# 第3章 手机取证的流程和规范

对于手机取证的流程和规范，目前国内还没有统一的标准，本章参考了各国计算机取证和手机取证的流程、规范和规定，并根据国内实际的取证调查实际进行了修改，提出了基于国际标准、符合国情的手机取证调查流程和规范，在目前相关法规尚未完善的国内，这些流程和规范能够给予手机取证调查人员一定价值的参考。

## 3.1 流程与规范概述

手机取证作为电子数据取证的一个新兴领域，在国内，目前尚未形成健全和受到广泛认可的流程和规范，如同计算机取证一样。而在西方国家，与电子数据取证有关的法律法规已十分成熟，在业内已经具有一系列被广泛接受和认可的流程规范，下面是几个在电子数据取证领域具有指导性作用的指导性原则。

- 英国高级警官协会 ACPO：Good Practice Guide for Computer based Electronic Evidence(计算机及电子证据指导原则)[①]，如图 3-1 所示。
- 美国司法部 DoJ：Electronic Crime Scene Investigation：A Guide for First Responders，Second Edition(电子犯罪现场调查：现场响应指导原则 第二版)[②]，如图 3-2 所示。

除了这两个广为人知的标准，其实，早在 2002 年，国际计算机证据组织(International Organization on Computer Evidence，IOCE)就推出了一个关于电子证据的指导纲领 Guidelines for Best Practice in the Forensic Examination of Digital Technology(数字技术取证调查指导纲领)[③]。在今天看来，这个指导纲领对于很多技术方面的描述都已显得有些过时，但是，其中所阐述的指导原则却一直被沿用至今。

在国外，此类适用于计算机取证的原则已经被广泛应用在包含手机取证在内的各种电子数据取证领域中，并被广大从事电子数据取证的调查人员所接受。经过十余年的发展，电子数据取证理论和法律问题在西方已十分完善，可谓“前人之述备矣”，这些原则中对于电子证据的定义、处置、保全是具有指导性意义的，所有基于电子介质的取证工作均

① ACPO Good Practice Guide for Computer based Electronic Evidence：http://www.dataclinic.co.uk/ACPO%20Guide%20v3.0.pdf.

② Electronic Crime Scene Investigation：A Guide for First Responders，Second Edition：http://www.nij.gov/pubs-sum/219941.htm.

③ Guidelines for Best Practice in the Forensic Examination of Digital Technology：http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html.


图 3-1　ACPO 指导原则

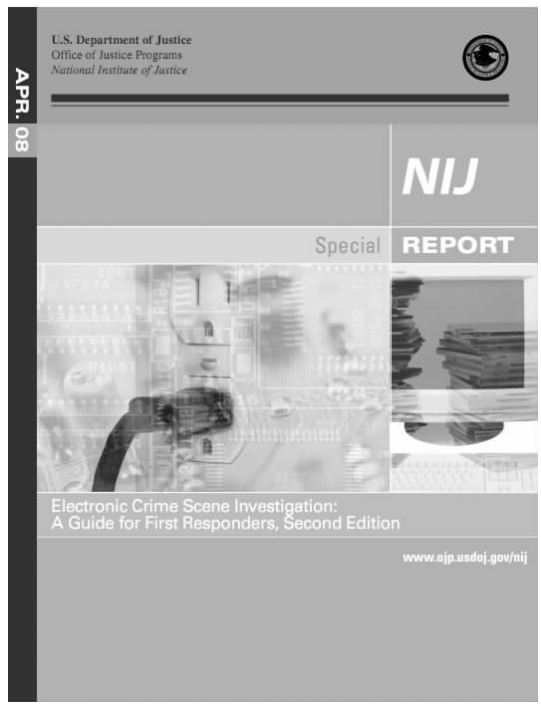



图 3-2　美国司法部指导原则

可以以此类权威指导原则为参考。

同时，针对手机取证，在一些西方国家也已经有了专门的行业指导原则，如美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）于 2007 年起发布了一系列的专门针对手机取证的指导文档：

- Guidelines on Cell Phone Forensics（手机取证指导原则），如图 3-3 所示。

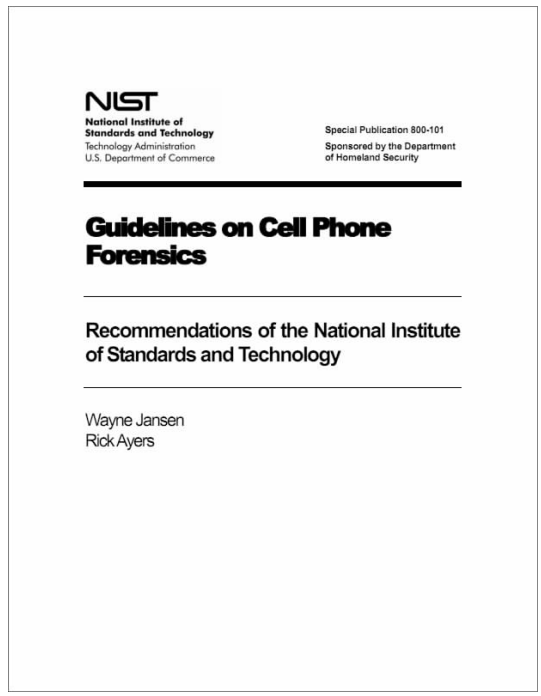


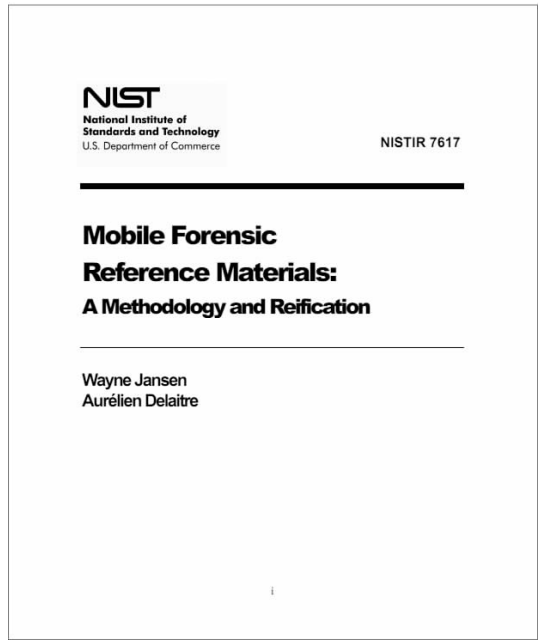

图 3-3　NIST 800-101 文档
Guidelines on Cell Phone Forensics（手机取证指导原则）

- Mobile Forensic Reference Materials：A Methodology and Reification（手机取证参考资料：理论和实务），如图 3-4 所示。

