

# 《电子证据调查学》教学大纲

杜春鹏 编写

## 目 录

目 录.....	1368
前 言.....	1371
一、开设电子证据调查学的背景.....	1371
二、电子证据调查学学科特色.....	1371
三、存在的问题.....	1371
四、本学习课程希望达到的目标.....	1371
推荐书目.....	1371
第一章 电子证据概述.....	1373
第一节 电子证据的概念.....	1373
一、电子证据的概念.....	1373
第二节 电子证据及其相近概念.....	1374
一、电子证据和一些相关联概念的辨析.....	1374
第三节 电子证据的特征.....	1374
一、存储方式上和传统证据形式有异.....	1374
二、传播的方式上，电子证据可以快速的无限的传递.....	1375
三、在感知的方式上的无形性.....	1375
四、数据的脆弱性.....	1375
复习与思考题.....	1375
拓展阅读书目.....	1375
第二章 电子证据的法律定位和学理分类.....	1376
第一节 电子证据的法律定位（一）.....	1376
一、电子证据法律定位的必要性.....	1376
第二节 电子证据的法律定位（二）.....	1376
第三节 电子证据的法律定位（三）.....	1377
第四节 对电子证据的法律定位的正确看法.....	1378
一、以上各种说法的意义.....	1378
二、对电子证据法律定位综合的看法.....	1378
第五节 电子证据的学理分类（一）.....	1379
一、对电子证据进行分类的必要性.....	1379
第六节 电子证据的学理分类（二）.....	1379
第七节 电子证据的学理分类（三）.....	1380
第八节 电子证据法和对研究的意义.....	1381
一、国内外电子证据立法现状.....	1381
二、电子证据法研究的意义.....	1381
复习与思考题.....	1381
拓展阅读书目.....	1382
第三章 电子证据的收集.....	1383
第一节 取证主体（一）.....	1383
一、电子技术专家.....	1383
第二节 取证主体（二）.....	1383

二、网络警察.....	1383
第三节 取证的方法和步骤（一）.....	1384
一、电子证据取证的思想方针.....	1384
二、电子证据取证的特殊性.....	1384
三、电子证据取证的事前态度.....	1384
四、电子证据取证的基本的思想方法.....	1385
第四节 取证的方法和步骤（二）.....	1385
一、基本的方法（AAA 法，取证的框架）.....	1385
第五节 取证的方法和步骤（三）.....	1386
复习与思考题.....	1386
拓展阅读书目.....	1386
第四章 电子证据收集现场的操作.....	1387
第一节 电子证据收集的现场及相关工作（一）.....	1387
一、电子证据的现场.....	1387
二、预先评估现场.....	1387
三、建立调查队.....	1387
第二节 电子证据收集的现场及相关工作（二）.....	1388
四、建立攻击计划.....	1388
五、执行搜查.....	1388
第三节 不同类型电子证据现场勘查的工作要求.....	1389
一、单机现场.....	1389
二、网络现场.....	1389
复习与思考题.....	1389
拓展阅读书目.....	1389
第五章 电子证据的保全.....	1390
第一节 常规保全.....	1390
一、电子证据保全的重要性.....	1390
二、电子证据的常规保全方法.....	1390
第二节 公证保全.....	1390
一、电子证据公证保全的优越性和难点.....	1390
二、电子证据公证保全的方法.....	1391
复习与思考题.....	1391
拓展阅读书目.....	1391
第六章 网络基础知识.....	1392
第一节 OSI 网络模型简介.....	1392
一、OSI 参考模型（Open Systems Interconnection reference model）.....	1392
二、OSI 参考模型的具体分类.....	1392
第二节 计算机网络协议.....	1393
一、网络协议.....	1393
二、网络协议的种类.....	1393
三、TCP/IP 协议.....	1393
第三节 计算机网络协议分层的实现.....	1393
一、网络协议分层的实现——封装.....	1393

复习与思考题.....	1394
拓展阅读书目.....	1394
第七章 硬盘驱动器和存储介质基础.....	1395
第一节 什么是硬盘.....	1395
一、硬盘的逻辑结构.....	1395
第二节 操作系统.....	1395
一、操作系统通过设备的驱动程序来访问硬件.....	1395
二、任何操作系统都为存储设备提供基本输入 / 输出 (I/O) 接口.....	1395
三、文件系统.....	1396
第三节 磁盘数据的存储.....	1396
一、未分配空间.....	1396
二、不能真正删除硬盘上的数据.....	1397
第四节 国内外当前硬盘取证设备简介.....	1397
一、硬盘取证设备的要求.....	1397
二、目前国内外市场的主流设备.....	1397
三、手持式硬盘取证设备.....	1397
四、取证勘查箱.....	1397
第五节 代表性取证专业软件简介.....	1398
一、Encase.....	1398
二、FTK.....	1398
三、ForensicX.....	1398
四、TCT.....	1398
复习与思考题.....	1398
拓展阅读书目.....	1398
第八章 电子证据取证相关技术概要及发展目标.....	1399
一、数据获取技术.....	1399
二、数据分析技术.....	1399
三、电子证据取证的发展目标.....	1399

# 前 言

## 一、开设电子证据调查学的背景

(一) 大背景：从证据发展的角度上说，我们已经进入电子证据的时代，无论针对网络的犯罪还是利用网络为工具实施的传统犯罪已广泛存在。(既可以是传统犯罪的新形式，又在很大程度上增添了传统犯罪所不能够涵盖的内容)

发生在电子和数字领域中，特别是在电脑空间的新型犯罪方式变得越来越普遍。全世界的刑事司法机构正面临着越来越多的部分或全部通过 Internet 以及其他电子媒介实施犯罪的案例。

(二) 小背景：目前全国高校中开设“电子证据调查学”课程的几乎没有第二家。

1. 利：一定程度上而言是开先河之举，该学科发展前景广阔，具有深厚的社会现实和学科发展的需求。对该学科早接触、早入手能够占有一定的先机。

2. 弊：现实的学习条件相对较弱，没有现成的教材或者可以适合用来做教材的书。学科体系还没有很成型。若想在此学科上有所建树需要付出更多的努力。

## 二、电子证据调查学学科特色

(一) 由名称入手，电子证据、证据调查。(交集，兼顾一般、照顾特殊)

(二) 既有法律问题又有技术问题。电子证据的概念、特点、类别、法律地位、证据价值、电子证据各环节的规则性、程序性的要点。技术性问题与常规上的理解有不同，主要是层次上的。(二者兼有，同等重要)

(三) 本身属于应用性的学科，涉及的知识范围广，很多时候需要对其它学科的知识采取“拿来主义”。

## 三、存在的问题

(一) 信息技术的发展日新月异，尤其是对于一些具体问题的解决方案，今天适用，明天就有可能改变。对我们来说要抓基本方面。

(二) 关于电子证据的说法各不相同(谁说的都对)，这是阶段性的问题。只是采用一家之言，吸取并剖析。

(三) 总的来说，是新兴的学科门类，处于发展初期，复合型，前景看好。一个学习过程，更是一个探索过程。一定存在较多问题，要求：共同参与，完善课程和自己的知识结构。(考虑作为平时成绩)

## 四、本学习课程希望达到的目标

开拓视野，为大家打开新学科的一幅画卷。以识记为主，兼顾理解和应用。

具体包括：电子证据的概念，特点，法律属性，证据价值…

电子证据调查的基本程序和专门性要求……

计算机和网络的一些基本的底层知识：网络的分层介绍，网络协议的了解，存储器的存储原理，加密和取证的基本知识，一些实用的电子证据调查工具和设备……

## 推荐书目

刘广三：《计算机犯罪论》，人大出版社 99 年版。

何家弘：《电子证据法研究》，法律出版社 02 年版。

张越今：《网络安全与计算机犯罪勘查技术学》，清华大学出版社 03 年版。

公安部教材：《信息网络安全监察》，群众出版社 00 年版。

Alan M.Gahtan: “Electronic Evidence”, by the Thomson Professional Publishing 1999

段海新等译：《计算机取证：应急响应精要》人民邮电出版社 2003 年版。

常晓波译：《应急响应计算机犯罪调查》清华大学出版社 2002 年版。

何家弘：《证据调查实用教程》，人大出版社 00 年版。

Eoghan Casey: “Digital Evidence and Computer Crime”, by Academic Press 2000

有能力的话看国外的书较好，突出操作性。

期刊上我校未买理科的文库，应在工程类杂志上搜索有关文章，或通过一些协会获取内部资料。

## 第一章 电子证据概述

本章教学目的和基本要求：本章主要介绍电子证据的概念性问题，通过对电子证据这样一种新型证据形式的相近名称比较，给出了电子证据的概念。本章的重点在于对电子证据这样的一种新型证据有概念性把握，难点在于电子证据概念中相关要点以及相近概念的比较理解。

