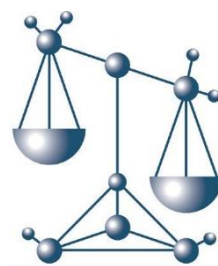


法庭科学电子物证检验的 基本要求

用于新建实验室的文件

国际法庭科学战略联盟（IFSA）

第1版

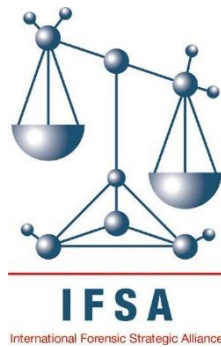


IFSA

International Forensic Strategic Alliance

国际法庭科学战略联盟

法庭科学电子物证检验的基本要求
用于新建实验室的文件
IFSA 基本要求文件 4



该中文版文件由原英文版翻译而来，方便使用中文的法庭科学实验室知悉文件内容。请注意，这并非官方翻译。

©2023年11月



目录

引言	4
前言	5
1 工作人员能力要求	6
2 仪器和耗材	8
3 采集、分析、解释和结果报告	10
4 程序、操作指南和确认	15
5 质量管理	17
6 术语表	18

引言

本文件由国际法庭科学战略联盟(International Forensic Strategic Alliance, IFSA)制订，文件中涉及的基本要求将有助于发展中国家的新建法庭科学机构为刑事司法系统提供科学服务。

本文件旨在规定一个为获得可靠结果所必需遵循的基础或起点。法庭科学机构应该建立在此基础上，并不断提高提供服务的质量。

本文件阐述了电子物证检验的最低要求，包括以下框架：

- 1、工作人员能力要求
- 2、仪器和耗材
- 3、采集、分析、解释与结果报告
- 4、程序、操作指南与确认
- 5、质量管理



前言

国际法庭科学战略联盟(IFSA)是6个运转中的地区性法庭科学实验室网络组成的多边伙伴联盟。

- 美国犯罪实验室主任协会(ASCLD)
- 欧洲法庭科学实验室网络(ENFSI)
- 澳大利亚和新西兰法庭科学实验室高级管理者协会(NIFS ANZ)
- 拉丁美洲犯罪学和法庭科学学院(AICEF)
- 亚洲法庭科学学会(AFSN)
- 南非州地区法庭科学学会(SARFS)

IFSA 与莱弗休姆法庭科学研究中心(Leverhulme Research Centre for Forensic Science)、联合国毒品与犯罪问题办公室(United Nations Office on Drugs and Crime, UNODC)和国际刑警组织(INTERPOL)这三个战略伙伴有着紧密合作。

IFSA 认识到,无论是在现场还是在实验室进行的程序,法庭科学实验室的质量管理框架都为提供优质且标准化的结果发挥着重要作用。

2012年2月,在维也纳由UNODC主办的IFSA专门会议上,讨论了发展中国家新建法庭科学实验室的需求,会议决定制定一系列基本要求文件(Minimum Requirement Documents, MRD),以填补目前为管理这些实验室提供有效建议的空白。

在缴获毒品鉴定、DNA分析和犯罪现场勘查等三个特殊领域,分别已编制和修订了第一份文件。这些文件主要集中在质量控制方面,使用简单术语、插图以及词汇表来指导用户理解文档中的重要概念。其他领域的最低要求文件(MRDs)目前正在开发中。欲了解更多信息,请参阅IFSA网站:www.ifsa-forensics.org。

这些MRD文件旨在作为新建法庭科学实验室起始阶段的开端指南,以便迅速建立他们的质量管理体系和科学/技术能力。一旦形成了这种能力,这些实验室应该在此基础上继续发展,通过对制定的标准进行认证,不断努力改进服务质量。

在起草这些文件的过程中,来自6个地区性法庭科学学会的科学工作组和专家们以及IFSA的战略伙伴们,在多轮研讨中作出了宝贵的贡献。没有大家的参与,就不可能形成该系列中最终的基本要求文件。

