕业证书（含尚未取得毕业证书的在校应届毕业生）；或取得本职业或相关职业四级/中级工职业资格证书（技能等级证书），并具有经评估论证、以高级技能为培养目标的高等职业学校本专业或相关专业毕业证书（含尚未取得毕业证书的在校应届毕业生）。

(3) 具有大专及以上学历本专业或相关专业毕业证书，并取得本职业或相关职业四级/中级工职业资格证书（技能等级证书）后，累计从事本职业或相关职业工作2年（含）以上。

具备以下条件之一者，可申报二级/技师：

(1) 取得本职业或相关职业三级/高级工职业资格证书（技能等级证书）后，累计从事本职业或相关职业工作4年（含）以上。

(2) 取得本职业或相关职业三级/高级工职业资格证书（技能等级证书）的高级技工学校、技师学院毕业生，累计从事本职业或相关职业工作3年（含）以上；或取得本职业或相关职业预备技师证书的技师学院毕业生，累计从事本职业或相关职业工作2年（含）以上。

具备以下条件者，可申报一级/高级技师：

取得本职业或相关职业二级/技师职业资格证书（技能等级证书）后，累计从事本职业或相关职业工作4年（含）以上。

1.9.2 鉴定方式

分为理论知识考试、技能考核以及综合评审。理论知识考试以笔试、机考等方式为主，主要考核从业人员从事本职业应掌握的基本要求和相关知识要求；技能考核主要采用现场操作、模拟操作等方式进行，主要考核从业人员从事本职业应具备的技能水平；综合

评审主要针对技师和高级技师，通常采取审阅申报材料、答辩等方式进行全面评议和审查。

理论知识考试、技能考核和综合评审均实行百分制，成绩皆达60分（含）以上者为合格。

1.9.3 监考人员、考评人员与考生配比

理论知识考试中的监考人员与考生配比为1:15，且每个考场不少于2名监考人员；技能考核中的考评人员与考生配比不低于1:5，且考评人员为3人（含）以上单数；综合评审委员为3人（含）以上单数。

1.9.4 鉴定时间

理论知识考试时间不少于90 min，技能考核时间不少于120 min，综合评审时间不少于20 min。

1.9.5 鉴定场所设备

理论知识考试在标准教室或机房进行；技能考核在具有必备的电子数据取证分析设备、软硬件设施的场所进行；综合评审可在配有教学设备的标准教室或实训场所进行。

2. 基本要求

2.1 职业道德

2.1.1 职业道德基本知识

2.1.2 职业守则

- (1) 遵纪守法，爱岗敬业。
- (2) 爱护设备，安全操作。
- (3) 诚实守信，保守秘密。
- (4) 勇于创新，精益求精。
- (5) 管控流程，保障隐私。
- (6) 履行义务，保护数据。

2.2 基础知识

2.2.1 基础理论知识

- (1) 计算机硬件基础知识。
- (2) 计算机软件基础知识。
- (3) 操作系统基础知识。
- (4) 数据库基础知识。
- (5) 计算机网络基础知识。

2.2.2 相关法律法规、管理规定、标准知识

- (1) 《中华人民共和国刑法》相关知识。
- (2) 《中华人民共和国治安管理处罚法》相关知识。
- (3) 《中华人民共和国劳动法》相关知识。
- (4) 《中华人民共和国民法典》相关知识。
- (5) 《中华人民共和国网络安全法》相关知识。
- (6) 《中华人民共和国密码法》相关知识。

职业编码：4-04-05-08

- (7) 《中华人民共和国数据安全法》相关知识。
- (8) 《中华人民共和国个人信息保护法》相关知识
- (9) 电子数据取证分析相关管理规定、标准相关知识。