学时分配：

### 第一节 电子证据的概念

#### 一、电子证据的概念

科学的界定电子证据的概念是研究电子证据调查等相关问题基本出发点。

##### （一）外译词汇

“Electronic Evidence” 电子证据

“Computer Evidence” 计算机证据

“Digital Evidence” 数字、数码、数位证据

“Computer-based Evidence” 基于计算机的证据

“Computer-produced Evidence” 由计算机形成的证据

“Computer-created Evidence” 由计算机创制的证据

“Computer-generated Evidence” 由计算机生成的证据

“Computer-stored Evidence” 由计算机存储的证据

“Computer-related Evidence” 和计算机相关的证据

“Evidence from Computer Record” 源于计算机记录的证据

##### （二）中文表述

电子证据，计算机证据，计算机数据证据，电子数据证据，数据电文证据，电子文件证据，网络证据等。

叫法不统一、不同的表述间的特定含义并不一致，可能只是倾向于某种特定的方面。

##### （三）着眼点

1. 人们开始从不同的着眼点认识到存在有这样一种证据，而且随社会生活的发展，它所占据的位置还会越来越重要。

2. 各种对“电子证据”（暂时如此叫）的不同叫法总体上能够反映出这样一点：电子证据的出现和发展与电子技术、数字技术的存在和发展有密切的关系。

（四）广义上可以定义电子证据为：“以电子形式存在的，用作证据使用的一切材料及其派生物。”

1. 电子形式：这种物质的存在形式是早已有之（自然界的存在），但真正为人们所认识和应用是从近代的电子技术的诞生开始的。其特点在于我们对此种形式的感知，是需要通过一定的仪器设备并要有一定的技术手段才可以转换为我们可以接受的形式。绝大多数的情况下我们难以直接通过自身的感官来感受之。

电子形式具体指“由介质、磁性物、光学设备、计算机内存及类似设备生成、发送、接收、存储的任一信息的存在形式。”（印度《1999年信息技术法》之规定）

对于实际生活中常遇到的由电子形式材料转化的派生物也将其视为电子证据。（如通过打印机输出的计算机内部存储文件，不同于一般的纸面书证，因为其不具有独立性，是居于派生证据地位

的电子证据。)

2. 电子证据是借助电子技术或电子设备而形成的。电子技术包括但不限于计算机技术, 但随着计算机技术的迅猛发展与广阔应用, 它所占据的份额和地位越发的的重要。电子技术中基于模拟信号的技术同样占有一定位置。

3. 电子证据是作为证据使用的材料。如国外称尚未作为证据使用的材料为“Information”, 提交为证明案情使用后改称之为“Evidence”。同一事物由于用途的变化引起的一定的称谓上的变化。

## 第二节 电子证据及其相近概念

### 一、电子证据和一些相关联概念的辨析

#### (一) 电子证据和计算机证据

1. 计算机证据是以计算机为基础或是和计算机相关联的证据。电子证据和计算机证据二者被认为是一种交叉的关系。

2. 按照常规的理解(现代微电子技术意义上的计算机)应该是包容的关系, 计算机证据包容于电子证据。不太严格的情况下可以将两用语互换使用。

#### (二) 电子证据和数字证据

1. 数字证据一词在在英文法律文献中常有出现。奥恩·凯西 2000 年版《数字证据与计算机犯罪》(Eoghan Casey: “Digital Evidence and Computer Crime”, by Academic Press 2000.)

书中定义“数字证据是指包含有下述各种数字式数据的证据, 即能够证明发生了某一犯罪的数字, 或者能否在犯罪行为与犯罪人、犯罪行为与被害人之间建立某种联系的数据。”

2. 从电子和数字两个词汇上入手, 电子技术包括数字电子技术和模拟电子技术。

3. 故而电子证据的外延大于数字证据, 数字证据从属于电子证据。

#### (三) 电子证据和科学证据 (Scientific Evidence)

1. 对于“科学证据”一词尚无普遍认同之定义。

2. 美国联邦司法中心、康乃尔大学法学院、美国法学院协会的观点:

(1) 美国联邦司法中心 1994 年《科学证据参考指南》将科学证据界定为专家证据、尤其是案件中涉及科学和技术争议的专家证据。(此观点中没有谈及电子证据)

(2) 康乃尔大学法学院的网站把电子证据与科学证据分为两个独立频道。

(3) 美国法学院协会将科学证据与专家证据合并称作是“专家与科学证据”(Expert and Scientific Evidence), 也不包括电子证据。

3. 由此, 电子证据和科学证据属于平行关系。

4. 科学证据主要包含精神病学、心理学证据, 毒物学和化学证据, 及指纹、枪弹、DNA、可疑文书、测谎等。电子证据可由当事人使用普通的方式举证、质证。

## 第三节 电子证据的特征

### 一、存储方式上和传统证据形式有异

需要借助一定的电子介质(主要是光、磁)。由于存储的容量可以很大, 故而电子证据的表现形式可以以多媒体形式出现, 可以为文本、图像、图形、声音、动画的集合体。

## 二、传播的方式上，电子证据可以快速的无限的传递

本质上电子证据是数据（信息），可以通过有线或无线的方式在虚拟的空间飞速传播。而且这种数字式的传播基本上是不失真的，可以方便快速的精确复制。

## 三、在感知的方式上的无形性

电子证据离不开电子设备而且不能脱离特定的系统环境。电子证据大体上可以看作是基于计算机的证据（Computer-based Evidence），传统书证是基于纸面的证据（Paper-based Evidence）。

（一）电子证据是以声、光、电、磁等形式存在于媒体介质之上的，它的实体是电磁波和二进制数据编码。这些信号和编码是肉眼无法直接观看的无形体，只有通过特定的设备和技术才能显示为肉眼可见的有形内容。

（二）显现电子证据必须依赖于专门的电子设备主件和配套的系统软件环境。收集电子证据时，应该保存相应的软硬件，保全电子证据的运行环境，并能在适当的时候可以以打印输出或屏显等方式显示出来。

## 四、数据的脆弱性

1. 对于电子证据来说，不论是数字形式还是模拟形式，由于它是保存在可擦写的记录介质上，如磁带、磁盘、可擦写光盘等等，在其存储、传输和使用过程中，极易遭受到外来的破坏。

2. 不同观点：传统的书证一旦原件受到破坏，无法复原证据；电子记录被删改、复制的痕迹均可以通过技术手段分析认定，硬盘的擦写记录可以跟踪捕捉到，从这个意义上讲电子证据较传统证据具有更强的稳定性和安全性。

### 复习与思考题

1. 电子证据的概念是什么？和相近的一些名称有什么联系和区分。
2. 电子证据的特点是什么？

### 拓展阅读书目

1. 刘广三：《计算机犯罪论》，人大出版社 99 年版。
2. 何家弘：《电子证据法研究》，法律出版社 02 年版。

## 第二章 电子证据的法律定位和学理分类

本章教学目的和基本要求：本章主要介绍电子证据这一新形式的证据在法律上的定位以及如何对其进行合理的学理分类加以了探讨。重点在于如何恰当的对电子证据进行合理定位。难点在于对电子证据中“原件”的理解。

学时分配：

### 第一节 电子证据的法律定位（一）

#### 一、电子证据法律定位的必要性

对电子证据这一新型的证据恰当的进行法律上的定位，关系到解决电子证据问题的大思路。具体应该考虑是否给予电子证据以证据地位以及给予其怎样的证据地位两方面大问题。

我国相关法律规定：“证明案件真实情况的一切事实，都是证据。”面对世界电子化、信息化的潮流，赋予电子数据证据的地位为应当之举。各国立法实践也如此。目前争议的焦点在于给予电子证据怎样的证据地位这一问题之上。

现有关于电子证据法律定位的观点：

（一）视听资料说：早期的看法认为电子证据属于视听资料。

1. 96年最高检在《检察机关贯彻刑诉法若干问题的意见》当中规定：“视听资料是指以图像和声音形式证明案件真实情况的证据。包括与案件事实、犯罪嫌疑人以及犯罪嫌疑人实施反侦查行为有关的录音、录像、照片、胶片、声卡、视盘、电子计算机内存信息资料等。”

2. 有关教材章节设置也如此。

3. 理由：①视听资料是指可视、可听的录音带、录像带之类的资料，电子证据可显示为“可读形式”，因而也是“可视的”；②视听资料与电子证据在存在形式上有相似之处，都是以电磁或其他形式而非文字符号形式存储在非纸质的介质上；③存储的视听资料及电子证据均须借助一定的工具或以一定的手段转化为其他形式后才能被人们直接感知；④两者的正本、副本没有区别（相对）；⑤把电子证据归于视听资料最能反映它的证据价值；等。

4. 反面意见：①视听资料和其他证据相比强调的是以声音、图像而并非文字内容证明案件的真实情况，将电子证据中文字之“可视”和视听资料之“可视”混在一起并不合适。

②从证据的角度来看，视电子证据为视听资料不利于电子证据在诉讼中充分发挥证据的作用。我民法规定对视听资料应结合其他证据查明其真伪才可作为认定事实之依据，这样若某一案件中只有电子证据即使其非常可靠，也难以仅据此来定案。

### 第二节 电子证据的法律定位（二）

（二）书证说：近年来学者借鉴国外的电子商务法律文件的经验，提出了电子证据系书证的观点。

1. 理由：①电子证据和普通书证一样是将其内容记载于一定的介质之上的，无非一种介质是常见的纸张，另一种是光磁的存储介质。记录的方式和介质不同，但能够记录同样的内容。②电子证据通常也是以其所代表的内容来说明案件的某一问题，需要通过输出、屏显等方式才可以被人们看见和利用，具有书证的特点。③1999年《合同法》11条：“书面形式是指合同书、信件及数据电文（包括电报、电传、传真、电子数据交换和电子邮件）等可以有形的表现所在内容的形式”，