在美国具有一定影响力的、由 FBI、CIA 和特勤局调查人员成立的数字证据科学工作组（Scientific Working Group on Digital Evidence，SWGDE）在总结和整合 ACPO 及 NIST 指导方针的基础上，于 2009 年 5 月发布了 Best Practices for Mobile Phone Examinations（手机取证调查的最佳实践），阐述了手机取证所涉及的常用概念，以及从手机证据的收集到最终检验分析直至存档需要注意的事项和重点，为手机取证调查人员提供了简明扼要的指导规范，如图 3-5 所示。

本章节中，对于手机取证的具体流程和规范主要参考和遵循了上述 6 个规范，并根据国内手机取证调查实际进行了相应的扩展和延伸。

同时，随着近年来国内各类执法部门逐步提高了对于电子数据取证的重视，也推出了一些行业标准以及操作规范，如表 3-1 所示。对于国内执法部门的取证调查人员，应根据自己的实际情况遵循符合自身调查要求的流程、规范和制度。



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 7617

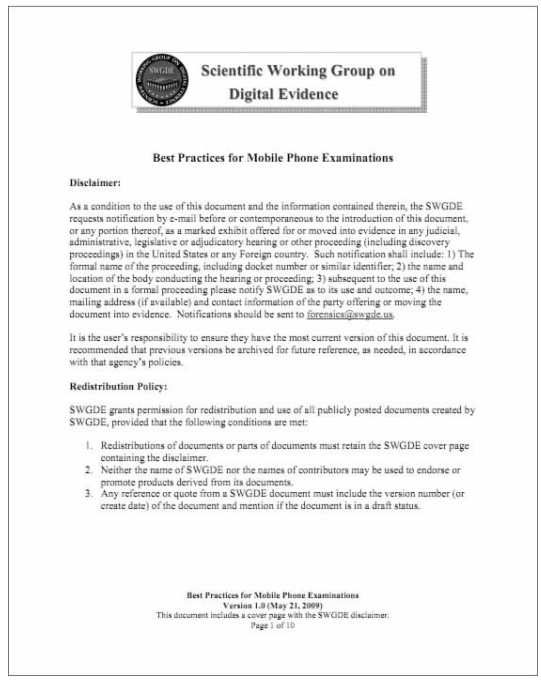
**Mobile Forensic Reference Materials:**
**A Methodology and Reification**

Wayne Jansen
Aurélien Delaitre

i

图 3-4　NISTIR 7617 文档

Mobile Forensic Reference Materials：A Methodology and Reification(手机取证参考资料：理论和实务)



Scientific Working Group on
Digital Evidence

**Best Practices for Mobile Phone Examinations**

**Disclaimer:**

As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to forensics@swgde.us.

It is the user's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived for future reference, as needed, in accordance with that agency's policies.

**Redistribution Policy:**

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistributions of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.



图 3-5　Best Practices for Mobile Phone Examinations(手机取证调查的最佳实践)

**表 3-1　国内电子数据取证的行业指导规范及相关规定摘录**

| 法条、制度或规定 | 内 容 摘 要 |
| --- | --- |
| 《最高人民法院、最高人民检察院、海关总署关于办理走私刑事案件适用法律若干问题的意见》（2007 年 7 月 8 日） | 二、关于电子数据证据的收集、保全问题<br>走私犯罪侦查机关对于能够证明走私犯罪案件真实情况的电子邮件、电子合同、电子账册、单位内部的电子信息资料等电子数据应当作为刑事证据予以收集、保全<br>侦查人员应当对提取、复制电子数据的过程制作的有关文字说明，记明案由、对象、内容，提取、复制的时间、地点，电子数据的规格、类别、文件格式等，并由提取、复制电子数据的制作人、电子数据的持有人和能够证明提取、复制过程的见证人签名或者盖章，附所提取、复制的电子数据一并随案移送<br>电子数据的持有人不在案或者拒绝签字的，侦查人员应当记明情况；有条件的可将提取、复制有关电子数据的过程拍照或者录像 |
| 最高人民法院关于开展《人民法院统一证据规定（司法解释建议稿）》试点工作的通知（法[2008]129 号） | 第十四条（证据及其种类）<br>（七）音像、电子证据，是指以磁带、光盘、胶片或者电子芯片等储存的信息，记述有关案件事实的资料<br>第十六条（原始证据优先）<br>调查人员调查收集的物证、书证和音像、电子证据，应当是原物、原件、原始载体，提取原物、原件、原始载体确有困难的，在下列情形下，也可以是经核对无误的复制品或者照片、副本或者复制件，但应当在调查笔录中说明来源和取证情况<br>第二十条（音像、电子证据的规格）<br>音像、电子证据，应当注明作者或者收集人的姓名，制作或者收集时间、地点、过程<br>声音资料应当附有该声音内容的文字记录；<br>电子证据应当附有提取、复制过程的有关文字说明，注明提取和复制的时间、地点，电子数据的规格、类别、文件格式，提取、复制电子数据的提取人、持有人和保管人<br>第一百条（电子证据的辨认与鉴真）<br>电子证据的真实性，在对方提出异议时，由制作人、见证人和保管人以及其他了解该电子证据制作、保管过程的人辨认和鉴真<br>电子证据的辨认和鉴真包括不限于以下因素<br>（一）生成、存储、传递和保存方法的可靠性<br>（二）生成、存储、传递和保存环境要素及相关协议<br>（三）电子文件的属性和品质<br>（四）可能进入信息交流系统的人及其对该系统的熟悉程度<br>（五）设立密码、电子签名、用户名、账号的电子证据，其密码、电子签名、账号的设立人、使用人、所有人以及该用户名或者账号的使用情况<br>（六）传输过程中的解密性<br>（七）系统硬件是否完好，软件是否可靠，系统运行是否正常，是否受到过病毒等的侵袭；存储的资料是否存在被编辑、修改的可能性<br>（八）复制件制作的方法是否真实完整地反映了原件记载的内容 |
| 《人民检察院电子证据鉴定程序规则（试行）》（最高人民检察院，2009 年 4 月） | （全文略） |