3. 工作要求

本标准对四级/中级工、三级/高级工、二级/技师、一级/高级技师的技能要求和相关知识要求依次递进，高级别涵盖低级别的要求。

3.1 四级/中级工

职业功能	工作内容	技能要求	相关知识要求
1. 电子数据提取与固定	1.1 电子数据保全	1.1.1 能使用录像录屏设备对电子数据取证行为进行记录 1.1.2 能使用工具对电子数据进行保全 1.1.3 能使用工具对电子数据存在环境进行保全	1.1.1 电子数据保全相关工作流程 1.1.2 电子数据保全操作方法 1.1.3 电子数据校验方法
	1.2 计算机数据提取与固定	1.2.1 能使用工具对目标存储介质数据进行镜像文件制作 1.2.2 能使用工具将目标存储介质数据复制到其他存储介质上 1.2.3 能使用工具对计算机虚拟机进行镜像制作 1.2.4 能对计算机虚拟机特定数据进行提取与固定	1.2.1 存储介质数据镜像制作方法 1.2.2 存储介质数据复制方法 1.2.3 计算机虚拟机镜像制作方法 1.2.4 计算机虚拟机特定数据提取与固定方法

续表

职业功能	工作内容	技能要求	相关知识要求
1. 电子数据提取与固定	1.3 移动终端数据提取与固定	<p>1.3.1 能使用系统备份工具对安卓终端中的数据进行提取与固定</p> <p>1.3.2 能使用系统备份工具对 iOS 终端中的数据进行提取与固定</p> <p>1.3.3 能使用系统备份工具对鸿蒙终端中的数据进行提取与固定</p>	<p>1.3.1 安卓终端备份方法</p> <p>1.3.2 iOS 终端备份方法</p> <p>1.3.3 鸿蒙终端备份方法</p>
	1.4 工控设备数据提取与固定	<p>1.4.1 能使用工具提取常见工控设备系统日志</p> <p>1.4.2 能使用工具将常见目标工控设备数据复制到存储介质上</p>	<p>1.4.1 常见工控设备系统日志获取方法</p> <p>1.4.2 常见工控设备数据复制方法</p>
2. 电子数据恢复	2.1 文件恢复	<p>2.1.1 能使用工具基于文件系统进行文件恢复</p> <p>2.1.2 能使用工具基于文件特征进行文件恢复</p>	<p>2.1.1 基于文件系统进行文件恢复的方法</p> <p>2.1.2 基于文件特征进行文件恢复的方法</p>
	2.2 数据恢复	<p>2.2.1 能使用工具基于系统架构进行数据恢复</p> <p>2.2.2 能使用工具基于文件结构进行数据恢复</p>	<p>2.2.1 基于系统架构进行数据恢复的方法</p> <p>2.2.2 基于文件结构进行数据恢复的方法</p>

续表

职业功能	工作内容	技能要求	相关知识要求
3. 电子数据分析	3.1 计算机取证分析	3.1.1 能使用工具对计算机系统在线进行分析 3.1.2 能使用工具对磁盘、U盘、光盘等存储介质数据进行分析 3.1.3 能使用工具对磁盘、U盘、光盘等存储介质镜像数据进行分析 3.1.4 能使用工具对计算机备份数据进行分析	3.1.1 计算机系统在线数据分析方法 3.1.2 存储介质数据分析方法 3.1.3 存储介质镜像数据分析方法 3.1.4 计算机备份数据分析方法
	3.2 移动终端取证分析	3.2.1 能使用工具对移动终端备份进行数据分析 3.2.2 能使用工具对移动终端镜像进行数据分析 3.2.3 能使用工具对移动终端进行数据分析	3.2.1 移动终端备份解析工具使用方法 3.2.2 移动终端镜像解析工具使用方法 3.2.3 移动终端镜像中特定文件查看与导出方法 3.2.4 移动终端备份中特定文件查看与导出方法
	3.3 电子数据取证分析报告编写	3.3.1 能使用工具生成电子数据取证报告 3.3.2 能根据国家相关规定编写电子数据取证分析报告	3.3.1 电子数据取证报告生成方法 3.3.2 电子数据取证分析报告编写方法与要求