IFSA希望,在新建法庭科学实验室迈向建立优质法庭科学服务的过程中,这些文件将能发挥重要作用。

IFSA 委员会

2023年9月

1 工作人员能力要求

所有实验室的工作人员必须明确了解自己的职责，并且应始终根据实验室制定的道德准则/专业技能和行为准则(见下方脚注中的实例)¹履行自己的职责。

本节给出了实验室电子物证分析工作人员所需的基本教育水平和（技能）培训的 建议。

1.1 教育

这一鉴定专业往往因教育要求是非传统性的原因而变得复杂。对数字证据进行检验、搜索、提取、展示、解释和保存需要熟练的和多元化的技能，这些技能不仅在传统刑事技术领域需要，也在刑事司法体系以外的其他行业普遍常见，如银行业、多媒体、电信、软件工程等。

这往往导致很难为负责电子物证检验的鉴定从业者制定一个独立的最低培训课程。使专业人员既可以像娱乐行业的多媒体专家一样随意操作，也可以在法庭科学领域自如胜任。

尽管对高等教育要求并不具体，但基于从事工作的性质和复杂性，从业者(检验员/技术员)应持有大学学位或信息技术专业的同等学历(例如网络、音频视频、编程等方面的专业体系认证，或来自认可机构提供的特别注明电子物证的认证)。而且，检验鉴定服务机构还应有证明在岗的实验室教育、培训和经验与实验室开展的鉴定工作相匹配。

鉴于快速发展的技术环境，保持和提升现有电子物证检验人员的技术能力是一个重要的优先事项。必须积极寻求继续教育的机会(如参加学术会议、网络研讨会和查阅相关科学文献)，并应通过专业组织（例如与IFSA合作的组织）以及正式和非正式的论坛与志同道合的从业者互动交流。

除了与电子物证检验相关的技术技能外，优秀的从业人员还应根据其岗位接受以下方面的教育：

- 处理复杂的勘查情况；
- 证据拍照和录像技能；
- 案件管理系统；
- 较强的沟通能力（书面和口头），以及能够用简单的语言表达复杂的内容；
- 在司法（法律程序）环节中展示证据挖掘的能力。

¹区域性法庭科学组织采用的道德准则示例：

- 美国犯罪实验室主任会The American Society of Crime Laboratory Directors (ASCLD) – www.asclcd.org
- 欧洲法庭科学实验室网络The European Network of Forensic Science Institutes (ENFSI) – www.enfsi.eu
- 澳大利亚和新西兰法庭科学实验室高级管理者协会The National Institute of Forensic Science Australian New Zealand (NIFS ANZ) – www.anzfss.org
- 拉丁美洲犯罪学和法庭科学学院Academia Iberoamericana de Criminalística y Estudios Forenses (AICEF) – www.aicef.net
- 亚洲法庭科学学会The Asian Forensic Sciences Network (AFSN) – <https://www.afsn.asia>

1.2 培训

实验室应为新工作人员或新任务制定书面的培训计划。培训应由精通业务、能力胜任和经验丰富的从业人员提供，并且要考虑把检验人员从一般性的通用人才培养成某一专业分支的专业人才(专业分支范围广泛，包括音频和视觉处理、加密算法、工业控制系统、高级手机取证等)。然而，在实验室达到这个专业水平之前，应考虑将复杂疑难的分析工作外包或寻求跨实验室间的合作。培训的类型和级别应针对每个机构电子物证团队的服务模式后具体确定(例如现场提供或仅在实验室进行)。

如果检验鉴定服务机构缺乏相应的技能和经验(例如财务数据分析、多媒体等)，或者待培训的检验人员数量不足以匹配举办内部课程所付出的组织管理工作量，则可以考虑将培训项目全部或部分外包。但是，只有在能够获得合格证书的情况下，这种方式才应被纳入考虑。如果所提供的只是一份参与证明，那么就不能保证技术人员参加培训后的技能水平一定会比培训前有所提高。