续表

| 法条、制度或规定 | 内 容 摘 要 |
| --- | --- |
| 《最高人民法院、最高人民检察院、公安部、国家安全部、司法部关于办理死刑案件审查判断证据若干问题的规定》（法发[2010]20号） | （二）收集电子数据应当依法制作笔录，详细记载取证的参与人员、技术方法、步骤和过程，记录收集对象的事项名称、内容、规格、类别以及时间、地点等，或者将收集电子数据的过程拍照或录像<br>（三）收集的电子数据应当使用光盘或者其他数字存储介质备份。监管机构为取证人时，应当妥善保存至少一份封存状态的电子数据备份件，并随案移送，以备法庭质证和认证使用<br>（四）提供通过技术手段恢复或者破解的与案件有关的光盘或者其他数字存储介质、电子设备中被删除的数据、隐藏或者加密的电子数据，必须附有恢复或破解对象、过程、方法和结果的专业说明。对方当事人对该专业说明持异议，并且有证据表明上述方式获取的电子数据存在篡改、剪裁、删除和添加等不真实情况的，可以向人民法院申请鉴定，人民法院应予准许 |
| 《最高人民法院 最高人民检察院 公安部关于办理网络赌博犯罪案件适用法律若干问题的意见》（公通字[2010]40号） | 五、关于电子证据的收集与保全<br>侦查机关对于能够证明赌博犯罪案件真实情况的网站页面、上网记录、电子邮件、电子合同、电子交易记录、电子账册等电子数据，应当作为刑事证据予以提取、复制、固定<br>侦查人员应当对提取、复制、固定电子数据的过程制作相关文字说明，记录案由、对象、内容以及提取、复制、固定的时间、地点、方法，电子数据的规格、类别、文件格式等，并由提取、复制、固定电子数据的制作人、电子数据的持有人签名或者盖章，附所提取、复制、固定的电子数据一并随案移送<br>对于电子数据存储在境外的计算机上的，或者侦查机关从赌博网站提取电子数据时犯罪嫌疑人未到案的，或者电子数据的持有人无法签字或者拒绝签字的，应当由能够证明提取、复制、固定过程的见证人签名或者盖章，记明有关情况。必要时，可对提取、复制、固定有关电子数据的过程拍照或者录像 |
| 《最高人民法院关于审理证券行政处罚案件证据若干问题的座谈会纪要》（2011年6月23日） | 二、关于电子数据证据<br>会议认为，证券交易和信息传递电子化、网络化、无线化等特点决定电子交易信息、网络IP地址、通信记录、电子邮件等电子数据证据在证券行政案件中至关重要。但由于电子数据证据具有载体多样，复制简单、容易被删改和伪造等特点，对电子数据证据的证据形式要求和审核认定应较其他证据方法更为严格。根据行政诉讼法第三十一条第一款第（三）项的规定，《最高人民法院关于行政诉讼证据若干问题的规定》第十二条、第六十四条的规定，当事人可以向人民法院提供电子数据证据证明待证事实，相关电子数据证据应当符合下列要求<br>（一）无法提取电子数据原始载体或者提取确有困难的，可以提供电子数据复制件，但必须附有不能或者难以提取原始载体的原因、复制过程以及原始载体存放地点或者电子数据网络地址的说明，并由复制件制作人和原始电子数据持有人签名或者盖章，或者以公证等其他有效形式证明电子数据与原始载体的一致性和完整性<br>（二）收集电子数据应当依法制作笔录，详细记载取证的参与人员、技术方法、步骤和过程，记录收集对象的事项名称、内容、规格、类别以及时间、地点等，或者将收集电子数据的过程拍照或录像<br>（三）收集的电子数据应当使用光盘或者其他数字存储介质备份。监管机构为取证人时，应当妥善保存至少一份封存状态的电子数据备份件，并随案移送，以备法庭质证和认证使用<br>（四）提供通过技术手段恢复或者破解的与案件有关的光盘或者其他数字存储介质、电子设备中被删除的数据、隐藏或者加密的电子数据，必须附有恢复或破解对象、过程、方法和结果的专业说明。对方当事人对该专业说明持异议，并且有证据表明上述方式获取的电子数据存在篡改、剪裁、删除和添加等不真实情况的，可以向人民法院申请鉴定，人民法院应予准许 |

由于目前国内针对电子数据取证方面的标准和规范尚不健全，所以，本章节的描述主要从技术以及操作实务上进行探讨，具体法律法规和操作程序不做讨论，仅供广大读者参考。

## 3.2 手机取证流程与规范概述

### 3.2.1 手机取证的基本流程

在实际现场取证过程中，针对不同的案件或是调查需要，以及从传统证据和其他电子证据的调查因素考虑，手机取证调查应遵循的流程也不尽相同，本节的主要目的是提出一个通用的流程模型，具体应遵循的流程可以结合实际调查情况进行。

在现场进行电子数据取证时（包含手机取证），一般情况下可能会涉及不同身份的人员，如表 3-2 所示。

**表 3-2　电子数据取证现场调查角色表**

| 角　　色 | 职 责 描 述 |
| --- | --- |
| 现场处置人员/应急响应人员 | 现场处置人员应在第一时间到达调查现场，现场处置人员应当接受过专业训练，了解如何在现场快速、准确地识别电子证据，并具备基本的电子证据保护、固定知识，负责和现场其他执法人员沟通和协调关于电子证据的事宜。根据现场情况进行电子数据取证评估，并根据评估结果为决策者提供建议，决定后期是否需要电子数据取证专业人员支持<br>在手机取证调查中，担任这个角色的人员应当在第一时间到达现场，快速判断现场是否有涉及需要进行手机取证调查的证据介质，并根据案件情况协助其他调查人员进行手机应急供电、无线信号屏蔽等必要措施，并及时向案件负责人报告案件中涉及的手机证据情况 |
| 调查员/调查主管 | 调查员或调查主管，根据现场处置人员提供的信息和建议，判断是否需要进行进一步取证调查分析，调查主管还负责制订调查计划，包括如何在现场进行证据固定，将哪些证据带回实验室进行后期分析，该案件主要的分析方向，组织哪些专业技术人员参与调查分析；根据调查进展将调查情况及时向上级领导汇报；最后，根据实际调查情况组织撰写并形成电子数据取证/手机取证调查报告<br>在手机取证调查中，调查主管是整个案件中手机取证的负责人，主要责任是根据现场处置人员和技术人员的建议，判断如何开展和进行手机取证调查，并确定手机取证调查的方向和进度，并将手机取证工作的进展和结果向直属上司进行汇报 |
| 技术人员 | 实际参与电子数据取证/手机取证调查的人员，根据调查员/调查主管的决策在现场进行电子证据/手机证据的识别和收集，并进行现场的处置和调查分析。技术人员接受过专业的培训，具有调查经验并能够熟练使用相关的调查工具。在现场调查中，通常需要一名或多名专业技术人员，以便应对不同的调查需求。如在进行现场电子数据取证调查时，需要有专业的计算机调查取证技术人员和手机取证调查人员待命<br>在手机取证调查中，技术人员是具体手机取证调查工作的执行者，技术人员主要负责在现场进行手机证据的必要处置和处理，包括对手机进行现场收集、根据情况进行必要的处置（如无线信号屏蔽），在必要的情况下，还应该在现场使用专用的手机取证工具对手机进行提取和分析。在手机证据被转移至实验室环境后，技术人员还应在取证调查员的指导下进行一些特定的手机取证工作（如镜像制作、多媒体文件提取等） |

