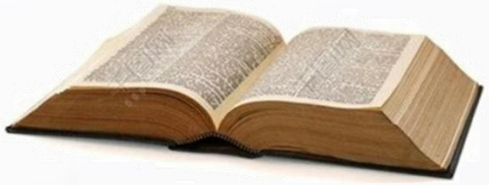
信息安全法律基础

法律遵从，科技向善

——共建网络空间安全



第7章 电子数据取证与法律规制

第7章 电子数据取证与法律规制

7.1 电子数据取证的发展历程

7.2 电子数据取证的立法规制

知识点探究

- 了解和学习《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》、《公安机关办理刑事案件电子数据取证规则》等相关法规，收集相关案例，探讨电子数据取证的法律规制。
- 收集相关案例，探讨电子数据取证的技术问题。

7.1 电子数据取证的发展历程

7.1 电子数据取证的发展历程

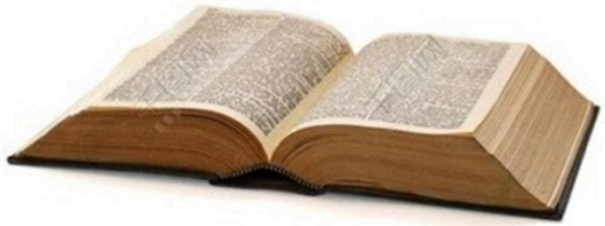
7.1.1 电子数据取证的概念

- 电子数据取证是随着信息技术的飞速发展而出现的一门新兴学科，相关研究始于1984年美国联邦调查局（FBI）成立的计算机分析响应组（CERT）。
- 20世纪90年代初，美国联邦犯罪调查实验室创立“数字取证科学工作组（SWGDE）”，工作组首次提出了“计算机潜在证据”的概念，是“电子数据取证”概念的雏形。

7.1 电子数据取证的发展历程

7.1.1 电子数据取证的概念

- EE-discovery—电子文件或者电子数据的获取。（由诉讼各方当事人及其律师负责取证工作）
- Computer Forensic—对以比特形式存储或者传递的数据加以恢复、保存、检查的各种工具或技术。（由特别聘请或委托的计算机专家负责取证工作）
- 电子数据取证—能够为法庭接受的、足够可靠和有说服力的、存在于计算件机和相关外设中的电子证据的确定、收集、保护、分析、归档以及法庭出示的过程。
- 在网络犯罪侦查领域，对网络犯罪行为进行分析以确认犯罪，很大程度上是对电子数据的获取过程。



7.1 电子数据取证的发展历程

7.1.2 国外电子数据取证的里程碑

1 1995-2005年，电子数据取证成为专业技术领域

- 电子数据取证发展的三个驱动因素
  - 技术爆炸—计算机、互联网等新技术催生了新的产业，也伴生了新的犯罪。
  - 儿童色情案件的不断出现—这种“新”违规行为导致数字证据数量不断增加。
  - 2001年的911事件—虽然计算机在劫持事件里几乎没有直接的发挥作用，但是调查人员在世界各地的计算机上找到大量证据，证明恐怖分子像其他人一样大量使用了计算机。
- 1999—2000年，高科技犯罪小组委员会和数字取证科学工作组（SWGDE）发布了数字取证原则。美国犯罪实验室主任协会暨实验室认证委员会（ASCLD/LAB）和SWGDE合作把数字证据学确认为实验室学科。2004年FBI的北德克萨斯计算机取证实验室成为第一个获得认可的数字取证实验室。

7.1 电子数据取证的发展历程

7.1.2 国外电子数据取证的里程碑

2 2005-2010年，数字取证成为信息安全专业的核心技能

- 2006年美国法院通过新的民事诉讼规则，将电子数据界定为新的证据形式，并开发名为“电子发现”的强制性系统处理电子证据。
- 2007年FBI宣布计算机分析响应组（CERT）检查的证据超过2.5PB。
- 各种取证套件（如EnCase和FTK）以企业安全和电子发现的目的在企业部署，并应用于虚拟化、存储区域网等新兴取证环境。