所以电子证据系书证的一种。④各国在立法上尝试功能等价法旨在填平传统书证和电子证据的差异。

2. 反面意见：①我国相关法律明确规定，书证需提交原件。若电子证据作为书证的话难以解决法律上要求书证需是原件这一问题。大多数情况下，电子证据是以自动程序生成、传输和交换的，有时候录入人在录入以后销毁了底稿或不用底稿直接录入。这些情况下都难以认定电子证据的原件。（如何认定“原件”是一个问题）②书面形式并不等同于书证，勘验笔录、鉴定结论等都可以是书面形式但不是书证。（证据形式划分标准在于证明机制）③书证说难以圆满地回答计算机声像资料、网络聊天资料的证明机制问题。

（三）物证说：我国有少数人主张物证说。（一些电子证据勘查仪器明确使用这一说法：电子物证）

一些文章中如此说：电子证据在无需鉴定的情形下属于书证，需要鉴别其真伪时可能成为物证；电子证据属于学理上的广义的实物证据。（并非诉讼法所规定的物证）

奥恩·凯西 2000 年版《数字证据与计算机犯罪》：“数字证据是物证的一种。虽然数字证据不像其他形式的物证那样有形，它仍然属于物证。”

1. 理由：①数字证据是由能借助特定工具和技术加以收集并分析的各种磁性物质和电脉冲物质所形成的；（任何信息的表达均是借助于物质的载体）②许多法庭承认此种无形物可以作为证据扣押。

2. 反面意见：理由充分，但仅仅涉及电子证据的一部分（数字式电子证据），又限于刑事司法领域，有一定的局限性。

### 第三节 电子证据的法律定位（三）

（四）鉴定结论说：少数学者所持的看法，是从转换角度所得出的结论。

1. 冯大同《国际货物买卖法》：“法院或当事人对电子数据的可信性有怀疑，可由法院指定专家进行鉴定，辨明真伪，然后由法院确定其能否作为认定事实的根据。”

2. 反面意见：鉴定的目的为了解决案件中某些关系是否存在、某些事实或现象的真伪、某些事实的有无、某些事实的程度及某些事实的因果等。这些需要鉴定的关系、事实或现象等通常应是可采用的证据，只是由鉴定的方式确定其是否可采信。故而只有在电子证据被采用的前提之下才需要专家就其真伪进行分析判断，才需要法院依据鉴定结论确定其是否可以作为认定事实的根据。

（可用作证据—可采用的证据—具体的证明力，层次关系）

（五）独立证据说：代表最新的思潮。

1. 任何传统的证据形式均无法将电子证据完全囊括，出于法律的前瞻性，应把电子证据增加为一类独立的证据类型。尤其是从构建有利于电子商务法律环境的角度出发，就上市交易的现实需求来讲，应将电子证据作为一类独立的新型证据来对待。

2. 不同意见：证据的分类以证明机制为标准，电子证据的出现并未创造出一种新式的证明机制，仅仅是外在形式的不同。独立证据说旨在一定程度上强调电子证据的重要性，但尚有方方面面的问题存在，也会给我国目前本就不严密的“证据七分法”制造混乱。

（六）混合证据说：认为电子证据不属于某一种传统的物证，也并非独立的新型证据，而是若干传统证据的组合。持这种观点的学者很少。

1. 蒋平在《计算机犯罪问题研究》中提出把电子证据分为四类：书证、视听资料、勘验检查笔录和鉴定结论。

2. 不同意见：混合说一定程度上代表解决电子证据问题的正确思路，但有关电子证据形式的三种划分并不周严，这种划分缺乏理论依据。

## 第四节 对电子证据的法律定位的正确看法

### 一、以上各种说法的意义

这些说法由各自的出发点来看均有一定的合理性,但整体上看只反映了部分电子证据的法律定位。在现阶段我们对电子证据的研究处于起步阶段时,各种说法均有一定的启发意义。

### 二、对电子证据法律定位综合的看法

(一)加拿大学者加顿曾经说过:“在司法中使用电子证据的最大挑战在于,不能轻易地将其划归传统的证据类型。”

“名不正则言不顺”。对电子证据作法律上合适的定位具有重要的意义,而这一工作又具有相当的难度。运用电子证据时首先需探明对其进行合理定位的深层原因。如果定位问题搞清楚了,电子证据的许多障碍最终将迎刃而解。

(二)解答电子证据究竟处于何种地位的问题,一方面不能漠视我国现行的证据分类体系,另一方面必须找出电子证据同其他七种传统证据的真正差异,在此基础上才能得出科学的结论。(基础的出发点)

1. 电子证据和传统证据之差异在于载体方式的不同,而并非证明机制的不同。

2. 我国现行刑事诉讼法、民事诉讼法与行政诉讼法对证据的分类虽略有不同,但均大概可以分为物证、书证、视听资料、证人证言、当事人陈述、鉴定结论以及勘验检查笔录七种。相应地,电子证据基本也应分为电子物证、电子书证、电子视听资料、电子证人证言、电子当事人陈述、关于电子证据的鉴定结论以及电子勘验检查笔录七种。

(1) 电子物证:系指电子形式存在的“实在证据”(Real Evidence),以电子信息的存在和状况来证明该案件的事实。

(2) 电子书证:系指电子形式的“书面证据”(Document Evidence),记载了当事人之间的书面意思表示。典型的如电子邮件和 EDI 方式签订的合同。

(3) 电子视听资料:系指电子形式的音像证据,和纸面形式的音像证据相对。主要是各种数码摄、录材料。

(4) 电子证人证言:系指以电子方式存在的言词证据,如网聊的纪录、电话录音等。

(5) 电子当事人陈述:与电子证人证言相似,无非陈述的主体有所不同。

(6) 有关电子证据的鉴定结论:系指由专家对存在有问题(主要是真伪)的计算机记录进行鉴定,出具的鉴定书中所反映鉴定结论。

(7) 电子勘验检查笔录:系指司法人员与行政执法人员在办案过程中以电子形式做出的勘验、检查笔录。

3. 如果司法人员在具体案件中都能为所取得的电子证据进行准确定位,那么就完成了系列工作的首要一步。

(1) 电子证据同传统证据相比,不同之处是在于载体方式方面,而非证明机制方面。这就决定了电子证据绝非一种全新的证据,而是传统证据的演变形式。换言之,我国所有传统证据均存在着电子形式。

(2) 对于电子证据法律地位的科学看法:它不是一种独立的证据形式,而是分别属于传统证据的范畴。在我国一时还难以通过证据立法对证据的“七分法”进行修正的情况下,这种定位无疑会是最合理的选择。它是我国展开电子证据研究的基本出发点,也应是寻求解除电子证据法律障碍的立论依据。

## 第五节 电子证据的学理分类（一）

### 一、对电子证据进行分类的必要性

（一）对某项事物分类是对其进行深入性研究的必经途径和重要方面。对电子证据进行分类是研究这一新生事物的重要方法与途径。

（二）电子证据出现和发展的历程

1. 早期的电子证据为电子通讯类证据。如电话、电报等。
2. 计算机出现后，单一计算机系统的电子证据大量出现。如单个的电子文件、数据库。
3. 互联网出现和成熟以后，开放的计算机系统电子证据广泛出现。如电子邮件、电子公告、电子签名等。

（三）模拟式电子证据和数字式电子证据

1. 模拟式电子证据是通过信息中的某些特征的具体数值或量来记载电子信息的内容。（连续）
2. 数字式电子证据是通过信号的离散状态的各种可能组合所赋予各种数值或其他信息的方法来记载电子信息的内容。（离散）

3. 特点：

- （1）模拟式电子证据记载的信息具有连续性，数字式电子证据记载的信息呈离散状态。
- （2）模拟式电子证据复制时有一定的损耗，数字式电子证据基本可以无损复制。
- （3）模拟式电子证据在剪辑上较困难，删改后容易发现；数字式电子证据是以离散的电磁信号存在，易被删改而不被发现。（恰是基于前两点）
4. 在真实性方面，模拟式电子证据优于数字式电子证据；证明力方面，数字式电子证据的复制品更精确，优于模拟式电子证据（证明力应结合具体条件，不可一概而论）。
5. 二者并非截然分开，模拟式电子证据和数字式电子证据可以通过一定的技术手段加以转变，所以在鉴别其真伪时，应注意考虑有无转换的可能性。这也是一个新课题。（如数码摄录设备的模数转换器）

## 第六节 电子证据的学理分类（二）

（四）数据电文证据、附属信息证据和系统环境证据

1. 此种分类是依照档案学和鉴定学进行的分类。
2. 为保证电子证据的真实性，要求保证电子证据的数据自身，以及该数据产生的时间、地点、形成人、形成机构的职业背景、业务活动等相关内容的真实可靠。电子证据还离不开特定的系统环境，特定的电子数据只有借助其原始的系统软硬件环境才会得到最真实地体现。

3. 按照这种要求，可以对电子证据作如下划分：

（1）数据电文证据：指的是数据电文正文本身，是记载法律关系的发生、变更和灭失的数据。如 E-mail 和 EDI 正文。（主要证据）

（2）对应的附属信息证据指的是数据电文在生成、存储、传输、修改、增删这一过程中引起的相关记录。如系统日志，文件属性信息。其作用在于可以证明电子数据的真实性。（形成的证据保管链条，但也要考察真实性属性，改动很容易）