3.2 三级/高级工

职业功能	工作内容	技能要求	相关知识要求
1. 电子数据提取与固定	1.1 计算机数据提取与固定	1.1.1 能使用工具对计算机操作系统进行备份 1.1.2 能提取常见计算机操作系统日志 1.1.3 能提取常见数据库日志 1.1.4 能提取常见服务的应用日志 1.1.5 能使用工具对远程计算机进行镜像	1.1.1 计算机操作系统备份方法 1.1.2 计算机操作系统日志提取方法 1.1.3 常见数据库日志提取方法 1.1.4 常见服务应用日志提取方法 1.1.5 远程计算机镜像方法
	1.2 移动终端数据提取与固定	1.2.1 能使用第三方备份工具对安卓终端中的数据进行提取与固定 1.2.2 能使用第三方备份工具对 iOS 终端中的数据进行提取与固定 1.2.3 能使用工具对移动终端模拟器中的数据进行提取与固定 1.2.4 能使用工具对非主流系统终端中的数据进行提取与固定	1.2.1 第三方备份工具使用方法 1.2.2 移动终端模拟器数据提取与固定方法 1.2.3 非主流系统终端数据提取与固定方法

续表

职业功能	工作内容	技能要求	相关知识要求
1. 电子数据提取与固定	1.3 工控设备数据提取与固定	<p>1.3.1 能对工控设备中存储的流量日志进行提取与固定</p> <p>1.3.2 能获取常见工控设备系统应用数据</p>	<p>1.3.1 工控设备流量日志提取与固定方法</p> <p>1.3.2 工控设备系统应用数据获取方法</p>
	1.4 智能芯片数据提取与固定卡取证	<p>1.4.1 能使用工具对常见的移动终端芯片进行数据提取与固定</p> <p>1.4.2 能使用工具对常见的物联网芯片进行数据提取与固定</p> <p>1.4.3 能使用工具对常见的存储卡芯片进行数据提取与固定</p>	<p>1.4.1 常见移动终端芯片数据提取与固定方法</p> <p>1.4.2 常见物联网芯片数据提取与固定方法</p> <p>1.4.3 常见存储卡芯片数据提取与固定方法</p>
2. 电子数据恢复	2.1 文件恢复	<p>2.1.1 能判断文件的存在性</p> <p>2.1.2 能对自定义文件系统进行文件恢复</p>	<p>2.1.1 文件存在性判断方法</p> <p>2.1.2 自定义文件系统文件恢复方法</p>
	2.2 数据恢复	<p>2.2.1 能判断数据的存在性</p> <p>2.2.2 能对无文件系统的数据存储进行数据恢复</p>	<p>2.2.1 数据存在性判断方法</p> <p>2.2.2 无文件系统数据存储的数据恢复方法</p>

续表

职业功能	工作内容	技能要求	相关知识要求
3. 电子数据分析	3.1 计算机取证分析	<p>3.1.1 能对计算机中的非主程序数据进行定位与分析</p> <p>3.1.2 能对计算机中的关键数据进行定位与分析</p>	<p>3.1.1 计算机中非主程序数据定位与分析方法</p> <p>3.1.2 计算机中关键数据的定位与分析方法</p>
	3.2 移动终端取证分析	<p>3.2.1 能对移动终端中的非主程序数据进行定位与分析</p> <p>3.2.2 能对移动终端中的关键数据进行定位与分析</p>	<p>3.2.1 移动终端中非主程序数据定位与分析方法</p> <p>3.2.2 移动终端中关键数据定位与分析方法</p>
	3.3 分析程序编写	<p>3.3.1 能使用 Python/Java/C/C++/C#等一种或多种编程语言开发程序对提取与固定的数据进行分析</p> <p>3.3.2 能使用常用的第三方分析库对提取与固定的数据进行分析</p>	<p>3.3.1 分析程序的编写方法</p> <p>3.3.2 常用第三方分析库的使用方法</p>
	3.4 数据统计及挖掘	<p>3.4.1 能对数据进行清洗与预处理</p> <p>3.4.2 能根据数据获取人员自然属性</p> <p>3.4.3 能根据数据获取人员关系基本模式</p> <p>3.4.4 能根据数据分析数据规律与统计信息</p>	<p>3.4.1 数据清洗与预处理方法</p> <p>3.4.2 表数据整理与信息获取方法</p> <p>3.4.3 数据规律与统计信息分析方法</p>