3 2010年以来，传统电子数据取证技术面临巨大挑战

- 加密、云计算、大数据等新技术发展，各国纷纷立法保护网络隐私，传统技术手段无法有效解决新形势下电子数据取证困境，电子数据取证技术不断升级。

7.1 电子数据取证的发展历程

7.1.3 我国电子数据取证的现状

1 电子数据取证规制

- 2008年公安部网络安全保卫局颁布《公安机关网安部门电子数据检验鉴定实验室能力和装备分级标准》，第一次对各级公安机关的**电子数据取证能力**提出了分级要求和装备标准，电子数据取证工作方式从单兵设备模式转变为**实验室模式**。
- 2012年，刑诉法、民诉法和行政诉讼法均明确**电子数据证据作为独立的证据形式**。应用电子数据取证技术的执法行业由以公安的网安部门为主，演变为各个执法部门都采用电子数据取证技术来为执法保驾护航。
- 2016年10月1日起施行《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》。
- 2019年2月1日起施行《公安机关办理刑事案件电子数据取证规则》。

7.1 电子数据取证的发展历程

7.1.3 我国电子数据取证的现状

2 电子数据取证技术与行业

- 2001年，我国从针对黑客入侵取证开始引入计算机取证技术，以现场取证和介质分析系统为主。
- 2006年，专门针对手机取证的产品开始在市场上出现，并针对中国的山寨机，内置了山寨机字库提取分析模块，成为执法人员标配设备。
- 2008年，国内多家电子数据取证产品供应商开始提供自主研发的电子数据取证产品，国产自主知识产权的产品开始挤占国外进口产品的市场空间。
- 2010年，实验室装备向集成化和系统化方向发展，多接口、多功能的一体化取证设备开始应用于实验室，并采用集中存储，分布式处理的思想进行升级改造。

7.1 电子数据取证的发展历程

7.1.4 电子数据取证的发展趋势

1 从“事后取证”向“中期研判”、“前期采集”发展

- 电子数据证据的获取时点呈现前置趋势，可以帮助案件侦破和事前预防。
  - 面向前期的数据采集产品（手机数据采集、计算机数据采集、暴恐/非法内容检测产品）
  - 面向中期的大数据研判平台
  - 融合前期采集、中期研判、后期取证各类产品，形成数据安全全生命周期的统一解决方案

2 取证对象种类越来越多

- 大数据、云计算、嵌入式、传感器技术，使得数据源无处不在，取证对象的种类和数量较传统提高了几个数量级。
- 云端、暗网、智能汽车以及其他智能设备的取证需求不断出现，部分厂商如美亚柏科推出包括汽车取证系统、暗网取证系统、无人机取证系统等新形态的商业化电子数据取证设备。

7.1 电子数据取证的发展

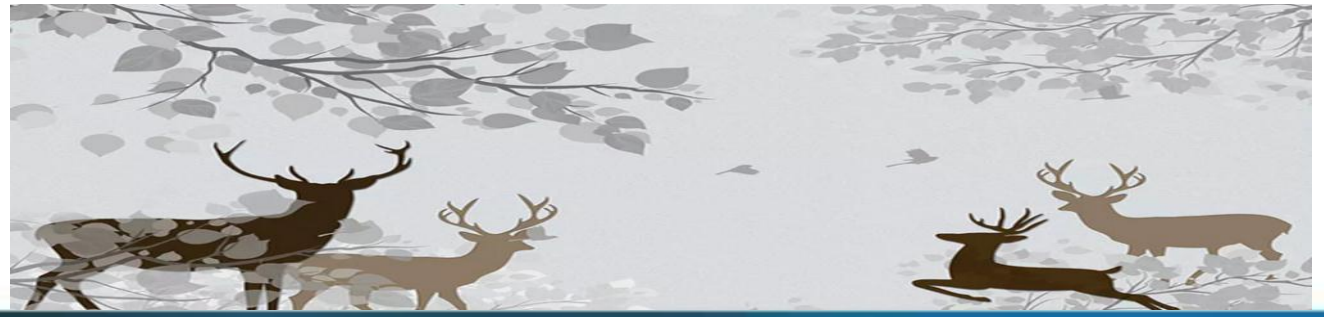
7.1.4 电子数据取证的发展趋势

3 反取证技术和隐私保护带来挑战

- 加密、匿名、隐写等反取证技术给电子数据取证工作带来很大挑战。
- 由于隐私保护等原因，终端和操作系统厂商，特别是移动终端和移动操作系统（iOS、Android）加大了数据保护力度，电子数据取证已经演变为取证厂商和设备厂商之间的安全对抗。
- 电子数据取证厂商使用“漏洞”思维解决电子数据取证对抗问题。