续表

| 角　　色 | 职 责 描 述 |
| --- | --- |
| 证据管理人员 | 负责在现场对现场处置人员/应急响应人员以及调查员/调查主管要求提取的电子证据进行收集和固定，与现场技术人员进行协作；同时对所有固定（扣押）的电子证据进行拍照或录像，并按照不同的电子证据类型进行适当的封装和保全处置，登记现场所有电子证据在册，便于后期核对和校验<br>有时，证据管理人员与现场处置人员/应急响应人员两个角色可以由同一人担任<br>在手机取证调查中，证据管理人员应协助和监督现场处置人员/应急响应人员进行手机及其他与手机取证调查相关证据的收集和整理，并对相关证据进行书面和影像记录，其后应采用适当的方法对手机及其相关证据进行封存和固定 |
| 取证调查员 | 主要指在将电子证据固定、保全并带回取证实验室进行后期分析时，进行后期详细调查分析的专业人员，取证调查员接受过完整的计算机取证培训，具备进行调查取证的相关资质或认证，具有长时间的相关电子数据取证经验，能够独立完成多种类型的电子数据取证工作，通常，取证调查员是电子数据取证的专家，能够从专业技术角度为调查主管、技术人员提供案件管理和技术角度的建议<br>在手机取证调查中，取证调查员根据所获得的手机相关证据的情况判定采用何种方式或使用何种工具进行取证分析，并负责主要证据的勘验工作，在一个手机取证调查中可以由多个手机取证调查员进行不同项目的调查分工，或是针对同一项目进行验证 |

一般来说，处理现场的手机证据时，应当按照上述角色的描述进行分工，并按照：现场处置→证据识别→证据固定→证据记录和封存→现场分析→实验室分析→结果校验→出具报告 这样的总体流程进行处理。

在现场对于手机的处理具体操作流程，可以按照图 3-6 中的流程图进行。

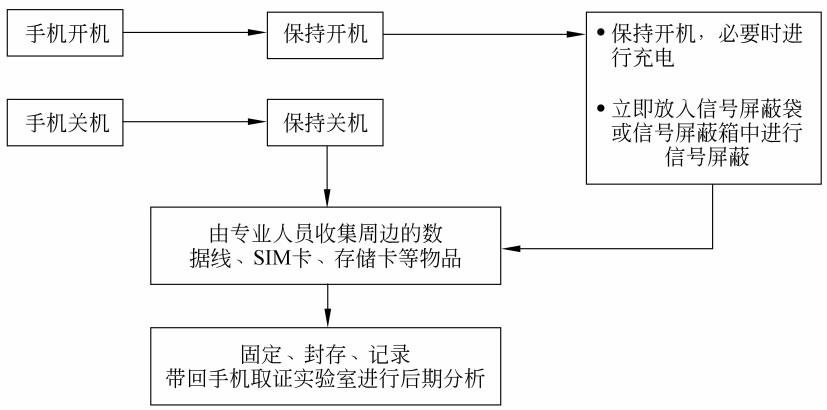



图 3-6　手机等移动通信设备的现场处置流程

**与手机取证相关的周边物品**

- 手机设备本身
- SIM/USIM/UIM 卡模块
- SIM/USIM/UIM 卡板
- 记录着 PIN 码或 PUK 码的运营商服务卡

- 存储卡
- 手机数据线
- 手机充电线缆
- 手机充电适配器
- 手机包装盒、说明书及保修卡
- 可能与手机进行过同步的计算机(台式机、平板电脑及笔记本计算机)
- 手机附近记载着数字或账户信息的即时贴、纸片等
- 其他

注意：在任何电子数据的取证行为中，调查人员的人身安全都是最重要的，在保证人身安全的同时，应尽可能地对所做的所有操作进行记录(包括但不限于文字、照片和视频等方式)。

### 3.2.2　手机取证的规范和原则

手机取证和其他所有电子数据取证一样，面对的都是电子证据，电子证据最大的特征是易失性，即证据很容易被损坏或改变，相对于计算机硬盘，手机取证调查的主要对象——手机，在这一点上表现得更为明显。在调查现场，如果手机长时间放置导致低电量自动关机，那么手机中存储的数据就很可能会丢失；如果盲目将处于开机状态的手机关机，或者直接取出 SIM 卡等存储介质，手机中的通话记录等重要信息也有可能丢失；如果长时间将手机开机放置，新进短信和来电有可能替换或者覆盖掉之前的信息，也会导致证据的丢失。所以，如何在现场适当地处置手机及手机取证相关的物品，除了需要手机取证调查人员根据自身的工作经验进行判断外，还应当严格遵守一系列的取证规范和取证原则。

在计算机取证中，英国高级警官协会 ACPO Good Practice Guide for Computer based Electronic Evidence(计算机及电子证据指导原则)是最为权威的、认可度最为广泛的电子数据取证准则之一，这个原则包含了 4 点，此处，我们结合手机取证调查对这 4 点原则进行逐一细化解释。

ACPO 计算机及电子证据指导原则如下。

#### 1. 不损害原则

在手机取证中，不损害原则是最基本的原则，此处的“损害”可以从两个层面理解：首先是针对设备本身的物理介质不能进行损坏，例如，针对获取的手机等电子设备应当采用防水防尘和防静电的介质进行包装，并轻取轻放；其次，是针对设备中的数据，同样也需要做到不损害，如要绝对禁止盲目对手机进行开关机操作、盲目直接操作手机，针对无法即时取证的手机应当根据情况采取应急充电或信号屏蔽等措施。

#### 2. 避免使用原始证据原则

在计算机取证中，按照此原则，调查人员应当主要采用证据硬盘的副本盘进行调查，而手机取证的特性决定了手机的内存较难进行位对位的完整复制操作。在技术条件允许的情况下，调查人员应当对手机内存制作镜像，并主要对手机内存镜像进行分析；针对

SIM/USIM/UIM 卡和手机存储卡，都应当先制作副本，再对副本进行取证分析。

### 3. 记录所做操作

记录所做的操作，是包括手机取证调查在内的任何电子数据取证工作的硬性要求，由于电子数据的更改不可逆转，所以，从现场识别和固定证据开始，到针对手机进行实验室取证分析的全过程，都需要对所做操作和流程进行记录，这种记录一般可以采用文字记录，或使用数码相机、数码摄像机进行拍摄。对取证流程的完整记录能够确保取证结果的可重现性，从而提高手机取证调查结果的可信度。

### 4. 遵循相关的法律法规

由于目前我国法律中针对电子证据的规定尚属空白，在法定的证据类型中也尚未明确将电子证据纳入其中，所以，在进行手机取证的调查工作时，取证调查人员除了遵循上述的手机取证调查流程和原则之外，还应尽可能遵循其他传统取证调查的规范和规定。