（3）对应的系统环境证据是指数据电文运行时所处的硬件和软件环境，尤其是指相关硬件规格或软件的版本等信息。（庭审或是鉴定时显现数据电文，保证其以原始面貌显现）

（五）封闭系统中的电子证据、开放系统中的电子证据与双系统中的电子证据

1. 此种分类是根据电子证据的运行环境进行的。电子证据对载体形态的依赖性较大，不同系统环境常会决定证据的本质差别。

(1) 封闭系统是由独立的一台计算机组成的系统，或多台以局域网方式连接的计算机组成的系统。不对外界开放，用户相对固定，能够迅速的跟踪查明电子证据的来源。如银行、证券业、交通运输业的员工均用自己固定的终端进行内部数据的交换。

(2) 开放系统是由多台计算机组成的广域网、城域网、校园网等系统，证据来源不易确定。

(3) 双系统是封闭系统和开放系统的合称，指既能够经常出现于封闭系统又能经常出现于开放系统的电子证据。如 EDI 证据和电子签名。

2. 做此划分的意义：确定证据调查的思路，明确取证方向。

(1) 封闭系统的相对人确定，案发以后可直接通过传统查证方法查找作案行为人；开放系统的行为人不明确，首先应查处在哪台机器上实施了犯罪行为，继而才能在此基础上查处犯罪人。

(2) 封闭系统下的电子证据以计算机本身的存储和显现的证据为主；开放系统下的电子证据常体现于第三方的网络服务器所存储和显现的证据；双系统下的电子证据应视具体环境而定。故而可见，不同系统下的电子证据在可采性和证明力方面的情形复杂程度相差很大。

### 第七节 电子证据的学理分类（三）

(六) 电子设备生成证据、存储证据和混成证据

1. 电子设备生成证据指完全由计算机等设备自动生成的证据。其特点在于它的生成基于计算机的内部命令，不掺杂个人的意志，具有较高的准确性而且其自身的证明力大小主要就是取决于其准确度的高低，如 ATM 机。（关系相对简单）

2. 电子设备存储证据指单纯由计算机等设备所录制的有关信息所得来的证据。此种证据应考虑计算机设备的准确性和影响录制的其他因素。

3. 电子设备混成证据指计算机存储兼生成的证据，是由计算机设备录入信息以后再由其内部运行而得来的证据。它具有上述两种证据的性质特点，对其判断的情形要复杂得多。（可借此确定调查思路）

(七) 原生电子证据和派生电子证据

1. 原生证据是直接来源于案件事实或原始出处的证据；派生证据是经过相应的一些中间环节所形成的证据。

2. 据此分类方法，电子证据可以分为原生电子证据和派生电子证据。但按照这种传统方式对其划分却存在不同程度的法律障碍。

(1) 传统观点：原生电子证据是指电子数据首先固定于其上的媒介物，即最先有某一电子证据的光磁存储介质。除此之外任何由此信息复制得来的信息均属派生电子证据。

局限：如此定义的话数据电文之收件人总是得到的为该“原件”的副本，无法满足电子商务中须提交原件的要求。（和一些现状矛盾，且不具备现实意义）

(2) 联合国国际贸易法委员会观点：对某一直接输入计算机的数据电文，从它首次转化为电子形式起保持完整并未被改动，可以在今后显示为人们可知的形式就可视其为“原件”。

这是一种依照“功能等同法”的观点，是按照解决电子商务中面临“原件”要求的一种解决办法，主要从维护信息之真实可信度为着眼点。

局限：着眼点在于解决电子商务中遇到的法律障碍，仅适用于电子书证，不适用于电子物证和视听资料。

(3) 美国主流观点：电子证据满足以下两条件时属于原生证据。

①当有关数据存储于计算机内部时，能准确反映数据的打印物或其它输出物；②电子证据表现

为副本时，制作者或发行者意图使其具有同文书本身具有同等效力。（不限于自然意义上的“原生”）

这是一种扩大到拟制意义上的原生证据，一定程度上代表了解决电子证据原始性的正确思路。

#### （八）“拟制原件说”

原生电子证据指电子数据本身，或者是制作者或发行者意图使其具有同等效力的副本；并不限于信息首先固定时所在的媒介物，而是对当事人而言具有法律效力和最终完整性的数据。即原生电子证据不限于自然意义上的原生证据，还包括当事人拟制（自己约定、认可）的原生证据。派生电子证据指的是通过其他正确录制的方法所产生的副本。

## 第八节 电子证据法 and 对其研究的意义

### 一、国内外电子证据立法现状

（一）在证据法较为发达的英美法系国家，电子证据法得以诞生和发展，许多研究被吸收为立法成果。

（二）大陆法系国家虽未见相对独立的电子证据法和集中、详细的电子证据的条款规定。但已有相关的规则、规定出台。（如电子签名法）

（三）电子证据法是指各国用于规范电子证据的可采性和证明力，以及用于规范如何收集、保全、举出、质疑和认定电子证据各环节的一系列法律法规的总和。

1. 电子证据法的具体体现形式可以是专门的《电子证据法》、《计算机证据法》，也可以是其他诉讼法或证据法中关于电子证据的专门规定，还可以是实体法或其他法律当中涉及电子证据的零散条款。

2. 我国现有的法律法规虽目前鲜有对电子证据的专门立法，但毕竟一些法律法规中已出现一些零散的条款，电子签名法也于去年得以实施。

3. 借助于证据立法和电子商务立法的外部环境，电子证据方面的相关立法会逐步丰富、完善。

### 二、电子证据法研究的意义

（一）随电子商务和电子政务案件、计算机犯罪案件和涉及电子证据的传统犯罪不断增多；加之我国证据立法已进入议事日程。电子证据的重要性凸现。

（二）对电子证据相关的法律全面深入的研究，有重大的理论和现实意义。

1. 对学界，通过介绍、传播国外的立法经验，澄清对电子证据不准确的认识，充实证据法理论，开拓证据法学的研究空间。

2. 对立法机关，能提高即将着手的证据立法和电子商务立法的质量，避免立法出现缺失。

3. 对政府机关和司法机关，能指导其开展电子政务、开展电子商务监管、完成相关犯罪的刑事司法。

4. 对企业，促进其广泛参与电子商务。避免商业欺诈和不利的诉讼境地。

5. 对个人，能对人们参与网络活动提供帮助，维护不同人群享受电子技术带来的便利时的各项合法权益。

### 复习与思考题

1. 电子证据的概念是什么？和相近的一些名称有什么联系和区分。
2. 电子证据的特点是什么？

### 拓展阅读书目

1. 何家弘：《电子证据法研究》，法律出版社 02 年版。
2. 公安部教材：《信息网络安全监察》，群众出版社 00 年版。

## 第三章 电子证据的收集

本章教学目的和基本要求：本章主要介绍了取证的主体以及取证的方法和步骤，主要知识点在与取证的一般主体和特殊主体，取证的 AAA 方法等方面。重点需要对这些知识点的具体内容有准确了解，难点在于清楚思想指导方法和具体操作方法在取证过程中各自的作用和联系。

学时分配：

### 第一节 取证主体（一）

通常取证主体随案件中举证责任分担的不同而不同，而对于特殊的证据由证据性质的不同也会对取证主体有影响。电子证据由于其自身特点导致对其的取证方式具有特殊性，由此要求对电子证据取证有特殊的取证主体。

#### 一、电子技术专家

（一）电子技术专家指对电子技术有专长的人。

（二）电子技术专家可以帮助

1. 从获取某一电子证据的困难程度和最终的可能结果分析，给出是否提取该电子证据之建议；
2. 制定提取某一电子证据的计划、步骤及相应的要领；
3. 协助搜查、扣押计算机硬件，寻找潜在的电子证据，依照法定的程序提取，从技术层面上确保所提取证据的真实性和完整性；
4. 恢复被删除的某一电子证据或整个系统；
5. 协助保管某一电子证据，使其不被改动；
6. 作为专家证人出庭作证，介绍收集、保全电子证据的技术过程的可靠性，接受当事双方的质询；
7. 对有关电子证据之专门性问题做出鉴定结论。

（三）不可以迷信或过度依赖电子技术专家

1. 电子技术专家限于自身条件往往只能注意案件中的技术问题，考虑不到犯罪人的对抗行为，在取证过程中没有这种基本的意识而发生低级错误。
2. 电子技术专家的利益与证据调查人员不可能总一致，总会或多或少的存在一些偏差，有时甚至是背离。
3. 电子证据专家收集、保全电子证据的方法并不一定会符合证据可采性的要求。如电子证据专家有可能会因为法律知识的缺乏而致使本来具有很强证明力的证据因为是非法收集的而被排除采用。
4. 电子证据取证过程中，应强调专门的调查人员和电子证据专家之间的紧密配合和互相监督。

### 第二节 取证主体（二）

#### 二、网络警察

（一）网络在给人们带来便利的同时，也带来了由网络引发的新问题——网络安全问题。网络犯罪（或利用网络途径的传统犯罪）较典型传统犯罪相比有一些特点：

1. 技术性强，通常的犯罪人都具有较高的计算机技能，且会利用高科技手段来掩盖犯罪，使

侦查取证工作困难。

2. 网络犯罪行为地和结果地互相分离，有别于传统犯罪而使得传统的侦查机关采取传统的侦查手段会束手无策。

(二) 对策：建立专门的维护网络安全的警察队伍——网络警察，由他们负责搜寻和犯罪相关的电子证据；监控网上犯罪；负责和外地，外国相应的网络侦查机关开展合作；搜集证据、辑查犯罪以及侦破国际犯罪。