培训的有效性应作为实验室质量体系的一部分进行评估。

通过正式和非正式培训课程，以及通过内部、外包或外部课程获得的技术技能都应备案。鉴于信息技术领域的不断发展，应重点考虑培训的频率。无论提供商业还是内部培训课程，接受培训的检验人员应在评估后获得证书，该证书应清楚地说明其能力范围以及该能力的失效时间。尽管未经评估的培训课程在培养检验人员方面也具有明显的作用，但在培养新人员时不应只依赖这些课程。

在独立承担案件检验工作之前，人员或方法应经过评测是胜任还是熟练，并应通过定期评估和测试确保持续认证。

认证文件和持续专业培养的备案记录也是必不可少的。

培训计划应旨在培养以下技能：

- 常见电子物证来源的基本识别、保存和安全处理；
- 电子数据的提取检验；
- 熟悉加密哈希技术，以确保证据完整性，并熟悉常用算法 (MD5, SHA1,² SHA256)；
- 在检验的每个步骤中验证文件完整性并保持证据链(通过应用加密签名，最终由可信任且单独安全的第三方验证)；
- 在加密签名的镜像中保存原始数据；
- 检验分析与分析内容有关的证据副本；
- 记录查找内容和相关信息，以确保可重复性；
- 解释报告结果；
- 检测异常结果并在质量体系中记录反馈；
- 法庭陈述。

²SHA256优于MD或SHA1

2 仪器和耗材

2.1 设施

尽可能将物证接收、处理的存储介质与物证检验区域分开(因为很多电子物品看起来很相似,以防混淆和发生物证丢失的可能)。

用于提取分析电子物证的区域应尽可能连接不间断电源(UPS),以最大程度减少数据损坏和证据丢失。足够数量的电源插座、防静电垫、照明、温度/湿度控制和门禁都是需要考虑的注意事项。

对电子物证操作的任何区域都禁止放置食物、饮料和未封装的液体。

如果进行音频处理,提供专门的“隔声”环境可以大大提高检验人员的工作能力。同样,提供专门的照明或屏蔽设备也将有助检验视频资料。

所有涉及存储、处理和分析的区域都应是安全的并需安装门禁,所有未经授权的人员都必须始终在检验人员的陪同下才能进入区域。他们还应在登记簿上登记签到/离开,以便记录他们在管控区域的时间。

易于清洁的专用搜查室是有必要的,便于处理电子物证(例如笔记本电脑)的同时,提取电子和生物特征(例如指纹, DNA)证据。

存储和处理电子物证的区域应有静电保护装置,以防止损坏证据。

2.2 仪器

固定、提取和处理电子物证所使用的设备有很多,用于检验电子物证的关键设备包括(但不限于):

- 网络基础设施和信息通信技术架构(存储和备份提取的数据);
- 摄像机,用于记录现场、物品和发现的物证(静态照片和动态视频);
- 计算机,用于现场(笔记本)和实验室处理电子物证;
- 只读设备,可确保电子物证安全连接到取证计算机(硬件和/或软件);
- 镜像软件,用于提取有加密签名的证据副本(开源、商业和/或免费);
- 可引导媒介和/或其他所需的硬件,无需使用取证计算机,可直接连接电子物证进行数据传输并提取数据;
- 最新版取证软件(开源、商业和/或免费软件),用于检验和分析证据副本;
- 还应具有完整地记录和复现操作过程的功能;
- 手机数据提取工具; ;
- 刻录设备(例如DVD刻录机),用于制作在法庭展示的证据报告;
- 其他与提取相关的硬件及数据线,用于特殊电子设备的数据提取。

检验人员应维护并熟悉多种操作系统(包括Windows、MacOS和Linux)。所有检验计算机、只读设备和取证软件都应经过核查确定满足日常检验需要。为保证质量并满足可追溯性,所有重要设备的维护和核查日志都应保存记录。