4 综合取证技术是未来发展方向

- 电子数据证据以各种形式存在，不再是单一的“数据孤岛”，单兵工具无法统一处理各种电子数据证据，需要研发综合取证产品和取证大数据平台，构建大数据综合研判系统。



7.2 电子数据取证的立法规制

7.2 电子数据取证的立法规制

7.2.1 电子数据取证立法规制的背景

- 随着互联网的快速发展，不仅是网络犯罪案件，越来越多的传统刑事案件也需要电子数据取证，迫切需要建立**电子数据取证规则体系**。
- 2012年以前，大多数对电子数据的规定仅仅局限于鉴定范畴，极少有文件提及电子数据收集提取的问题。在案件侦查、起诉和审判的实践过程中，多将电子数据转化为其他证据类型使用。
- 2012年，修改后的《刑事诉讼法》将电子数据确立为**法定证据类型**，从根本上确立了电子数据的**独立证据地位**。
- 同年，最高人民法院出台了《关于适用〈中华人民共和国刑事诉讼法〉的解释》，第九十三条和第九十四条对电子数据审查判断的**最基本原则**进行了规定。
- 2014年，最高人民法院、最高人民检察院、公安部联合出台了《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》，专设一章对电子数据的收集以及专门性问题的认定若干原则进行了明确。

7.2 电子数据取证的立法规制

7.2.1 电子数据取证立法规制的背景

- 2016 年，最高人民法院、最高人民检察院、公安部联合出台了《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》进一步统一了公检法部门在司法实践中对电子数据的认识和判断标准，提出了电子数据收集提取、审查判断的具体方法，明确了电子数据真实性、合法性、关联性审查的原则，确立了扣押原始存储介质为主、提取电子数据为辅、打印拍照为例外的电子数据取证原则。
- 为各地公安机关更好地执行《规定》，规范公安机关在办理刑事案件过程中的电子数据取证工作，公安部于2018年12月13日发布了《公安机关办理刑事案件电子数据取证规则》。

7.2 电子数据取证的立法规制

7.2.2 《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》

- 2016年9月9日，最高人民法院、最高人民检察院、公安部印发《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》的通知，本规定自2016年10月1日起施行。
- 目的：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，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，制定本规定。
- 《规定》框架
  - 一、一般规定
  - 二、电子数据的收集与提取
  - 三、电子数据的移送与展示
  - 四、电子数据的审查与判断
  - 五、附 则

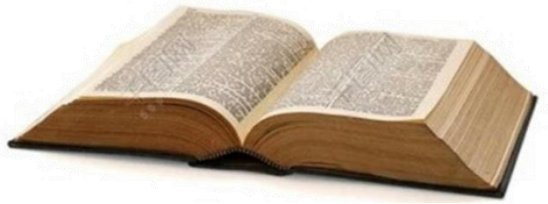
7.2 电子数据取证的立法规制

7.2.2 《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》

- 相关定义
  - **电子数据：**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。
  - **存储介质：**具备数据信息存储功能的电子设备、硬盘、光盘、优盘、记忆棒、存储卡、存储芯片等载体。
  - **完整性校验值：**为防止电子数据被篡改或者破坏，使用散列算法等特定算法对电子数据进行计算，得出的用于校验数据完整性的数据值。