在手机取证的实际操作过程中，有时很难完全保证遵守上述 4 条原则，比如，从理论上讲，将关闭的手机打开，即使有电磁屏蔽环境隔绝手机与移动通信网络连接，手机中的数据也会发生改变，这种改变目前是无法避免的，手机取证调查人员应当在保持对证据产生最小改变的情况下从手机中提取数据。

## 3.2.3 手机取证中电子证据和传统证据并存的探讨

手机取证调查很多时候并不是独立进行的，尤其是针对政府执法部门的手机取证调查人员，他们面对的往往不是单一的需要进行电子物证的提取，而是同时伴随着许多传统证据的综合调查，让我们来看一个例子。

**传统物证还是电子证据的两难选择**

张三，是一个工作在某执法机关取证一线的执法人员，他的职责是在刑事案件的现场尽可能地提取与案件有关的电子证据。某天，在一个凶杀案的犯罪现场，张三和刑事技术人员李四发现了一部沾有血迹的手机，大量血迹分布在手机屏幕和键盘上，在手机背面隐约可见一些带有灰尘的指纹，这让张三和李四犯了难：如果先由刑事技术人员李四进行血迹和指纹提取，张三担心他所使用的方法可能会损坏手机硬件，这样提取过后可能不利于张三再进行手机数据的提取；而如果先由手机取证调查员张三提取电子证据，那么他需要先抹掉血迹和灰尘，才能够看清键盘屏幕并接入数据线进行提取，这样就会把血迹和指纹破坏掉。

究竟该怎样取证才能保证尽可能多地提取到证据呢？

像这个例子中张三和李四所遇到的情况，在执法部门的取证工作中经常会遇到，这个问题也是很多工作在政府执法部门的调查人员长期以来一直关注的一个热点，那么，究竟应该怎样处理传统证据和电子证据之间的冲突问题呢？

这个问题应该说没有一个固定的答案，在不同的调查环境和背景下，电子数据取证调查人员应当和刑事技术人员根据实际调查的案件情况，合理分析所需开展的调查项目及

其可能造成的影响，并进行评估，尽可能地优化取证流程。如在上面的案例中，张三和李四应该根据证据的实际情况进行评估分析，比如，需要提取物证的手机后壳为光滑平面，提取目的是血指纹和汗指纹，那么，刑事技术人员李四有可能采用茚三酮或四甲基联苯胺进行化学处理，相对于某些包含金属粉末的指纹粉（如铝粉），简单的表面化学处理法一般不会影响电子设备的正常使用，那么，可以由李四先进行指纹和血迹的提取。正常情况下，对于处于关闭状态的手机，只要不进行手机开机操作和拆卸电池操作，简单的外壳处理不会影响内部数据的存储，所以，在李四进行完指纹、血迹的提取后，张三可以继续进行手机证据的提取。

当然，上面只是一个简单的例子，笔者也并非专业刑事技术人员，在真正的调查环境中，情况可能远比此复杂，本节中这个例子只做抛砖引玉，目的是提请电子数据取证调查人员注意，在一些情况下，电子证据和传统证据并不存在太多冲突，电子数据取证调查人员应适当了解案件中涉及的其他非电子证据的处理方法和影响，在遇到此类冲突时积极与其他调查人员沟通协调，以期尽可能多地提取、尽可能少地破坏证据，更好地满足调查需求。

在 ACPO 的 Good Practice Guide for Computer based Electronic Evidence（计算机及电子证据指导原则）中，对于在处理手机证据的其他证据时，也进行了如下描述：在处理（手机）之前，应当考虑到手机上其他类型的证据，如 DNA、指纹、毒品和触媒等，并参考犯罪现场手册按适当的程序进行处理，或征求负责人的意见。①

## 3.3　手机证据的保存

在所有电子数据取证工作中，证据的保存是一切取证工作的前提，证据保存需要在不改变电子证据原始状态和内容的情况下，根据电子证据载体的特性妥善地保管。

通常情况下，手机证据的保存可以分为查找、识别、记录和收集几个步骤。

### 1. 查找

查找证据，就是在现场取证时，需要细致准确地查找可能与将要进行的手机取证调查相关的证据，查找证据工作需要取证调查人员具备一定的证据搜索经验，了解和熟悉可能与手机取证相关的物品和材料。如在现场调查时，应仔细搜索手机附近的抽屉、桌面等位置，并主动寻找手机的数据线缆和充电线缆。

### 2. 识别

识别证据，指在查找到可能与手机取证工作存在关系的证物后，需要在现场进行判断，分析和评估其是否可能存在取证价值。如在现场查找到一块手机电池，调查人员需要判断是否属于本次调查所涉及的手机设备。

### 3. 记录

根据手机取证规范，在进行手机取证的全过程中，调查人员都应当对所有操作进行记录。如查找与手机取证相关的证据，需要即时记录证据的外形、形状和状态，并进行拍照

① Good Practice Guide for Computer based Electronic Evidence Verison 3, ACPO, Page 36.

记录；在进行封存时，需要在证据封存袋标记识别文字；在进行手机无线信号屏蔽时，应使用数码摄像机对过程进行拍摄。

#### 4. 收集

在进行手机证据的现场收集时，应当注意同时收集手机的各种附件和周边产品，如手机电池、手机数据线缆和充电线缆、手机充电适配器、SIM/USIM/UIM 卡、手机存储卡、手机包装盒以及手机说明书和保修证书等。

根据美国司法部 Electronic Crime Scene Investigation：A Guide for First Responders，Second Edition（电子犯罪现场调查：现场响应指导原则 第二版）和 ACPO Good Practice Guide for Computer based Electronic Evidence（计算机及电子证据指导原则）对于现场证据保存的指导原则，对于现场手机证据保存的描述，应当注意以下几点。

- 处于开机状态的手机不能进行关机操作，关机将可能导致数据丢失。
- 处于关机状态的手机不能进行开机操作，也不能从手机中移除电池、SIM/USIM/UIM 卡或手机存储卡。
- 处于开机状态的手机，在现场识别后应立即进行无线信号屏蔽。
  - 对于移动通信信号的屏蔽，可采用手机信号屏蔽袋、手机信号屏蔽箱或手机信号干扰器[①]进行，目的是防止手机与网络连接产生数据变化。
  - 在一些情况下，还需要关闭手机的 WLAN 无线网络功能或进行 WLAN 信号屏蔽，这样可以有效防止手机通过无线网络被远程控制进行数据擦除等操作。
- 对处于开机状态的手机，应当采取适当的方法查看其电池电量，并根据需要进行应急充电。
  - 查看手机电池电量应采取适当的方法，如手机处于锁定状态，可以轻击手机键盘上除通话、挂断和电源之外的其他按键点亮屏幕。
  - 对手机进行应急充电，应首先确认手机型号、充电接口类型、充电电压和充电电流，应尽可能使用该手机附带的充电器进行充电，充电时仍需保持相应的无线电隔离或屏蔽。
- 如遇到带有密码保护屏幕锁定的手机，取证人员应避免尝试输入密码，以防止由于超过密码错误次数导致数据被抹除。
- 在对手机证据进行包装时，应采用防潮、防尘、防静电的专用物证袋，做好标记和记录后放入稳固的包装箱/包装袋中，并注意轻取轻放。