只有经过安全使用设备培训的检验人员才能操作连接,将电子物证接入检验设备进行读取检验。

2.3 耗材

电子物证检验中常用的耗材包括：

- 存储介质，用来存储数据备份和镜像；
 - ◇ 照相机和录像机中的闪存卡；
 - ◇ 存储小数据量的闪存卡、U盘、DVD光盘、磁盘；
 - ◇ 存储大数据量的硬盘；
- 一次性手套，检验人员佩戴免受有害物质损伤，同时也是保护物证避免污染，尤其是当必须先进行电子物证检验时，确保其他证据的完整性（通常是指生物物证）；
- 一次性口罩，确保其他证据的完整性（通常是指生物物证）。

当在多个检验案例之间重复使用数据存储介质时，应当按照相应的规范和程序执行，防止操作过程中造成数据泄漏和存储介质污染。例如，与磁盘擦除操作和核查程序相关的记录都应作为案例档案的一部分予以保存。当磁盘数据被擦除后，必须在使用之前进行验证以确保磁盘被正确擦除，对于容量为4TB 以上的磁盘还应进行额外检查，确保擦除操作有效。

3 采集、分析、解释和结果报告

电子物证检验能力可以定义包括以下几个技术：

- 识别，
- 保存，
- 提取，
- 检验，
- 分析，
- 电子物证检验报告。

3.1 采集

进行搜查是为了定位和确定可能对案件有证据价值的证据。这通常是在对存储设备、局域网、广域网、云环境、虚拟专用网和电信网络设备进行广泛检查之后进行的，以确定是否应将特定设备或环境作为可能的证据包括在内或排除在外。关于是否搜查和扣押物品的原因和决定，应当作为重要内容记录在案卷中。

电子证据包括以多种方式在电子设备上生成或记录的数据。通常在电子证据检验中确定的常见数据类型包括：

- 有效/逻辑数据和元数据(指系统普通用户可见的数据。本文档就是“有效数据”的一个例子)；
- 嵌入式文件元数据和文件/操作系统元数据(指系统存储文件的相关信息，
- 包含时间和日期、路径、硬件和软件的序列号)，某些特殊类型的元数据（如以非标准的方式存储的DVR数据，只能通过制造商的软件或特定领域的软件读取)；
- 备份(包括正规企业备份的重要数据、移动电话数据和云数据³)；
- 无效(已删除)数据(通常包括对系统的普通用户不可见，但可以使用专业知识和工具恢复的数据。这些数据可能是由用户或系统自动删除)；
- 易失性数据(指计算机关闭即消失的数据。最常见的易失性数据是存储在系统内存中的信息)；
- 电信网络数据(包括系统与互联网或企业内部网交互而发送和接收的部分网络流量数据)。

可以提供电子证据的常见电子物品类型包括计算机、笔记本电脑、移动设备、移动应用数据、云数据、网络数据、企业系统、监控系统、车辆系统、无人机、船舶导航系统等。

³ 检验人员应保证在处理云数据时不违反国家法律法规

关注不同类型数据的特点是很重要的，因为在解析数据、提取数据、记录结果、预处理呈现证据价值、封存和保管证据、在法庭上展示证据等各个环节，不同类型数据的处理会面对不同的需求和困难。此外，

应该仔细规划检验流程，以确保在关闭系统前先完成易失性即时数据的采集，以及与系统交互中的动态数据的采集(需要断开无线网络)。

在固定和处理电子物证的过程中，可能会经常遇到受保护或设置某种权限的信息(例如受律师-客户权限、法律专业权限保护或与议会/政府事务有关的保密信息)。应该制定一个恰当的操作程序，确保安全处理这些检材，同时只限于少数必要操作人员的范围内。