(三) 有关网络警察队伍的现状

1. 美国：

Computer Emergency Response Team

High Technology Crime Investigation Association

National Infrastructure Protection Center

负责及时应对网络运行中出现的紧急情况，协助收集隐匿在网络空间的证据，在网上追踪逃犯以及提供有关电子证据效力的法律帮助。

2. 我国状况：

我国安徽省最早出现网络警察，负责处理“欺诈、挪用公款、色情等犯罪案件”，公布计算机病毒情况和开发互联网过滤软件工作。各个省厅成立计算机安全监察处，公安部成立由计算机犯罪监察局。

3. 完善途径

(1) 招聘专业技术人才，扩充网络警察队伍；

(2) 对网络警察及时培训；

(3) 鼓励网警和民间组织及商业公司合作；

(4) 建立全国性协调机构；

(5) 加强电子证据取证国际性合作。

### 第三节 取证的方法和步骤（一）

#### 一、电子证据取证的思想方针

电子证据的取证涉及到对电子证据的保存、识别、提取、归档和解释，以作为证据或作为动机分析的依据。电子证据取证工作需要遵循一种明确的、严格定义的方法和程序，对于非同一般的事件又需要灵活机动的处理不可墨守成规。

#### 二、电子证据取证的特殊性

电子证据取证和其他类型传统证据的调查取证工作有所不同。传统的暴力案件现场需要在拍照，搜寻证据和供比对的样本并且需要控制样本以便和证物对照。电子证据的调查工作当中也存在有类似的工作。但许多时候，调查人员向需要对整个系统（无论是单机还是大容量的磁盘阵列服务器甚至是整个网络）进行重建，这是不同于传统证据取证但在电子证据取证中常见的工作。

#### 三、电子证据取证的事前态度

调查初始，就要认真对待每一个案件。不要随意的开始检查某一台计算机，判定它是否有问题然后再将其作为一个证物来对待；而应该一开始就把计算机作为证物来对待，即便以后发现它并不能成为证物。如果在开始时主观的认为某一台计算机没有取证价值而后来发现了有不法行为的痕迹，就需要确认已经完整的记录下来所采取的某一个步骤及采取该步骤的原因。记录的工作对于任

何证据调查工作都很重要，尤其对电子证据调查更是这样。

#### 四、电子证据取证的基本的思想方法

取证的基本思想方法是相对固定（fixed）的，一定时期内不会随着计算机技术的量变而改变，除非计算机技术产生了根本性的质变，可以概括其为 AAA 方法。

### 第四节 取证的方法和步骤（二）

#### 一、基本的方法（AAA 法，取证的框架）

1. 在不对原有的证物进行任何损坏或改动的前提之下获取证据；（Acquire）
2. 证明所获取的证据和原有的数据是相同的；（Authenticate）
3. 在不改动数据的前提之下对其进行分析；（Analyze）。

##### （一）获取证物

##### 1. 证据监督链（chain of Custody）

做好监督链的目的为了保护证物的完整性而且能够证明在这一过程中证物并没有被改动。监督链是一个简单有效的过程，记录了证物在案件周期内的完整经历。

##### （1）谁收集的证物？

##### （2）在何处收集，怎样收集的？

##### （3）谁拥有该证物？

##### （4）证物如何存储，受到了怎样的保护？

##### （5）谁将证物从存储设备中取出以及取出的原因？

（6）任何接触过证物的人员取走和归还的时间，使用证物的目的都应该有完整的记录。而且接触的人员应该尽可能的少，“每个有能力接触到证物的人都有能力篡改证物。”

##### 2. 收集

（1）证物收集的复杂性反映出事件本身的复杂性。收集证物时应尽可能收集一切通过合法手段所获得的东西。包括一些看上去没有证据价值的东西，甚至是废纸。现场的呈现仅有一次。

（2）对于和 ISP 有关的证物必须尽快行动。因为日志文件的保存都是受时间限制的。对于准备

##### （3）作为证据使用的日志应要求服务商合适的保存。

##### 3. 标识

（1）对于证物进行准确的标识和统计是必要的。标识中应该有案件编号、简要描述、签名和收集的时间等信息。

##### （2）标识工作的进行可以借助一些表格软件或是手工进行。

##### 4. 运输

运输工作应以保证证物的安全为基本要求。针对证物的不同情况采取不同的措施来加以保证。运输的容器上应有封条。

##### 5. 存储

恰当存储证物既是器材本身物理上的要求也是其作为证物的法律价值要求。证物应存储在安全且访问受到限制的地方。

## 第五节 取证的方法和步骤（三）

### （二）鉴别证物

这个环节里需要证明调查人员在取证过程中没有造成任何对原证物的改变；或者虽然有改变，这种改变也是由计算机的本质特征造成的，同时这种改变对证物在取证意义的价值没有任何影响。

1. 计算机磁盘驱动器会逐渐老化，但无论是可读的文本还是图片都不会因为这种老化而显示出别的不相关信息。任何文本和图片的存储、设置都是源于有动机的人类的行为。

2. 可以采取在取证过程中的一些方法保护证物：

（1）通过证物监督链可以证明在取证过程没有引起对原有证物的任何改变，由证物所推测出来的事件发生的情况也是真实可信的。（规程上）

（2）对证物的完整性验证和对其添加时间戳也能解决证物真实可靠性问题。（技术上）

（3）一般是通过计算一种类似电子指纹的值加以实现的。电子指纹的对象可以是单个文件到整个硬盘。这是来于密码学的技术，指纹值称之为哈希值，可以通过软件计算完成，这只需要在取证的软件中添加这种功能。收集数据时就要计算和记录哈希值，日后可由此证明用做检查的数据拷贝和收集的原始数据是完全相同的。

### （三）分析证物

1. 分析阶段在一定程度上是取证工作的核心部分。基于客观、科学的技术原理对电子数据、程序代码、电子设备及相关的文字资料进行分析：就电子数据之来源、特征、传播途径和范围；程序的来源和功能；电子设备的功能；嫌疑人的特征、行为动机及后果做出定性或定量的分析结论。

2. 对证物的分析工作常常是在物理层进行，意外损坏证据的可能性很大。一般的原则是使用原始证物的数字拷贝分析，这样即便受损也很容易恢复。

3. 完成以上证据搜寻工作后，应在用于分析的机器硬盘上做几份拷贝。当需要有文件嵌入到报告中时，可进行格式上适当的整理以增强可读性。这样得到的文件某些属性会发生改变。但只要原始证据安全保存着，只是为了报告的目的而仅对证据的电子拷贝作了格式上的修改，就仍然是没有问题的。

（四）电子证据取证的过程基本是上述三步骤。一个成功的调查活动需要严格遵循种种证物的收集和看管规则，又要具备相当的灵活性甚至想象力。在此之间寻找到的一种平衡是最好的状态，这依赖于知识和经验的长期积累。这些只是一个大致的有关取证方法、步骤的范本，遇到实际情况时未必总要遵循这些步骤。在每一个不同的犯罪现场不可能有现成的蓝本，必须要在坚持基本规则顺序的前提下灵活机动，根据实际情况有所改变。

### 复习与思考题

1. 电子证据的取证主体都有哪些？如何认识他们在取证工作中各自的地位和作用。
2. 电子证据取证的事前态度是什么？AAA方法的内容具体都指什么？

### 拓展阅读书目

1. 公安部教材：《信息网络安全监察》，群众出版社 00 年版。
2. Alan M.Gahtan: “Electronic Evidence”, by the Thomson Professional Publishing 1999

## 第四章 电子证据收集现场的操作

本章教学目的和基本要求：本章主要介绍了在电子证据现场的一些具体的组织工作和对不同类现场的要求。重点在于对电子证据现场的系列具体工作有较明确的了解，难点在于把握这些序列的工作并不是机械的，而是需要根据具体场景的不同，灵活机动的开展。

学时分配：

### 第一节 电子证据收集的现场及相关工作（一）

#### 一、电子证据的现场

刑事案件的现场指罪犯实施犯罪的地点，常是遗留物证痕迹较多的场所。而遗留电子证据的场所包括传统现场和非传统现场，即物理空间和虚拟空间。虚拟空间具有抽象性、不可见性和潜在性。在勘查阶段主要的任务是能够在这种特殊的现场提取到有用信息。

#### 二、预先评估现场

主要方面包括了解搜查的位置、类型和要取得的设备以减少搜查过程中的无用功。

（一）得到待勘查区的图纸。要尽可能的划出地形或取得地面设计的副本，相关的信息可以从被调查地区的建筑承包商以及其他熟悉的的人士处获知。

（二）查明计算机类型、数量以及涉及的介质。计划好需要的搜查设备以及用于备份嫌疑人设备所需的存储介质。

（三）备好相关的软硬件。应及早作准备，在紧急的情况下自己的筹集更困难。这一步工作提前做得越好，工作开展后遇到的压力才会越小。

（四）确保预先拥有的工具箱里的所有工具名目。预先制作好需要的工具或设备的列表，搜查的准备工作就会容易。

（五）备好备份及拷贝所需要的介质。

#### 三、建立调查队

由于证据调查的工作量大，需要安排合适的人数以及有工作基础的人员组成完整的调查队。

（1）调查总监：应具备调查复杂案件的丰富经验，负责处理媒介关系、管理并安排人事和设备以及监督整个调查的进程。

（2）讯问小组：该小组应不少于两人，职责是询问每一个证人和犯罪嫌疑人。成员须具备丰富的审讯技能。

（3）素描和影像小组：由一名或以上的成员构成，素描下整个犯罪现场，对房间编号，对整个现场内外的所有证据进行拍照，适当时应以摄像的方式记录下细节和全过程。

（4）物理搜查小组：该小组应安排一名以上成员搜集每一个房间，找出每一证据所在的位置，并以彩色记号标志出这些证据以便证据查封小组的识别。他们需要对搜查的项目有详尽的了解，具备周全认真的工作品质。