7.2 电子数据取证的立法规制

7.2.2 《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》

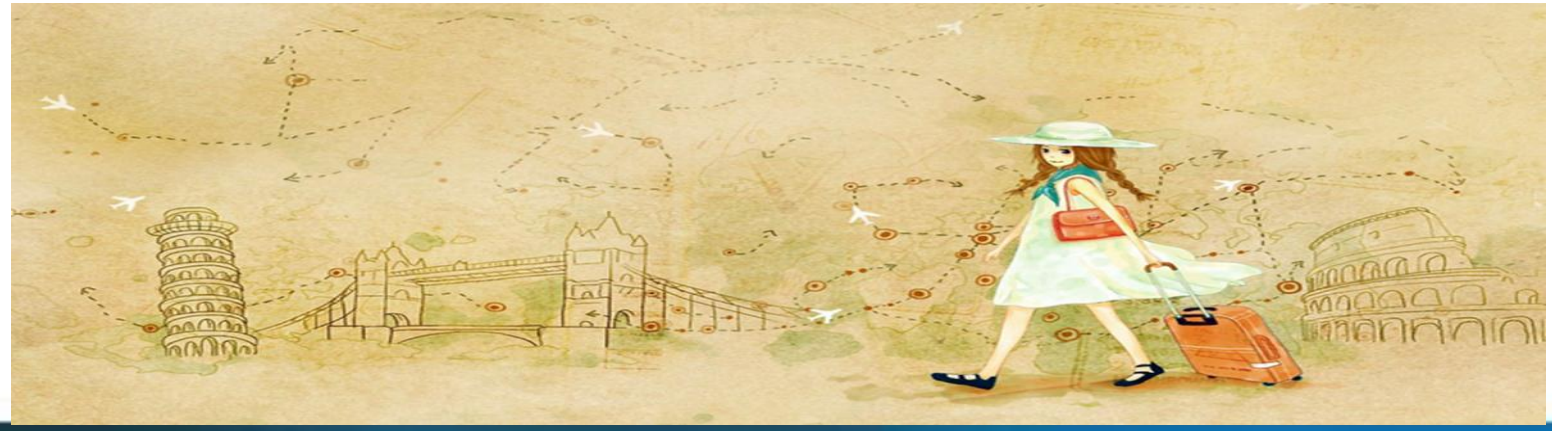


- 相关定义
  - **网络远程勘验**：通过网络对远程计算机信息系统实施勘验，发现、提取与犯罪有关的电子数据，记录计算机信息系统状态，判断案件性质，分析犯罪过程，确定侦查方向和范围，为侦查破案、刑事诉讼提供线索和证据的侦查活动。
  - **数字签名**：利用特定算法对电子数据进行计算，得出的用于验证电子数据来源和完整性的数据值。
  - **数字证书**：包含数字签名并对电子数据来源、完整性进行认证的电子文件。
  - **访问操作日志**：为审查电子数据是否被增加、删除或者修改，由计算机信息系统自动生成的对电子数据访问、操作情况的详细记录。

7.2 电子数据取证的立法规制

7.2.3《公安机关办理刑事案件电子数据取证规则》

- 本规则2018年12月13日发布，自2019年2月1日起施行，公安部之前发布的文件与本规则不一致的，以本规则为准。
- 制定《规则》目的
  - 为规范公安机关办理刑事案件电子数据取证工作，确保电子数据取证质量，提高电子数据取证效率，根据《中华人民共和国刑事诉讼法》《公安机关办理刑事案件程序规定》等有关规定，制定本规则。



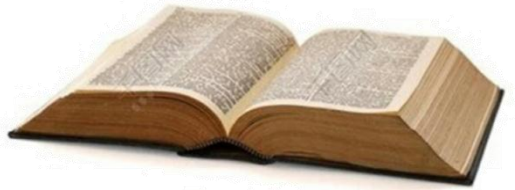
7.2 电子数据取证的立法规制

- 《规则》框架
  - 共五章61条

- 第一章 总 则
- 第二章 收集提取电子数据
  - 第一节 一般规定
  - 第二节 扣押、封存原始存储介质
  - 第三节 现场提取电子数据
  - 第四节 网络在线提取电子数据
  - 第五节 冻结电子数据
  - 第六节 调取电子数据
- 第三章 电子数据的检查和侦查实验
  - 第一节 电子数据检查
  - 第二节 电子数据侦查实验
- 第四章 电子数据委托检验与鉴定
- 第五章 附 则

7.2 电子数据取证的立法规制

- **《规则》特点**



1 综合各个警种电子数据取证工作特点和实际

- 综合分析刑事案件现场勘查、扣押时拍照打印，电子数据网络在线提取等情形，参考毒品犯罪电子数据取证有关规定，从电子数据的现场处置到实验室检查，再到电子数据的委托检验均有规定。