## 3.4 手机证据的获取

在完成手机证据的初步检查和保存工作后，手机取证调查人员应根据调查工作的实际情况，决定如何开展对于手机证据的获取。通常情况下，手机证据的获取由现场环境和取证条件决定，一般可以分为：介质复制和镜像、可视化获取、逻辑导出和物理获取（物理

① 在国内，使用手机信号干扰器等无线发射设备需要经过无线电管理等部门许可，未经允许私自使用手机信号干扰器是违法行为。

转储)。

### 3.4.1　介质复制和镜像

介质复制是手机取证调查中应当优先进行的操作,主要目标是针对确认处于关闭状态(证据保存时已处于关机状态)的手机或移动通信设备的可拆卸存储设备和用户识别模块,如手机中所使用的 SD/MMC/MS/TF 等存储卡,和 SIM/USIM/UIM 用户识别卡,这两类设备由于其状态稳定,且标准化程度高,一般可以使用读写设备进行读写操作。

对于手机中插入的存储卡,在进行获取工作前,手机取证调查人员应当做好以下准备,见表 3-3。

**表 3-3　手机存储卡获取前的准备工作**

| 步骤 | 准 备 工 作 |
|---|---|
| ① | 确认手机处于关闭状态,并将手机置于带有无线电信号屏蔽的环境中。同时,手机取证调查人员应根据需要采用适当的静电保护措施,如放静电手套和放静电手环等 |
| ② | 根据调查需要和取证条件,选择适当的获取方式 |
| ③ | 取出手机中的存储卡,此过程中,如取出存储卡需要拆卸手机电池,则手机电池移除后不能立即装回手机,以防其自动开机。同时,如手机具有 SIM/USIM/UIM 等可拆卸用户卡,也应一并取出 |
| ④ | 根据选定的获取方式进行获取 |
| ⑤ | 获取完毕后及时将存储卡安装回手机,如需装回电池,需首先将手机存储卡和 SIM/USIM/UIM 等用户卡装回后再进行电池安装 |

手机取证调查人员可以采用以下方式进行手机存储卡的获取。

- 专用存储卡复制设备

目前,一些手机取证产品制造商推出了专门用于存储卡取证的设备,如美亚柏科公司 DC-800 存储卡获取设备可以将存储卡获取为 DD 镜像。


图 3-7　只读读卡器

- 电子数据取证软件和镜像软件

首先,应当使用具有写入保护的专用取证只读存储卡(见图 3-7)读卡器,待接入存储卡后,使用 EnCase(或 EnCase Imager)、FTK Imager 等软件将该存储卡直接获取为 E01 或 DD 等格式的证据镜像文件。

一般情况下,不推荐采用将存储卡复制为存储卡的方式(某些带有 USB 源和目标接口的复制设备可以实现),因为使用镜像方式更易于保存并且能够确保证数据不被损坏。

而对于手机中插入的 SIM/USIM/UIM 等用户身份识别卡,在具备条件的情况下,也应单独取出进行复制或直接检查,准备工作如表 3-4 所示。

表 3-4　SIM/USIM/UIM 卡获取前准备工作

| 步骤 | 准 备 工 作 |
| --- | --- |
| ① | 确认手机处于关闭状态，并将手机置于带有无线电信号屏蔽的环境中。同时，手机取证调查人员应根据需要采用适当的静电保护措施，如放静电手套和放静电手环等 |
| ② | 根据调查需要和取证条件，判断手机所使用的网络制式和 UICC 芯片卡类型 |
| ③ | 取出手机中的 SIM/USIM/UIM 卡，此过程中，如需要拆卸手机电池，则手机电池移除后不能立即装回手机，以防其自动开机。同时，如手机具有可拆卸的存储卡，也应一并取出 |
| ④ | 根据选定的获取方式进行复制或直接检查 |
| ⑤ | 获取完毕后及时将存储卡安装回手机，如需装回电池，需首先将手机存储卡和 SIM/USIM/UIM 等用户卡装回后再进行电池安装。如需要使用复制卡开启手机，则应保管好原始卡片，在复制卡装入手机开机时必须保证具有无线电信号屏蔽环境 |

手机取证调查人员一般采用专用的手机取证软件或工具进行手机 SIM/USIM/UIM 用户身份卡的获取或直接检查分析。

关于如何进行手机 SIM/USIM/UIM 卡的复制和直接检查分析，请参见本书第 4 章“SIM/USIM/UIM 卡和可移动介质取证”。

### 3.4.2　拍照获取

在本书的第 1 章中，对于手机的可视化取证已经进行了简要的介绍，并且列出了市场上常见的手机可视化取证设备。

在手机取证调查实际中，手机的可视化获取一般针对不具备数据接口或现有手机取证设备不支持的手机，在这种情况下，可视化获取是唯一能够对手机上的证据进行固定和检查的手段，所以，手机证据的可视化获取一般也可称为手机证据的可视化取证。

手机证据的可视化取证由于需要调查人员完全手工进行，往往需要消耗较长时间，这就要求在进行可视化获取之前，手机取证调查人员应做好一些充分的准备，这些准备主要包括如表 3-5 所示。

表 3-5　手机证据可视化取证前的准备工作

| 步骤 | 准 备 工 作 |
| --- | --- |
| ① | 确保取证环境具有可靠的无线电信号屏蔽设备 |
| ② | 确定手机所使用的充电接口，并准备相应的备用电源和充电适配器 |
| ③ | 确保符合所遵循的标准和规范要求，如相应的证据登记表单、指定数量的监督/见证人员 |
| ④ | 良好的光线环境，预先调试可视化取证设备，进行测试并查看样张 |
| ⑤ | 单色低对比背景的防滑垫、证据尺、参照物、证据标签 |

手机证据可视化取证的具体操作方式依手机取证调查人员选用取证工具的不同而不同，如采用 Fernico ZRT 系列设备，取证调查人员应在软件中输入正确的案件信息和编号；如采用 Project-A-Phone 系列设备，调查人员应当确认保存图片或视频的文件夹，并尤其需要注意在取证开始之前测试设备的对焦是否准确清晰。图 3-8 为可视化取证拍摄