（5）安全及逮捕小组：保护犯罪现场，保障人员和证据的安全，承担逮捕和犯罪嫌疑人的任务。实际操作中应尽可能多的配备该小组成员。

（6）技术证据没收及笔录小组：常由两至三名成员组成，通常分作计算机调查人员和专门的计算机专家。其任务是将证据资料输入计算机，将证据编号以后放进工作包或工作盒内，在对证据

拍照以后在工作盒上贴上标签并负责计算机拍照后的拆卸工作。

## 第二节 电子证据收集的现场及相关工作（二）

### 四、建立攻击计划

建立的攻击计划适合以图表和清单的形式做出。实践中使用的简洁的方法是按照 SMEAC（位置 situation、任务 mission、执行 execution、进入撤退的道路 avenues 和通信 communications）的五段式军事命令方法来建立计划。

（一）位置：对需要面对事物的人数、设备类型、地理位置等做好定义。

（二）任务：具体的情形对应不同的具体任务，如是想抓获犯罪嫌疑人还是查明犯罪嫌疑人的类型等。

（三）执行：具体怎样来完成任务，如选择合适的执行时机（如对商业单位调查时不影响其正常的运行）

1. 进入和撤退的路径：如何到达和处理现场所采用的方法会因调查的类型不同而不同，应考虑到安全及逮捕小组单独采取行动和有审计员参加的小组的行动有所不同；

2. 应考虑到怎样在出入犯罪现场时得到群众的帮助；哪些地方可以停车，哪些地方有潜在的障碍，哪里允许调查人员覆盖介质以及那里可以装载搜获的证据。

（四）通信：小组成员通常采用无线电或移动电话作为互相联系的方法，尤其不可忽视无线对讲机的作用。

（五）准备搜查令：对于涉及新技术的搜查令，应把搜查令提交给有经验的侦查员和公诉人以确保涵盖了所有的要点。

### 五、执行搜查

执行搜查时应遵循一些原则，如不要切断建筑物的电源，不要随意接近犯罪嫌疑人以免引起其怀疑而毁坏数据。

（一）封锁并监视可疑的犯罪现场，宣布办案人员的身份以及执行搜查的原因。

（二）记录这一过程。以照相、绘图、笔录方式对原始现场记录。

（三）保护现场

1. 立刻确认建筑物内所有计算机的位置。

2. 每台计算机都须有专人实施物理保护。

3. 移动计算机以前要拍照记录计算机自身和相对于其他物品的位置标明每一根连线的连接方式，贴上标号。

4. 在一个远离被调查计算机的地方讯问犯罪嫌疑人和询问证人。

（四）调查队成员各司其职

案件的负责人负责分配任务和有效地指导、解决问题并最好不要承担别的任务以便正确的评估和指导现场。制作草图、问讯、照相和搜查可以同时进行。每一分组安排一人撰写报告，所有的报告、草图、相片归总交于案件负责人。

（五）完成搜查

离开现场前询问小组工作情况并尽量的解决未完成的问题。将遇到的新问题记在一个为今后调查准备的进程笔记本里。

### 第三节 不同类型电子证据现场勘查的工作要求

电子证据现场勘查基本可划分为单机和网络现场的勘查。

#### 一、单机现场

技术手段和普通的勘查手段相结合，和犯罪有关的传统痕迹物证、外围设备等予以扣押。扣押的磁性介质、易损介质应以合适的方式包装保存。对发现的涉案数据进行妥当的复制，对遭受破坏和删改的数据应使用专门的设备读取残留的数据，有条件的话尝试对其恢复。

#### 二、网络现场

需要勘查的是由若干计算机构成的无形的大网，实际的情形更为复杂。证实犯罪的电子证据分散在这个网中，一方面给侦查人员发现证据造成了困难；反过来由于证据的分散，使之不易人为遭受灭失。

1. 网络上的电子证据源包括服务器日志、网络设备的内容及有线和无线网络上的流量。

2. 为了能够在网络上追踪犯罪并将犯罪活动与罪犯联系起来需要了解一些核心和底层的技术。比如为了有效调查计算机入侵需要对 TCP / IP 和相关操作系统有较深入的理解。至少调查人员应对网络有一个基本的认识，从而能够解释在计算机上发现的电子证据。

3. 如果调查人员不能理解在网络中何处可以发现信息，就会浪费大量有意义的时间并可能丢失有价值的证据；不能理解网络的工作原理则难以理解从网络上得到的任何数据。

#### 复习与思考题

1. 什么是电子证据的现场？
2. 电子证据现场勘查的种类有哪些？

#### 拓展阅读书目

1. 张越今：《网络安全与计算机犯罪勘查技术学》，清华大学出版社 03 年版。
2. 段海新等译：《计算机取证：应急响应精要》人民邮电出版社 2003 年版。
3. 常晓波译：《应急响应计算机犯罪调查》清华大学出版社 2002 年版。

## 第五章 电子证据的保全

本章教学目的和基本要求：本章主要介绍了对电子证据进行保全的两种典型方式。本章的难点在于电子证据和传统证据的很多不同，会导致对电子证据进行保全将面临到诸多的新问题。

学时分配：

### 第一节 常规保全

#### 一、电子证据保全的重要性

（一）证据保全即证据的固定和保管，是指用一定的形式将证据固定下来，加以妥善保管以便司法人员或律师分析、认定案件事实时使用。

（二）证据保全是取证制度的重要环节，是证据收集工作的延续。

（三）电子证据的保全相对于传统证据的保全工作更具特殊的意义。

（四）对电子证据的保全工作需要当事人或法院及时聘请技术专家加以辅助。

#### 二、电子证据的常规保全方法

（一）对电子证据的保全既可以是诉讼开始之前又可以是诉讼开始之后；既可以由当事人自行完成又可以由人民法院、人民检察院、公安机关、国家行政机关来完成。

（二）与传统的证据保全相比，电子证据的保全具有一定的特殊性。它显现为一种虚拟空间的保全，需要使用不同于传统保全的方法加以进行。

（三）电子证据的种类不同，对应不同类型的具体保全方法也有所不同。

1. 对电子证人证言、电子当事人陈述等言词证据，常用的保全方法是制作询问笔录和录制资料等；

2. 对于电子物证和电子视听资料，常用的方法是勘验并制作勘验笔录、绘图、拍照或录像，方便时加以扣押或封存、提取原始介质；

3. 对于电子书证，除了扣押以外，还可以缩微、复制、存档。

4. 对于电子笔录，常用的保全方法是打印出来并加以核正，然后盖章封存。

（四）实施保全时，为了确保其结果的有效性，应该尽量的通知双方当事人或其代理人到场，或安排证人见证。

### 第二节 公证保全

#### 一、电子证据公证保全的优越性和难点

（一）公证是指公证机关或公证人根据当事人的申请并依照法律规定，对法律行为、有法律意义的事实或文书的真实性、合法性进行证明的活动。

（二）公证所取得的证据可以为法院直接作为认定事实的根据，具有其他证据所不及的法律效力。

（三）公证是国家司法制度的组成部分，公证机关进行的证明活动必须严格按照国家规定的法定程序进行。

（四）电子证据是一种存在于虚拟空间的证据，不仅容易消失和改变，而且提取或保存的过程

很不直观，对其公正保全客观上存在较大的困难。必须要从技术上和制度上彻底解决这些难题。

## 二、电子证据公证保全的方法

电子证据公证保全是指通过公证的方法对电子证据进行固定和保管，其主体和程序与普通公证无异。

实践上对电子证据公正保全主要有两种形式。

### （一）传统公证保全

1. 公证人员同当事人见面后，接受并审查申请人员的委托，开展面对面的公证工作。
2. 其特点是前提依然基于当事人面对面的申请，公证人员也必须亲临现场。

### （二）网络公证保全

网络公正保全是一种保全电子证据的新颖而重要的手段。

网络公证保全是指由特定的网络公证机构利用计算机和互联网技术对互联网上的电子身份、电子交易行为、数据文件等提供增强的认证和证明以及证据保全的公证行为。

网络公证保全的特点

必须借助先进的网络技术才能进行。

在技术运作上具有快捷性、准确性。

是一种远程公证。

我国的网络公证目前仍然留有传统公证的痕迹，很多方面亟待完善。

## 复习与思考题

1. 试述电子证据保全的重要性。
2. 对电子证据保全的难点怎样把握。

## 拓展阅读书目

1. 何家弘：《电子证据法研究》，法律出版社 02 年版。
2. 段海新等译：《计算机取证：应急响应精要》 人民邮电出版社 2003 年版。

## 第六章 网络基础知识

本章教学目的和基本要求：本章主要介绍了和电子证据调查相关的网络基础知识。了解这些网络基础知识对于深入了解电子证据取证方向和途径有重要作用。本章重点在于了解网络信息在底层的运行基础及其与调查工作的关系。