3.3 二级/技师

职业功能	工作内容	技能要求	相关知识要求
1. 电子数据提取与固定	1.1 计算机数据提取与固定	1.1.1 能使用工具对计算机网络流量进行固定 1.1.2 能使用工具对计算机内存数据进行镜像制作 1.1.3 能对容器内特定数据进行提取与固定 1.1.4 能使用工具对容器进行镜像制作	1.1.1 网络流量抓包方法 1.1.2 计算机内存数据提取与固定方法 1.1.3 容器内特定数据提取与固定方法 1.1.4 容器镜像制作方法
	1.2 移动终端数据提取与固定	1.2.1 能获取安卓智能终端物理镜像 1.2.2 能使用工具对安卓终端数据进行提取与固定 1.2.3 能使用工具对 iOS 智能终端数据进行提取与固定 1.2.4 能对移动终端网络流量进行提取与固定	1.2.1 安卓智能终端物理镜像获取方法 1.2.2 安卓终端数据提取与固定方法 1.2.3 iOS 智能终端数据提取与固定方法 1.2.4 移动终端网络流量提取与固定方法
	1.3 物联网设备数据提取与固定	1.3.1 能对智能家居设备数据进行提取与固定 1.3.2 能对智能穿戴设备数据进行提取与固定	1.3.1 智能家居设备数据提取与固定方法 1.3.2 智能穿戴设备数据提取与固定方法
	1.4 工控设备数据提取与固定	1.4.1 能使用工具对常见目标工控设备进行镜像制作 1.4.2 能对工控设备网络流量进行提取与固定	1.4.1 常见工控设备镜像制作方法 1.4.2 工控设备网络流量提取与固定方法

续表

职业功能	工作内容	技能要求	相关知识要求
1. 电子数据提取与固定	1.5 网络安全防护设备数据提取与固定	1.5.1 能对入侵检测、防御系统数据进行提取与固定 1.5.2 能对蜜罐、沙箱系统数据进行提取与固定 1.5.3 能对其他常见网络安全防护设备日志进行提取与固定 1.5.4 能对常见网络安全防护设备网络流量数据进行提取与固定	1.5.1 入侵检测、防御系统数据提取与固定方法 1.5.2 蜜罐、沙箱系统数据提取与固定方法 1.5.3 常见网络安全防护设备日志提取与固定方法 1.5.4 常见网络安全防护设备网络流量数据提取与固定方法
2. 电子数据恢复	2.1 物理恢复	2.1.1 能对硬盘进行开盘修复 2.1.2 能对存储芯片焊接并对数据进行提取 2.1.3 能对移动设备的 JTAG 接口数据进行提取	2.1.1 硬盘开盘修复方法 2.1.2 存储芯片焊接和数据提取方法 2.1.3 移动设备 JTAG 接口数据提取方法
	2.2 集群恢复	2.2.1 能对磁盘阵列进行重组恢复 2.2.2 能对集群进行恢复	2.2.1 磁盘阵列重组方法 2.2.2 集群恢复方法
3. 电子数据分析	3.1 解密分析	3.1.1 能对加密文件进行识别和查找 3.1.2 能使用工具对加密文件进行解密 3.1.3 能解密加密磁盘、容器和系统 3.1.4 能使用工具对文件中包含的隐藏信息进行分析	3.1.1 常用加解密算法 3.1.2 加密特征和识别方法 3.1.3 密码解密相关工具