2 以实践中反映的突出问题为导向

- 对实践中广泛存在的录像、电子数据冻结的细节、拍照打印的适用性等问题均提出了解决办法。

3 坚持同有关法律法规保持一致和衔接

- 对“两高一部《规定》”进一步具体化， 将《公安机关办理刑事案件程序规定》、《公安机关刑事案件现场勘验检查规则》等规定以及有关警种出台的特别规定进行梳理研究，统一相关要求，保证同既有文件的协调一致。

7.2 电子数据取证的立法规制

- 《规则》内容释义

1 明确了电子数据取证的阶段划分

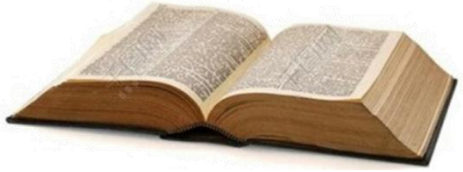
- 电子数据与物证不同，收集提取后需要公安机关进行恢复、破解、搜索、仿真、关联、统计、比对等处理后， 才能更好地展示。因此，《规则》第三条将电子数据取证划分为三个阶段：收集、提取电子数据；电子数据检查和侦查实验；电子数据检验与鉴定。

2 进一步强调了原始存储介质的扣押封存

- 《规定》明确了“能够扣押原始存储介质，应当扣押、封存原始存储介质”的原则，但实践中不封存或者封存不规范的问题仍然存在。因此，《规则》专门对电子数据原始存储介质扣押封存进行了规定。

7.2 电子数据取证的立法规制

- 《规则》内容释义



3 进一步统一电子数据现场取证规范

- 公安部《公安机关刑事案件现场勘验检查规则》第三十二条明确“勘验、检查与电子数据有关的犯罪现场时，应当按照有关规范处置相关设备，保护电子数据和其他痕迹、物证。”
- 公安部网络安全保卫局《计算机犯罪现场勘验与电子证据检查规则》对计算机犯罪现场的取证规则和文书进行了规范。
- 《规则》在同已有规定保持衔接的基础上，对现场收集、提取电子数据有关规范进行了统一，明确了现场收集、提取电子数据的适用情形、有关原则和笔录要求。

4 明确“拍照打印”方式的适用情形

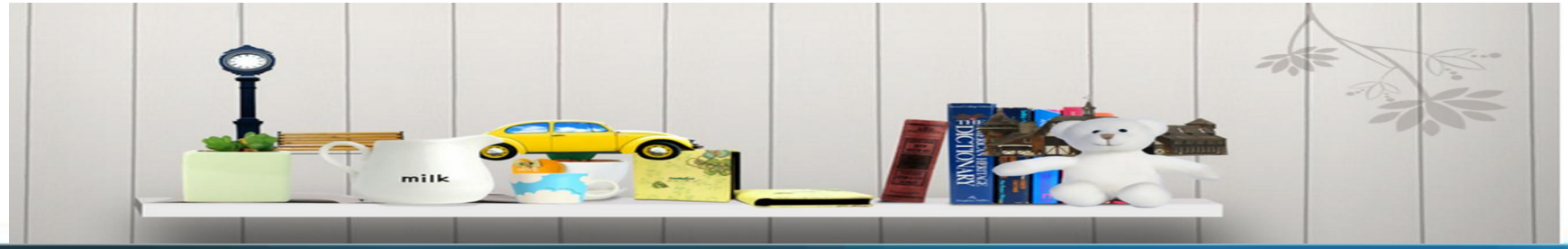
- 拍照打印方式具有操作简单、及时固证等优点，部分案件能够省去检查、检验、鉴定等后续环节，有利于节约侦查成本。为此，《规则》明确了在扣押原始存储介质前，可以通过拍照打印方式先行固定电子数据内容。