处理电子物证时，检验鉴定服务机构和委托双方(如受害者、被告、第三方等)的财务负担也是一个重要的考虑因素，因为它可能会限制刑事司法系统证据的质量、范围和价值。

对前端电子设备以及大型企业系统进行检验需要处理大量复杂数据，为处理这些指数级增长的生成数据而设计开发的软硬件工具数量也在不断增加，使用的工具必须考虑到检验鉴定的特殊需求，这一点至关重要。无论选择什么工具，无论是免费的还是商业的，都应该在使用前进行验证，以确保其满足实验室提出的所有检验要求。

制定提取采集流程时应充分考虑信息技术面临的特殊挑战，并考虑以下几个方面：

- 确定要寻找的目标(最好是在开始检验之前)；
- 满足扣押数据和电子物证的法律要求(如需搜查令的情况)；
- 尽量减少操作干扰，特别是对第三方或数据存储设备的干扰；
- 尽量减少采集的费用。这包括在现场识别和剔除无关的数据源，避免采集和存储不必要的数据；
- 使用独立、专业的检验系统和网络来存储和分析证据；
- 遵守实验室制定的规则和流程；
- 保存收集过程和重要决定的记录。

3.2 分析

一旦确定现有的或存储在设备及环境中的数据具有相关性和可能的价值，就应制定提取流程以最大限度地收集证据。应仔细考虑数据量、数据保存、数据丢失及/或损坏的风险，以及因提取可疑数据可能对各方面造成影响的潜在风险。

3.3 解释

3.3.1 整理结论

考虑到刑事司法制度对承担有关检验的司法管辖权限的特有要求，调查结果的报告需要更细致严谨地编写，例如提供给法院的报告，因为传统的报告编写方式往往不适用于电子证据的展示。

3.3.1.1 结构逻辑

由于采用不同的存储算法，有些电子设备中的数据看起来是非结构化的。而与原始数据相反，在法庭上呈现的结果则几乎都是导出和分析数据。这些数据的结构逻辑既要展示出清晰简明的信息，且又不能以任何形式改变元数据的性质和作用。

3.3.1.2 缩减和筛选数据

随着数据存储设备容量的增长，以及常规系统中文件数量的增加，检验人员已经无法遍历查看设备上的所有内容。因此，使用关键字、搜索条件和文件签名将数据量减少到可操控的级别就尤为重要。应用此类数据缩减策略时，应始终牢记以调查目标为导向，并应记录采用的关键决策，以便第三方能够重现分析路径。但即便采用数据缩减策略，从企业系统获得的数据量也往往会超出最先进的检验鉴定服务机构的能力范围，仍需要特别关注和披露。

3.3.1.3 格式

在生成报告时，应考虑到目标受众，以其能够轻松阅读和理解的格式展示数据。如果不这样做，就会存在遗漏或误解重要信息的风险。转换数据以提高可读性时，也应始终保留与原始未转化数据源相关的链接，以确保可溯源性。

例如当展示移动设备上发现的通话记录等电信数据时，“时间线”就是一个常用的展示方式。如果证据不按时间顺序展示，就很容易产生混淆。

3.3.1.4 核查

对电子设备中提取的数据进行技术检验，通常需要侦查员、当事人、法官在审前会议期间一起全面核查原始数据，以确定相关性并防止收集大量不相关数据，以及泄露受保护的数据类型。对所有生成的报告进行同行评审也应是该过程的一部分。将这部分工作纳入实验室质量体系，有助于确保报告包含恰当的信息。

3.3.2 保全

电子物证鉴定人员有责任保全证据，以防止数据丢失和毁坏，并应按照以下方式履行这项责任：

- 对不同来源获取的数据保持监管和管控；
- 固定保全数字证据，包括备份和灾后恢复详情；
- 记录证据展示策略和关键决策；
- 评估司法管辖权问题、数据量和要求的特殊性/范围；
- 尽可能将数据采集限定到具体的关键字、日期、文件名等细节；