的手机版本信息。


图 3-8　可视化取证拍摄的手机版本信息

在进行手机可视化取证时，除了对需要提取的如短信、通话历史记录、通讯录等信息进行拍摄或录像外，还应注意不要遗漏对于手机身份显示信息的拍摄和固定，在具备条件的手机上，应当调出手机相应的信息显示页面，这些页面包括手机 IMEI 号码、插入卡 IMSI/ICCID 号码、手机型号、手机序列号等，比如在采用 NOKIA S30、S40 和 Symbian S60 操作系统的诺基亚手机上，调查人员可以输入 * ＃0000＃和 * ＃92702689＃查询手机信息。

在实际的手机可视化取证案例中，使用 Paraben Project-A Phone ICD 系列可视化取证产品的手机取证调查人员可能会发现，在启用计算机软件后，可能会出现无法识别拍摄摄像头的情况，此时，调查人员应当确认取证计算机自带的摄像头或已接入的摄像头被禁用，或在菜单中指定设备自带的摄像设备。

以下提供了一些使用 Fernico ZRT 设备进行手机取证的实际调查图片，如图 3-9～图 3-14 所示。


图 3-9　对于手机外形、电池、SIM 卡的可视化取证，在进行可视化取证时，应使用标准的证据测量尺并在拍摄时一并摄入，必要时还可采用硬币等标准大小物品进行比对

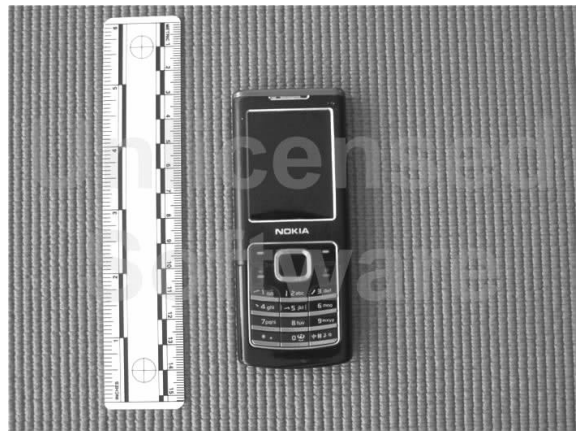



图 3-10　可视化取证之手机正面外观


图 3-11　可视化取证之手机背面外观

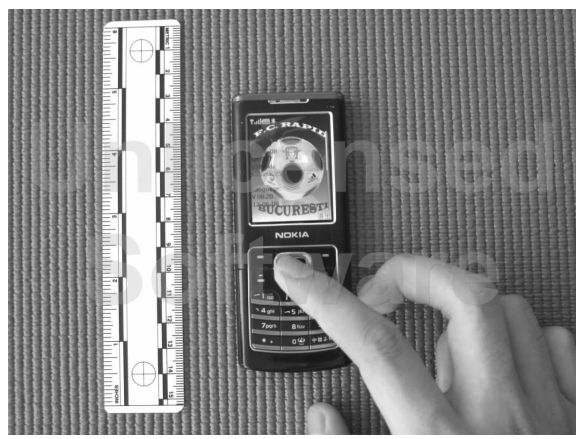



图 3-12　开机状态下的可视化取证

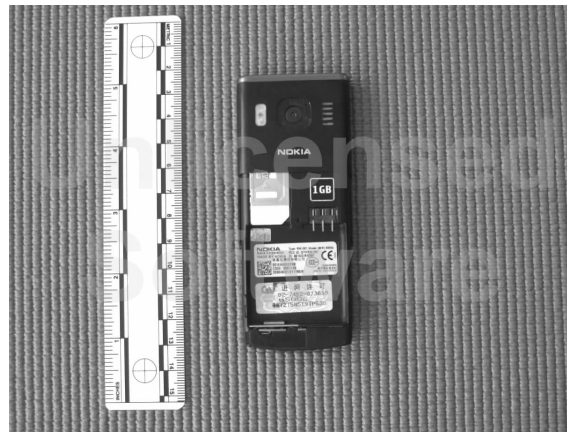



图 3-13　关机状态下的可视化取证——手机标签和信息

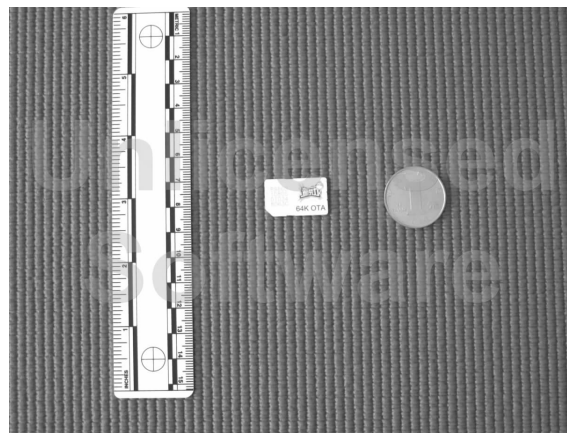



图 3-14　可视化取证——手机 SIM 卡

### 3.4.3　逻辑获取

面对大部分具有数据接口、蓝牙或红外模块，且具备计算机通信协议的手机，一般都应采用逻辑导出的方式进行证据获取，逻辑导出相对于可视化取证来说，能够完整获取大部分数据并且可以进行后期分析、搜索等操作；目前市场上大多数的手机取证软件所进行的取证工作，都属于本节所提到的逻辑导出范畴。

目前针对大多数智能手机来说，逻辑导出主要有两种情况：一是利用手机自身的厂商通信协议，直接从手机中将短信、通话记录和联系人等信息导出；另一种是在通信协议无法完整获取数据的情况下，使用专用的客户端（或称 Agent 程序）上传至手机进行数据获取。

采用厂商通信协议的手机大部分是智能手机，如 Windows Mobile 操作系统的智能手机，微软提供了 ActiveSync（Windows XP）和 Windows 移动设备中心（Windows Vista/Windows 7），用户可以直接使用这些程序对 Windows Mobile 手机中的短信、联系人等项

目进行管理;诺基亚公司为采用 Symbian 操作系统的手机提供了 PC Suite(PC 套件)或 Ovi Suite,这两款程序能够管理 Symbian 手机中的短信、联系人等信息,并可以进行应用程序管理。

使用厂商通信协议具有显而易见的优势——对制造商手机的兼容性较好,所以,大部分手机取证软件对于品牌智能手机都主要采用厂商通信协议的原理进行提取。

对于手机中证据的逻辑导出,一般情况下指的就是使用手机取证软件对手机证据进行提取的过程,在手机取证调查工作中,比较常用的进行手机证据逻辑导出的取证工具主要有 Oxygen Forensic Suite、Device Seizure、Cellebrite UFED、Logicube CellDEK、美亚柏科 DC-4500、上海盘石 SafeMobile 等,关于如何使用上述的这些软件进行手机证据的逻辑导出,读者可参见本书第 7 章“常见手机取证工具”。