7.2 电子数据取证的立法规制

- 《规则》内容释义

5 明确无见证人时录像规范

- 现场执法环节在扣押原始存储介质及现场提取电子数据环节无见证人见证的情况下，应当全程录像。
- 网络远程提取同现场情形存在较大区别，特别是网络带宽受限时，网络远程提取所需时间可能是现场的十几倍甚至上百倍，并且大多数时间是无人工干预的数据传输时间。公安部《规则》对此种情形的录像要求进行了区分，即对于重大案件、电子数据是关键证据等案件，应当全程录像；而对于一般性网络远程提取，则仅需对关键步骤录像。《规则》将人工操作的环节纳入关键步骤，大量的下载等无人工干预的过程未纳入关键步骤，不再需要录像。



7.2 电子数据取证的立法规制

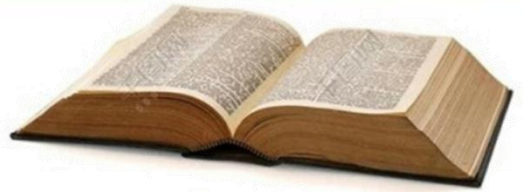
- 《规则》内容释义

6 明确登记保存的适用情形

- 公安部《公安机关办理刑事案件程序规定》第二百二十六条提出了登记保存的规定。
- 《规则》对登记保存的时间也进行了规定，明确“对登记保存的原始存储介质， 应当在七日以内作出处理决定，逾期不作出处理决定的，视为自动解除。经查明确实与案件无关的，应当在三日以内解除”。
- 例：在某案件中，涉案服务器多达800 余台，由公司自行建设维护，无法采取冻结措施（针对云服务），并且难以扣押，即使能够扣押， 也难以重建整个系统，为此公安机关采取了登记保存的措施。

7.2 电子数据取证的立法规制

- 《规则》内容释义



7 明确网络在线提取和远程勘验的区别

- 远程勘验兼具收集提取“电子数据” 和进一步收集“有关信息”、查明“有关情况”的功能，侧重于侦查人员分析、判断、发现过程， 是对虚拟现场、电子数据的客观描述，可以独立作为证据。
- 网络在线提取只有收集提取“电子数据”的功能， 主要是对电子数据来源的说明。

8 明确了网络在线提取的适用范围

- 《规则》将网络在线提取范围规定在境内电子数据和境外公开发布的电子数据。
- 境外非公开发布的电子数据，通过国际条约或者合作机制调取证据；通过勘验境内访问、下载终端间接获取；通过技术侦查措施获取；转化为其他类型的证据。
- 对“公开发布的电子数据”宜作扩大解释，不能机械地将是否需要用户名密码访问作为条件，如赌博、色情、诈骗等网站位于境外，境内不特定对象注册、登陆后均可以访问，可以使用网络在线提取。

7.2 电子数据取证的立法规制

- 《规则》内容释义

9 关于冻结电子数据的程序和期限问题

- 《规则》参考冻结存款、汇款等财产等程序，将冻结期限限定为六个月，并且明确不需要继续冻结电子数据时，应当在三日内通知电子数据持有人、网络服务提供者或者有关部门执行。同时，冻结方法增加了“写保护措施”。

10 明确了调证的异地协作流程

- 办理刑事案件常常涉及异地调证，实践中办案单位出差调证屡见不鲜，不仅耗费了大量人力、物力，而且严重影响了侦查效率。
- 《规则》规定文书盖章后邮寄，电子数据通过信息化系统传回，简化协作地审批流程，即由办案部门审批即可。

7.2 电子数据取证的立法规制

- 《规则》内容释义

11 明确了电子数据检查的性质

- 《规则》允许本案的侦查人员作为检查人员，并针对实践中办案人员交其他警种侦查人员检查的情形， 规定涉案原始存储介质或者电子数据移交需要履行相应的手续。
- 对检查人员要求具有专业技术，一般以公安机关警务技术任职资格为条件。
- 一名侦查人员可能同时满足“具有专业技术”和“具有专门知识”两个条件。

12 明确电子数据检查是否需要见证人

- 《规定》对电子数据检查未要求见证人见证。一方面，电子数据检查一般在备份件或者写保护情况下进行，对于既无法备份又无法写保护的特殊情形，要求全程录像；另一方面，电子数据检查的场所往往涉密， 不便寻找符合法定条件的人员担任见证人。
- 《规则》同样未对电子数据检查见证人作硬性要求。

感谢聆听