- 将提取数据保存到指定的专用文件夹，并使用加密哈希算法确保数据在每次传输过程中的完整性；
- 与侦查员沟通，以确保鉴定要求不会导致数据扣押数量过大、步骤繁琐。

3.3.3 多媒体数据解释

基于侦查目的，可以使用信号处理软件增强音频和视频证据，特别是在不太理想的条件下录制的音视频证据。通常建议对获取的原始证据进行处理，以免丢失数据。如果不可行，也允许处理转换后的多媒体数据，只要转换过程是合理的、完全公开的。信号处理技术(如滤波)的选择取决于对音视频证据的信号、噪声和失真特性的分析需求。如果增强后的检材是用于法庭展示，鉴定人员将被要求解释信号处理方法及该方法的局限性。一般来说，多媒体数据鉴定人员不提供语音或视频内容的解释，除非他们能够证明具有相应的能力，能使用已得到充分验证适用于特定案情的方法，并且了解与该方法相关的局限性和假设条件。

同样，仅当检验人员能够证明具有运用相关且经过充分验证的方法的能力时，才对音频或视频录制来源或与录制相关的活动做出解释。

3.3.4 挑战

电子物证检验人员可能会遇到以下挑战：

- 在禁止或不可能全面采集数据的情况下，需对数据进行抽样采集；
- 需要紧跟日益复杂的数据源；
- 需掌握广泛应用的加密算法；
- 使用企业级检验系统查看数据的职责；
- 将企业检验系统合并处理多个系统的职责；
- 电子物证检验人员会接触到很多令人不适的电子数据和图像，这在儿童性侵犯案件和反恐调查中很常见；
- 获取云端证据的需求(远程访问数据的立法权力)。

3.4 结果报告

实验室管理人员应确保检验人员编写的所有报告或陈述⁴中至少包含以下信息项：

- 唯一的案例标识号或参考编号；
- 检验人员的全名和身份；
- 所依据的所有相关信息和参考资料的详细信息；
- 检验中的任何限制(无论是由检验人员还是侦查人员提出的)以及检验人员对分析做出的任何假设；

⁴ ILAC G19:2014 S4.9

- 检验人员所采取的程序和操作的清晰阐述，包括所有相关的发现；
- 清楚地区分和确定事实证据，而不是审查员被授权发布的意见证据；
- 报告或陈述中提及的所有证据的保管链；
- 附在报告或陈述中的所有相关日志或原始证据(无论是纸质形式还是数字形式)都应明确说明，或应要求提供。

3.5 数据库

为了尽量减少检验人员接触到令人不适和有争议的材料(这可能导致不必要的压力并影响心理健康)，强烈建议使用哈希数据库。

这些可以仅由各个司法管辖区和机构创建和维护；不过，也应当考虑使用诸如国际刑警组织和VIC项目组分发的通用数据库。

绝不能仅仅依靠哈希数据库进行文件识别和处理，因为人为错误可能导致不正确的分类，或者不同司法管辖区之间的分类也可能不同。

4 程序、操作指南和确认

4.1 程序、操作指南

负责电子物证检验的检验鉴定服务机构制定程序规则应旨在确保相关性，并考虑到信息技术领域的不断发展的特点，制定目标如下：

- 调查各方当事人之间的适当沟通至关重要并确保：
 - ◇ 全面识别和发现所有信息来源；
 - ◇ 保留相关的证据；
 - ◇ 提供相关的证据。

沟通机制可能包括与调查人员磋商的流程，以帮助确定所需的协助类型或级别，这将有助于检验人员集中精力制定检验策略（日期/时间、证据类型），并确定可能影响流程或方法的任何特殊关注点（例如需要访问云数据）。

定义和记录程序的规则需要确保：

- 检验人员必须了解并遵循指导程序的规则；
- 检验人员必须了解支撑该流程的基础结构；
- 检验人员必须了解并遵循所有相关检验中规定的流程；
- 检验人员必须了解并记录检验的局限性；
- 应考虑与电子物证检验相关的风险，所有流程应始终考虑经费影响、操作中断、证据弱化、潜在的司法妨碍以及因发出全部访问指令而导致的失控和过度占用。典型的考虑因素包括：
 - ◇ 确定相关文件；
 - ◇ 通知文件所有者或保管人；
 - ◇ 与各方商定检验程序，特别是当进行企业系统检验时更有必要；
 - ◇ 保存相关文件；
 - ◇ 监督保管合规性；
 - ◇ 记录过程。