续表

职业功能	工作内容	技能要求	相关知识要求
3. 电子数据分析	3.2 构建电子数据分析模型	3.2.1 能对人物关系建立模型并进行分析 3.2.2 能对资金数据建立模型并进行分析 3.2.3 能对地理位置信息建立数据模型并进行分析	3.2.1 人物关系模型建立与分析方法 3.2.2 资金数据模型建立与分析方法 3.2.3 地理位置信息数据模型建立与分析方法
	3.3 逆向工程分析	3.3.1 能使用常见工具对程序进行简单静态分析 3.3.2 能使用常见工具对程序进行简单动态分析 3.3.3 能使用模拟程序获取程序运行信息	3.3.1 程序简单静态分析方法 3.3.2 程序简单动态分析方法 3.3.3 程序运行信息获取方法
	3.4 云服务功能分析	3.4.1 能使用工具启动、还原云服务及数据库 3.4.2 能还原云服务的虚拟网络拓扑 3.4.3 能分析数据库的连接地址与口令 3.4.4 能对服务器上的网站代码定位并分析其功能 3.4.5 能对数据库的关键表进行定位与分析	3.4.1 网站源码获取与分析方法 3.4.2 云服务网络拓扑知识 3.4.3 数据库连接信息分析方法 3.4.4 网站代码定位与功能分析方法 3.4.5 数据库关键表的定位与分析方法

续表

职业功能	工作内容	技能要求	相关知识要求
3. 电子数据分析	3.5 区块链数据分析	3.5.1 能对虚拟货币数据进行分析 3.5.2 能对虚拟货币资金交易记录进行分析 3.5.3 能对智能合约进行分析	3.5.1 虚拟货币数据分析方法 3.5.2 虚拟货币资金交易记录分析方法 3.5.3 智能合约分析方法
4. 培训与指导	4.1 培训实施	4.1.1 能制订培训工作计划 4.1.2 能编制和实施培训方案 4.1.3 能编写培训教材、讲义、课件 4.1.4 能进行培训宣讲	4.1.1 培训工作计划制订要求与方法 4.1.2 培训方案编制和实施方法 4.1.3 培训教材、讲义、课件编写方法 4.1.4 培训宣讲方法
	4.2 技术指导	4.2.1 能对三级/高级工及以下级别人员进行技能指导 4.2.2 能对三级/高级工及以下级别人员技能水平进行考核	4.2.1 操作经验和技能总结方法 4.2.2 技能和理论知识水平考核要求和方法 4.2.3 技能和理论知识水平考核内容制定方法

3.4 一级/高级技师

职业功能	工作内容	技能要求	相关知识要求
1. 电子数据提取与固定	1.1 数据固定	<p>1.1.1 能提出对前沿设备数据进行数据提取的方法</p> <p>1.1.2 能提出对存在系统限制的非主流设备进行数据采集的方法</p> <p>1.1.3 能提出汽车数据提取与固定的方法</p>	<p>1.1.1 前沿设备数据提取研究方法</p> <p>1.1.2 电子设备系统框架核心分析方法</p> <p>1.1.3 汽车数据提取与固定方法</p>
	1.2 数据解密	<p>1.2.1 能提出应用工具对主流应用数据进行解密的方法</p> <p>1.2.2 能提出应用工具对主流容器进行解密的方法</p> <p>1.2.3 能提出应用工具对前沿应用数据进行解密的方法</p>	<p>1.2.1 数据加密解密方法</p> <p>1.2.2 容器加密解密方法</p> <p>1.2.3 前沿应用数据解密方法</p>
2. 电子数据恢复	2.1 数据恢复	<p>2.1.1 能提出对前沿数据库系统进行数据恢复的实施方案</p> <p>2.1.2 能提出损坏文件数据修复的实施方案</p> <p>2.1.3 能提出通过备份、日志以及其他数据对数据库进行恢复的实施方案</p>	<p>2.1.1 数据库应用系统的设计方法</p> <p>2.1.2 主流文件的存储结构与恢复方法</p> <p>2.1.3 主流数据库系统数据存储原理与恢复方法</p>