学时分配：

### 第一节 OSI 网络模型简介

#### 一、OSI 参考模型（Open Systems Interconnection reference model）

（一）OSI 参考模型是基于国际标准化组织（ISO）的建议，是在每层使用的协议逐步标准化的基础上发展起来的。

OSI 参考模型共有七层，其分层原则是：

1. 根据不同层次的抽象分层；
2. 每层应实现一个定义明确的功能；
3. 每层功能的选择应有利于制定网络协议的国际标准；
4. 各层边界的选择应尽量减少跨过接口的通信量；
5. 层数应足够多，以免不同的功能混杂于同一层中；但层数也不宜太多，否则体系结构会过于庞大。

#### 二、OSI 参考模型的具体分类

（一）物理层（physical layer）：涉及到通信在信道上传输的原始比特流，保证一方发出二进制“1”时，对方收到的也是“1”而不是“0”。

（二）数据链路层（data link layer）：主要任务是加强物理层传输原始比特的功能，使之对上面的网络层表现为一条无错线路从而联系同一路由器的局域网内不同的计算机。

（三）网络层（network layer）：网络层关系到子网的运行控制，确认分组从源端到目的端如何选择路由。网络层常设有记帐功能，以对提供子网的服务进行量化。

（四）传输层（transport layer）：基本功能是从会话层接收数据，在必要时把它分成较小的单元传递给网络层，并确保到达对方的信息正确无误。

（五）会话层（session layer）：会话层允许不同的机器用户建立会话关系。会话层允许进行类似传输层的普通数据的传输，并提供对某些应用有用的增强服务会话，也可被用于远程登录到分时系统或在两台机器间传输文件。

（六）表示层（presentation layer）：表示层用于完成特定的功能。表示层以下的各层只关心可靠的传输比特流，表示层关心的是所传输信息的语法和语义。

（七）应用层（application）：应用层的功能是文件传输，不同的文件系统有不同的文件命名原则，不同的系统之间传输文件所需处理的各种不兼容问题也属于应用层的工作。

## 第二节 计算机网络协议

### 一、网络协议

计算机网络以资源共享为目的，其主要功能是相互通信和交流信息。由于连网的计算机类型各异，各自所使用的操作系统和应用软件也不尽相同，因此，为保证彼此间的通信能够畅通，应该有一个通信双方共同遵守的规则，这就是网络协议（protocol）。

### 二、网络协议的种类

计算机网络协议很多，除了 TCP / IP 协议，还有 Novell 的 IPX 协议、微软的 NetBIOS 协议、IBM 的 System Network Architecture 等。每个协议组都是对同一事物的不同表述。

### 三、TCP/IP 协议

（一）TCP/IP 协议是网际互联的一个协议簇，形式上是 Transmission Control Protocol/Internet Protocol 的缩写，是和网际互联相关的协议系列。

（二）TCP/IP 协议自二十世纪六十年代开发出来以后，便用于“异构”的网络环境，即 TCP/IP 协议可以在各种操作系统上实现，并已经成为建立计算机局域网、广域网的首选协议。

（三）TCP/IP 协议簇包含有网际协议 IP、地址解析协议 ARP、互量网控制信息协议 ICMP、用户数据报协议 UDP、传输控制协议 TCP、路由信息协议 RIP、简单邮件传输协议 SMTP、域名系统 DNS 等许多协议。

（四）TCP/IP 协议的开发早于 OSI 参考模型，所以不太符合 OSI 参考标准。大致上，TCP 协议对应于 OSI 参考模型的传输层。OSI 模型虽然是计算机网络协议的标准，但由于其开销大所以采用的并不多；TCP/IP 协议由于简洁实用从而得到了广泛的应用，成为 Internet 网络事实上的工业标准和国际标准。

（五）TCP/IP 协议的参考模型分为四层：

1. 物理链路层：通常包括操作系统中设备驱动程序和计算机中对应的网络接口卡，他们一起处理和电缆（或其它传输媒介）的物理接口细节。

2. 互连网层：提供无连接服务的数据传送机制，但并不保证传输的可靠性，只负责将分组信息发往任何网络并使分组独立的传向目标。

3. 传输层：位于 TCP/IP 模型中互连网层之上的一层，功能是使源端和目标端主机上的对等实体可以对话，与 OSI 的传输层在功能上相同。

4. 应用层：应用层位于传输层的上面，包含所有的高级协议。最早引入的是虚拟终端协议（Telnet）、文件传输协议（FTP）、简单邮件传输协议（SMTP）。

## 第三节 计算机网络协议分层的实现

### 一、网络协议分层的实现——封装

封装是实现网络协议分层的一种方法。它的思想是软件每层都会在网络流量的创建过程中实现特定的用途。模型中的每一层都往在网络上发送的数据包中添加信息或称报头（header）。

（一）生成 TCP/IP 网络流量的各个步骤：

1. 编辑邮件，单击发送按钮。

2. 生成电子邮件的应用程序创建自己的报头，将信息传递给传输层并被该层的 TCP 或 UDP 软件处理添加上 TCP 报头。

3. 传输层添加完 TCP 报头添加在邮件前边之后，TCP 软件将其传递各网络层在该层由 IP 软件处理。

4. 网络层创建完 IP 报头将之添加在电子邮件前边，继续由 IP 软件传递给数据链路层的网卡。在该层上创建数据链路层报头并生成网络介质上所使用的电子或光的 1 和 0 信号。

5. 接收端的计算机在物理层接收该数据包，并在每个相应的层以相反的顺序去掉各个报头。数据被由下至上传送至接收用户的应用层的栈。

(二) 分层概念在用于截获活动的通信时是一个需要考虑的重要事项。调查人员在没有得到授权截获通信的全文时，他们有可能被授权截获通常所说的事务 (transactional) 信息。事务信息中包含有 TCP/IP 数据包中的报头。

全文监视需要截获用户的数据；而决定通信的源和目标的事务截获仅仅是截获了 TCP 和 IP 的报头。

### 复习与思考题

1. OSI 参考模型的分层原则是什么？
2. 试述 TCP/IP 协议及其实现方式。

### 拓展阅读书目

1. 段海新等译：《计算机取证：应急响应精要》 人民邮电出版社 2003 年版。
2. 常晓波译：《应急响应计算机犯罪调查》 清华大学出版社 2002 年版。

## 第七章 硬盘驱动器和存储介质基础

本章教学目的和基本要求：本章主要介绍磁盘存储的概念与基本结构以及相关的用于磁盘存储调查的软硬件设备。本章重点在于深入的了解磁盘存储的基本原理以及如何从磁盘存储的不同空间调取数据。

学时分配：

### 第一节 什么是硬盘

#### 一、硬盘的逻辑结构

硬盘是由一个逐渐减小的数据结构的集合组成，每一个数据结构包含在下一个更大一点的存储体集合里。理解这些硬件和软件的层次以及它们是如何交互的，知道它们可能会有那些能够藏匿数据的电子角落对一个电子证据调查员非常必要。

##### （一）控制器

1. 硬盘如果没有总线（BUS）来和系统进行交互的话将毫无用处。总线是用于在计算机系统的组件之间传输数据的通讯线路。从本质上说，总线允许系统的不同部分共享数据。例如，总线将磁盘驱动器控制器、内存和输入/输出端口连接到微处理器。

2. 最为常见的接口是小型计算机系统接口（SCSI）和电子集成驱动器（IDE）。

##### （二）硬盘的结构

所有硬盘都有相同的基本结构。密封的硬盘外壳内是均匀覆盖磁性介质的盘片。每个盘片按照同心圆划分为磁道，盘片的上下各有一个带传动机构的存取臂称作读写磁头。所有的读写头作为一个整体在盘片组中移动。

##### （三）硬盘的软配置

硬盘可以被逻辑的划分为不止一个的分区，这些分区是一个单独的硬盘看起来像是多个独立的硬盘。分区表是全部主分区和扩展分区的索引，映射分区的位置与类型。

##### （四）查看与操作分区表

对一块硬盘进行分析前，应先获得关于它的配置的尽可能多的信息。多数 PC 操作系统会带有某个版本的 FDISK 程序，可用以显示分区数目和各分区的类型。

### 第二节 操作系统

#### 一、操作系统通过设备的驱动程序来访问硬件

理论上系统可以提供一种任何复杂应用程序都能使用的标准界面。即应用软件无需考虑到硬件系统的差别就可以顺利的在不同的平台上运行。这是因为操作系统和设备驱动程序通过了一个软件抽象层（应用程序接口）隐藏了这些信息。

#### 二、任何操作系统都为存储设备提供基本输入 / 输出（I / O）接口

Windows 本身并不提供取证分析时需要了解的更多的细节（非开放的），Unix 系统在这一方面提供的功能较强。

### 三、文件系统

(一) 文件系统是研究硬盘必须注意的重点。文件系统指文件命名、存储和组织的总体结构。它类似于数据库，是一组数据对象的集合，能从外部对其引用和操作。常见的有 NTFS, FAT, FAT32。

(二) 操作系统是通过文件系统存储和读取文件的。我们可以利用文件名、存储位置、日期和其他的特征访问各类文件。

(三) 文件系统同样有一个或多个索引(表)，每一个对象(文件)在这些表中都有一个唯一的标识，并含有相应的位置信息。用户在要求访问文件时系统就可以通过这些表找到对象。

(四) 让一台计算机能辨别某个特定的文件系统的过程称为装载文件系统。这一过程中，操作系统辨别出包含文件系统的特定分区，将该分区映射成一个具体的名字或路径，再把文件表复制到系统内存区，这样文件系统就可以被读写了。

(五) 和数据库一样，文件系统对特定大小的数据单元进行操作。在 Unix 中称之为“块”，在 Windows 中称之为“簇”(都是最基本的分配单位)。这些数据块是操作系统实际存入数据的最小存储单元，每个文件都是由若干个数据块组成的。