处理电子证据时需要采取一些步骤，主要包括：

- 收集电子证据；
- 整理案例元数据；
- 核查提取的数据以确定相关性；
- 生成结果报告。

4.2 确认

任何用于处理和分析证据的工具（开源、免费或商业）都应定期更新以改进现有方法或减少已知风险。每次更新后，都应通过验证评估其适用性。这样既保证结果是可靠的，并且使各方都知晓了解所使用工具的错误率。

由于商业工具并不总能够处理每一种情况，检验人员通常会开发一次性软件工具（通常称为“脚本”）来辅助处理证据。所有此类工具也应针对一系列已知（基准）数据集（适用的）进行测试，测试变量应涵盖定义特定数据集性质的隐式和显式参数，以确保其以正确方式运行，且所有衍生信息或证据都是可靠的，同时各方均应了解知晓所使用工具的错误率。测试记录应予以保留。

应定期检查用于保护证据数据源的只读工具、适配电源和数据线是否正常运行，以确保检验人员不会无意间更改证据源。当使用新的只读工具或升级现有工具（无论是软件还是固件升级）时，这一点尤为重要。应保存只读工具正确操作的日志记录，以供在法庭或审查流程中使用。

5 质量管理

质量管理是确保电子物证检验人员工作有效、可信赖的管理程序。质量管理应基于程序中的每一步，而不是在最后才进行检查。总而言之，该程序还应反映出持续改进的努力。

电子物证与传统刑事技术有些不同，许多司法辖区和场所并不寻求或保持ISO/IEC 17020或ISO/IEC 17025等质量体系认可。即使不需要完全认可，也应考虑采用部分国际标准，因为这些标准可以极大地帮助提高实验室工作的质量。至少，该单位应该寻求符合ILAC G19:2014的要求。

电子物证检验人员在处理现场和任何衍生证物时，至少应该有一个监管重要操作的检查清单（例如证物细节、技术/流程、使用的软件/硬件），以帮助保持证据和证据管理（或监管链）的完整性。

该场所应保持并遵循关于文件保留的程序，具体涉及：

- 熟练测试；
- 从业者的能力；
- 使用基准数据集对分析结果进行验证；
- 样品接收和处理记录；
- 数据保留；
- 纠正措施；
- 审计；
- 培训记录；
- 持续的专业建设；
- 法庭证词监督。

质量管理程序应具体说明并记录所有工作人员的责任、权限和相互关系，他们的管理、操作或验证都会影响到电子物证调查的有效性。

应考虑使用认证过的能力测试来验证电子物证检验的程序、实验室和从业者。如果有这样的能力测试，则应涵盖从初级通用电子证据处理技能到高级专业化分支学科的各种主题模块。电子物证检验所有步骤的错误率都需知悉并报告。

当没有认证的能力测试时，应寻求与同类实验室进行协作练习。这些练习的主要目的应是核查实验室的流程，以确保使用已知基准数据进行检验的一致性和有效性。这是对实验室方法的检查，而不是对个别工作人员的检查。



6 术语表

以下术语表不应被视为电子物证检验中遇到的术语的详尽列表，而是法庭科学领域广泛应用的术语。

DVD	数字多功能光盘
USB	通用串行总线
电子证据	电子证据是指以数字或模拟形式存储或传输的任何涉及调查或法庭事项的信息
数字证据	数字证据通常可以与电子证据互换使用，但可以用于特指以数字形式存储或传输的涉及调查或法庭事项的信息。
多媒体证据	涉及音频和视频录制以及图像的电子证据

IFSA 成员



战略合作伙伴





联系:

国际法庭科学战略联盟: <http://www.ifsa-forensics.org>