在进行手机证据的逻辑导出过程中,调查人员可能面临以下一些问题(见表 3-6),作者在此单独进行分析解答。

**表 3-6 手机证据逻辑导出 Q&A**

| Q | A |
|---|---|
| Windows Mobile 手机使用 USB 数据线连接取证计算机后,取证软件无法获取任何数据 | 大部分手机取证软件对于 Windows Mobile 操作系统手机的提取使用 ActiveSync 方式进行,调查员应确定手机和计算机建立了同步关系(Windows Mobile 手机默认顶部显示双向箭头),如无法建立同步关系,可通过禁用“高级网络”方式排除故障 |
| 诺基亚 Symbian 手机使用 USB 数据线连接取证计算机后,取证软件无法获取任何数据 | 大部分手机取证软件对于 Symbian 操作系统的提取是基于 PC Suite 进行(直接获取或上传程序)的,调查员应确定手机在连接计算机后选择相应的连接方式(如 PC Suite),如需上传提取程序,则同时应保证手机时间的设置准确无误,以避免出现证书失效 |
| 某品牌 Android 手机使用 USB 数据线连接取证计算机后,取证软件无法获取任何数据 | 由于采用 Android 操作系统的手机制造商较多,部分制造商使用了自行定义的同步程序,所以应首先确定该手机接入后计算机能够识别手机品牌及型号,然后才可继续进行取证工具的获取。同时,需要注意的是,Android 手机在进行一般逻辑获取时需要开启“调试模式”,在调试模式开启后,adb 才能正常连接 |
| 一台苹果 iPhone 手机,使用 USB 数据线连接取证计算机后,取证软件基本获取不到有价值的数据 | 如使用的取证软件通过通信协议方式获取,则一般情况下,未进行“越狱”的手机将可能无法获取正常的逻辑数据,而已经“越狱”取得权限的手机可以正常获取 |

手机证据的逻辑导出一般都由计算机上的手机取证软件或专用的手机取证设备进行,手机取证调查人员无须进行过多干预,所以提取方法和提取过程需要注意的主要在于如何防止出现手机证据损坏和丢失,逻辑导出过程中手机通常都处于开机状态,此时必须保证具有足够的电源供应和备用电源/充电器,并且必须具备可靠有效的无线电信号屏蔽措施。

在手机逻辑证据导出结束后,应及时将手机恢复至原始状态。

### 3.4.4 物理获取

可以用这样一个比喻来形容手机证据的逻辑导出和物理获取之间的关系:逻辑导

出，如同在计算机中打开磁盘，全部选择之后进行复制，而物理获取，某种程度上可以认为是对完整硬盘的复制，获取的内容如图 3-15 所示。

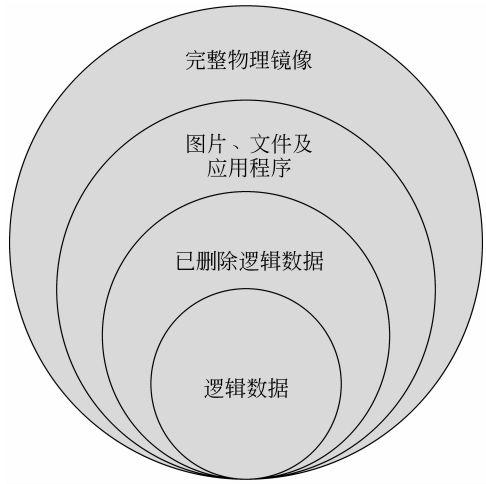



图 3-15　手机证据物理获取的内容

如同计算机取证中，调查人员可以方便地使用复制设备对硬盘进行复制一样，手机取证调查人员也希望能够完整地获取手机中的数据——当然不仅是目前存在的（即“逻辑数据”），还包括已经被删除的数据，而被删除的数据大多数具有更大的取证意义和价值。

但是，手机和计算机存储结构和原理的不同，决定了手机中存储的数据并不像计算机一样容易完整获取，手机中的存储往往会受多种文件系统、多种物理存储结构、不完全开放的接口等因素的制约；目前，针对 iOS 操作系统、Android 操作系统、部分 Symbian 操作系统以及一些非智能手机操作系统（如 MTK），一些手机取证设备制造商已经提供了解决方案，手机取证调查人员可根据调查实际选择适合的工具进行获取。

# 第4章 SIM/USIM/UIM卡和可移动介质取证

很多人认为，手机卡是手机取证调查的基本项目。那么，手机取证中涉及的手机卡分别有哪些类型呢？这些类型的卡分别具有什么特点，该如何对这些手机卡进行取证呢？通过本章的学习，读者将从中得到上述问题的解答。

移动电话的种类多种多样，但是，移动电话取证调查中，有一项调查是基本一致、同时也是必不可少的，这就是用户身份识别卡的调查和分析。

在手机取证调查分析中，用户身份识别卡的取证调查一般作为介质调查的第一个项目，手机取证调查人员往往会先对手机等移动通信设备中的SIM卡、USIM卡、UIM卡等身份模块单独进行调查，并根据需要进行卡复制、卡数据恢复等操作。在本章中，将主要针对SIM/USIM/UIM等用户身份识别卡的基本知识、取证项目、取证方法和工具进行简要介绍。

## 4.1 SIM/USIM/UIM卡简介

在本章的介绍中我们所称的“用户身份识别卡”可以看作一种统称，实际上，所有移动通信终端接入移动通信网络都会用到各种用户识别模块，而这些身份识别模块通常都以UICC[①]的形式存在，所以，不论是GSM、WCDMA还是CDMA网络所使用的用户识别卡，它们的外形看起来都是一致的（除了MicroSIM[②]、NanoSIM[③]等特殊设计卡片），但在不同制式的移动通信网络中，用户识别模块名称也不尽相同，下面将分别介绍。

### 4.1.1 SIM卡

在GSM网络中，用户识别码就是我们常说的SIM卡，这是目前最为常见的一种卡片类型，目前全球各国GSM网络中所使用的基本都是SIM卡，目前中国移动通信（以下简称“中国移动”）和中国联合网络通信（以下简称“中国联通”）的GSM网络均采用SIM卡作为用户身份识别模块。

SIM卡全称为Subscriber Identity Module，意为“用户识别模块”，如图4-1所示。SIM

① UICC：Universal Integrated Circuit Card，通用集成电路卡，就是通常所说的IC卡，UICC广泛用于移动通信用户身份模块、电子钱包、金融卡（银行卡）、安防系统身份卡等多个领域。

② MicroSIM：一种特殊设计的SIM卡，外形比传统SIM卡小，在本章的后部分具体介绍。

③ NanoSIM：一种特殊设计的SIM卡，主要用于iPhone 5等较新的手机中。