1. 显然数据块越大，读写磁盘的速度也就越快。这些数据块实际的表示了系统所能引用的最小数据。如果没有被用完的话文件的最后一个数据块就会产生或多或少的闲散空间，没有用到的部分就浪费掉了。

2. 数据块小的文件系统产生的浪费较小，但它的性能不如数据块大的文件系统好。为在性能和效率之间取得平衡，较新的文件系统在数据块的大小上有更多的灵活性。

(六) 格式化是把一个分区转换成操作系统能够识别的文件系统的过程。Windows 执行该操作的程序就叫格式化(format Command)；多数 Unix 系统中叫 mkfs。

## 第三节 磁盘数据的存储

### 一、未分配空间

计算机系统内有大量的未分配空间，其多数保存有各种各样的数据。这些数据很多时候不是人为隐藏的而是被操作系统“遗弃”的数据。

(一) 闲散空间是指文件最后一个数据块或簇中未使用的部分。只有文件大小正好是数据块(FAT32 的数据块是 4096 个字节)的整数倍时才没有闲散空间。平均的看每个文件占用的闲散空间有 0.5 个数据块大小。通过正常的文件系统接口访问不到这些闲散空间，因为操作系统本身不允许访问超过文件末尾的地方。

(二) 把文件读进内存时，闲散空间不会跟进来；把文件写到一个数据块不一样大的磁介质上，所形成的文件会有不同的闲散空间，而且可能包含有任何留在那种介质上的数据。无论是把文件通过邮件发给某人还是用 FTP 在网络上传输都不能把闲散空间里的数据带走。所以取证时对硬盘的拷贝并不能在文件的级别上进行，而必须对硬盘里所有的东西进行完全的映象。

(三) 未分配的簇指那些当前还没有被任何文件使用的块。一个频繁使用的系统中，所有的扇区都可能被写过多次，文件也经常的改换位置。一个应用程序改变一个文件并重写它以后原先改变的文件会被删除占用的所有数据块会被回收而处于未分配状态。这些簇中间保存原先文件中的所有数据，直到被重写为止。系统中“自由空间”的比例越大，未分配文件被改写前保存在系统中的时间就越长。

(四) 未分配的数据簇可用几种方式来进行检查。最为简便的方法是用一个取证工具包查看数据。Unix 系统下可以将整个分区看成一个单一的对象，利用 16 进制编辑器来搜索和检查整个分区

或硬盘。对一块硬盘检查时首先要了解它有几个分区，每一个分区有多大。所有分区加起来的大小是否等于整个硬盘大小。

## 二、不能真正删除硬盘上的数据

(一) 数据写到磁介质上时每一次都会留下浅浅的痕迹，甚至在介质被写过很多次以后每一次的痕迹仍然被留下来。

(二) 使用特殊的电子显微镜可以一比特一比特的恢复写过多次的磁道。曾有报道有科研人员能够恢复数据已经被覆盖了七次以上的硬盘。

(三) 一些商业公司常常提供数据恢复的业务，他们在硬盘厂商的授权和支持下能从出现故障甚至是有物理损坏的硬盘中获取大量有用数据。

## 第四节 国内外当前硬盘取证设备简介

### 一、硬盘取证设备的要求

随存储技术的发展，硬盘的种类增加、容量加大。这在给普通用户增加更多便利的同时，给使用硬盘取证也带来更多困难。完整、彻底、精确的获取数据是对硬盘取证的基本要求。同时具有高速度、多功能、智能化以及广泛的适用性是对此类取证设备的发展要求。

### 二、目前国内外市场的主流设备

1. 为司法需要专门设计的 SOLOIII、SOLO II、MD5、SF-5000 专用硬盘取证设备；适合 IT 业硬盘复制需要的 SONIX、Echo 硬盘拷贝机；

2. 以软件方式实现硬盘数据全面获取的取证分析软件如 Encase、FTK；综合实现硬盘取证和数据分析所需要的多功能取证箱如 Road MASSter II、“天宇”移动介质取证箱、“网警”计算机犯罪取证勘查箱；针对无法打开计算机机箱的硬盘专用获取设备如 CD-500、全能拷贝王。

3. 不同类型的取证产品有各自的特点和优势，依据不同的行业需求和功能需要应合理采取不同的方法与设备。为实现最佳的取证效果，还有必要深入挖掘各种产品的功能，对不同工具合理组合，建立所谓的取证勘查工具集合，以进一步增强取证能力。

### 三、手持式硬盘取证设备

手持式设备体积小、重量轻、使用方便、拷贝速度快，是目前硬盘取证之首选设备。多数手持式拷贝机以硬盘直接拷贝为主要方法，即将嫌疑人的硬盘取出直接与拷贝机连接实现硬盘数据的全面复制。一些新型的拷贝机除了直接拷贝还增加了 SATA 硬盘接口、SCSI 硬盘接口、USB 接口、PCMCIA 接口，进一步增强了其适用范围。

(一) 市场上手持拷贝机按性能大致可分为两代：

第一代硬盘拷贝机，速度最高达 1.8GB / 分钟。

第二代硬盘拷贝机，速度最高达 3.3GB/分钟。

(二) 按照用途分为司法专用型和民用型两种。

(三) 代表型号手持式硬盘拷贝机有 SOLOIII 硬盘拷贝机、MD5 硬盘拷贝机、SONIX 硬盘拷贝机等。

### 四、取证勘查箱

由于电子证据取证涉及的信息存储介质种类很多，主要有软盘、硬盘、光盘、闪存、各种数字

卡、ZIP、不同的掌上电脑及手机等。由此取证人员需要有一套适应面广、拷贝功能强、携带方便、使用灵活的移动取证平台以适应需要。目前国内外的有关此类产品从功能和形式上可划分为三类：改装型、工控型和组合型。代表产品如北京天宇晶远移动介质取证箱。

## 第五节 代表性取证专业软件简介

### 一、Encase

Encase 是被美国政府认可的计算机取证产品，是唯一的完全集成的基于 Windows 界面的取证应用程序，包括数据浏览、搜索、磁盘浏览、建立档案、建立证据文件、保存案例等功能。我国公安系统今后将以 Encase 作为主要取证的工具软件

### 二、FTK

Forensic Toolkit ( FTK) 是一系列基于命令行的工具，帮助推断 Windows NT 文件系统中的访问行为。它主要包括 Afind (根据最后访问时间给出文件列表)、Hfind (扫描磁盘中有隐藏属性的文件)、Sfind (扫描整个磁盘寻找隐藏的数据流)、FileStat (报告所有单独文件的属性) 等命令。

### 三、ForensicX

ForensicX 是运行于 Linux 环境，以收集数据及分析数据为主要目的的工具。它是和配套的硬件组成专门的工作平台来运行的。由于它利用了 Linux 系统支持多文件系统的特点，提供在不同文件系统中自动装配映象的能力、能够发现在分散空间的数据，还可以分析 UNIX 系统中是否有木马程序，新版本还有识别隐藏文件的工具。

### 四、TCT

The Coroner's Toolkit (TCT) 主要用以调查被“黑”的 Unix 主机，具备强大的调查能力。其特点是对正运行的主机活动进行分析，捕获目前的状态信息。

### 复习与思考题

1. 试述硬盘的物理结构和逻辑结构。
2. 了解磁盘上数据的具体存储方式。
3. 大致熟悉主流的取证软硬件。

### 拓展阅读书目

1. Eoghan Casey: “Digital Evidence and Computer Crime”, by Academic Press 2000
2. 段海新等译: 《计算机取证: 应急响应精要》 人民邮电出版社 2003 年版。
3. 常晓波译: 《应急响应计算机犯罪调查》 清华大学出版社 2002 年版。

## 第八章 电子证据取证相关技术概要及发展目标

### 一、数据获取技术

- (一) 对系统与文件的安全获取技术，避免对原始介质有任何破坏和干扰。
- (二) 对数据和软件的安全搜集技术，对磁盘及其他存储介质的安全无损备份技术。
- (三) 对已经删除的文件或破坏的系统的恢复、重建技术。

### 二、数据分析技术

在已经获取的数据流或信息流中寻找、匹配关键词或关键短语的技术。

- (一) 文件属性分析技术；
- (二) 文件数字摘要分析技术；
- (三) 日志分析技术；
- (四) 根据已获得的文件或数据的用词、语法和写作（编程）风格，进而推断其可能的作者的技术。（不仅仅是计算机技术）
- (五) 发掘同一事件的不同证据间的联系的分析技术。
- (六) 数据解密技术；
- (七) 密码破译技术；
- (八) 对电子介质中被保护的信息强行访问的技术。（如无需密码进入系统，系统漏洞）

### 三、电子证据取证的发展目标

(一) 电子证据进入并渗透人们生活的方方面面，传统犯罪活动逐步向数字化信息化的形式发展。电子证据取证从技术上要能够追踪最新的发展，能够对新型的犯罪手段和形式给与有效地遏制；同时从操作规程上满足法律法规对它的程序性要求，实现科学性和法律性的统一。

(二) 电子证据取证的发展目标和信息安全技术相结合，逐步建立完善的取证结构体系；网络协议的设计过程就应充分考虑对未来取证的需要，为潜在的取证活动保留充足信息；结合人工智能、机器学习、神经网络和数据挖掘技术的使用开发出更为简单通用的取证工具。