续表

职业功能	工作内容	技能要求	相关知识要求
2. 电子数据恢复	2.2 文件恢复	<p>2.2.1 能提出对前沿设备文件系统文件删除恢复的实施方案</p> <p>2.2.2 能提出对主流文件系统进行文件恢复的实施方案</p>	<p>2.2.1 主流文件系统数据存储原理与恢复方法</p> <p>2.2.2 主流文件数据结构与恢复方法</p> <p>2.2.3 前沿文件系统数据结构与恢复方法</p>
	2.3 系统恢复	<p>2.3.1 能提出对损坏系统进行恢复的方法</p> <p>2.3.2 能提出对大数据系统进行重组的方法</p>	<p>2.3.1 损坏系统恢复方法</p> <p>2.3.2 大数据系统重组方法</p>
3. 电子数据分析	3.1 电子数据分析模型构建	<p>3.1.1 能使用数据模型完成数据的关系、空间、时间等多维度分析</p> <p>3.1.2 能对数据进行关联碰撞分析</p> <p>3.1.3 能提出数据挖掘分析实施方法</p>	<p>3.1.1 数据挖掘与分析方法</p> <p>3.1.2 数据库应用系统设计方法</p> <p>3.1.3 数据分析模型建设方法</p>
	3.2 程序功能分析	<p>3.2.1 能提出分析程序主要功能的实施方案</p> <p>3.2.2 能提出监控程序行为的实施方案</p> <p>3.2.3 能提出对行为流量分析的实施方案</p>	<p>3.2.1 程序逆向分析方法</p> <p>3.2.2 程序监控分析方法</p> <p>3.2.3 行为流量分析方法</p>

续表

职业功能	工作内容	技能要求	相关知识要求
3. 电子数据分析	3.3 人工智能分析	3.3.1 能对基于人工智能的应用进行分析 3.3.2 能对基于人工智能伪造的数据进行分析	3.3.1 人工智能应用分析方法 3.3.2 人工智能伪造数据分析方法
4. 培训与指导	4.1 培训实施	4.1.1 能对培训需求进行分析 4.1.2 能编制培训规划 4.1.3 能对培训预算和决算进行审核	4.1.1 培训需求分析要求和方法 4.1.2 培训规划编制要求 4.1.3 培训预算与决算的审核方法
	4.2 技术指导	4.2.1 能对二级/技师及以下级别人员进行技能操作指导 4.2.2 能对二级/技师及以下级别人员进行技能水平考核 4.2.3 能组织开展技术改造、技术革新活动	4.2.1 技能操作指导方法 4.2.2 技能考核方法 4.2.3 技术改造与革新方法

职业编码：4-04-05-08

4. 权重表

4.1 理论知识权重表

项目		技能等级	四级/ 中级工 (%)	三级/ 高级工 (%)	二级/ 技师 (%)	一级/ 高级技师 (%)
基本要求	职业道德		5	5	5	5
	基础知识		15	10	5	5
相关知识要求	电子数据提取与固定		30	30	20	20
	电子数据恢复		30	30	20	20
	电子数据分析		20	25	40	40
	培训与指导		—	—	10	10
合计			100	100	100	100

4.2 技能要求权重表

项目		技能等级	四级/ 中级工 (%)	三级/ 高级工 (%)	二级/ 技师 (%)	一级/ 高级技师 (%)
技能 要求	电子数据提取与固定		40	30	20	20
	电子数据恢复		40	30	20	20
	电子数据分析		20	40	50	50
	培训与指导		—	—	10	10
合计			100	100	100	100