第 1 讲

电子证据如何讲故事————以网络犯罪案件为例

主讲人介绍

刘品新，现任中国人民大学法学院教授、博士生导师，兼任中国人民大学刑事法律科学研究中心副主任、法学院证据学研究所副所长、智慧法律科技创新研究中心主任、网络犯罪与安全研究中心执行主任。研究领域为证据法学、电子证据法、网络法学、网络犯罪治理、智慧司法。长期致力于法学与信息科学的交叉研究，撰写了《电子证据法》《网络法：原理、案例与规则》等著作。

讲座主题

电子证据是网络犯罪司法的基石，其奥秘在于科学地还原案件事实。作为一种信息量极大的证据，电子证据可以依靠内在属性、关联痕迹、证据组合、印证体系、“鉴——数——取”体系、两个空间对接等原理查明和证明案件事实。面对变幻莫测的网络犯罪，法律工作者应当解剖案例细节，沟通刑法、证据法与信息技术知识，培养专业办理高科技犯罪案件技能。

讲座内容

一、引言

法学大师边沁说过，证据是正义的基石。现在，我想说，电子证据是网络犯罪司法的基石！如果法律工作者不能搞懂善用电子证据，那么形形色色的网络犯罪就难以得到有效治理。相关的理论创新、制度建设、服务工作、人才培养等也会受制于“网络空间究竟发生了什么”等现象不明的问题。我们形成这一认识，很大程度上受到了何家弘教授早年断言的启发。

“就司法证明方法的历史而言，人类曾经从神证时代走入人证时代，又从人证时代走入物证时代，也许，我们即将走入另一个司法证明时代，即电子证据时代。”这是何家

弘老师在主编《电子证据法研究》时给我们讲的金句。现在看来，人类社会确实走向了“电子证据时代”。至少在网络犯罪司法领域中，“电子证据，为证据之王”是个现实。

我们通过调研发现，证据难题是网络犯罪司法的极大障碍。网络犯罪司法的证据难题主要包括：（1）如何指向和证明真正的作案人，即“工具人”问题；（2）如何证明情节严重，即“数数”问题；（3）如何有效审查指控证据，打造证据体系，即“证据审查虚化”问题；（4）如何实现罪刑均衡，精准地惩治和威慑网络犯罪，即“法定入罪门槛低、实际量刑缓刑多”问题。关于这些问题，我们也写了一些小文章发表、小报告提交。我们还发现，对于网络犯罪司法中的电子证据，公安司法人员、律师、鉴定人员等虽然遭遇了各种具体挑战，但总体来看“网络犯罪司法的电子证据问题趋于稳定”，归结为“如何取”“如何审”“如何用”三点。由此可见，要破解“网络犯罪证据难题”，就需要在“取”“审”“用”电子证据方面着力。

这三“点”归结起来就是一个中心任务，即如何有效使用电子证据进行网络犯罪案件事实的重建。为什么这么说呢？中国人民大学法学院教授李学军和朱梦妮同学的学术研究，给了我们这样的学术支撑。她们在《意见证据制度研究》一书中，归纳了培根和密尔的观点，揭示出“证据就是痕迹”的本质。大家知道，“痕迹”是一个很有意思的概念，它是“过去”留给“今天”的、是“今天”留给“将来”的，据此可以反推发生了什么“故事”。在侦查学领域，人们经常说侦查 / 办案就是“考古”，是通过查找各种“痕迹”进行“考古”，因此整个侦查 / 办案过程主要就是“案件事实重建”的过程。套用这些理论，电子证据就是“数字式痕迹”，网络犯罪司法中使用电子证据必须聚焦于“数字式案件事实重建”（Digital Event Reconstruction）。其实，“数字式案件事实重建”是西方法学领域中持续热络的一个研究主题。简单地说，它强调将电子证据看成一个信息“场”，由电子证据将案件事实的来龙去脉娓娓道来。这一“重建”也可以称为“电子证据重建”。它与人类社会出现的“人证重建”“物证重建”是一脉相承的，展示的威力更巨大。

本次讲座的正标题为“电子证据如何讲故事”，就是阐述如何用电子证据重建案件事实；副标题确定为“以网络犯罪案件为例”，可以理解为本次讲座要顺便讲讲我们团队参与办理网络犯罪案件的点滴事迹和一些感悟。

二、原理

掌握依靠电子证据重建网络犯罪事实的技能，需要了解电子证据的一些基本原理，包括准确认识电子证据、有力揭示网络犯罪中电子证据的特色和求助于合格的指导性理论。

什么是电子证据？最高人民法院、最高人民检察院、公安部发布的《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》给出了如下定义。其第 1 条第 1 款规定：“电子数据是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。”第 1 条第 2 款规定：“电子数据包括但不限于下列信息、电子文件：（一）网页、博客、微博客、朋友圈、贴吧、网盘等网络平台发布的信息；（二）手机短信、电子邮件、即时通信、通讯群组等网络应用服务的通信信息；（三）用户注册信息、

身份认证信息、电子交易记录、通信记录、登录日志等信息；（四）文档、图片、音视频、数字证书、计算机程序等电子文件。”第 1 条第 3 款规定：“以数字化形式记载的证人证言、被害人陈述以及犯罪嫌疑人、被告人供述和辩解等证据，不属于电子数据。确有必要的，对相关证据的收集、提取、移送、审查，可以参照适用本规定。”这是一个非常宽泛的定义，而且具有一定的开放性。可以说，一切“数字式信息”都有可能用作网络犯罪司法的证据。

那么，网络犯罪中电子证据的特色有哪些？这一问题主要是相对其他证据，相对其他案件而言的。吕宏庆同学曾经整理了国内外相关文献，概括出法律界不同人士提出的“技术依赖性”等五六十种说法，还被拿到人民大学的课堂上讨论。现在看来，这里概括的很多“特色”是似是而非的，至少是极富争议的（如“无痕性”）；很多“特色”是没有针对性的，不能将电子证据同传统证据区分开来（如“技术依赖性”）。在网络犯罪司法的语境中，我们强调的是电子证据具有“超容性”，也可以说是“巨量性”。下面我以这次讲座的海报发布过程中的“小插曲”为例进行说明。

这期讲座发送第一次海报时出了点小差错，主要是在微信公号发布的“推送摘要”一栏中，将举办日期写成了“1 月 18 日”（事实上的举办日期是 8 月 18 日）。假设我们要查清真相，那会是一个什么情形呢？我请郭树正同学做了一下简单检测，发现公号的第一次发送行为不仅产生了一个“公号消息”页面，同时也产生了很庞杂的信息，包括“本地留存信息”（如发布内容的数据、配图数据、关注者的数据、加密日志数据、加密数据库数据等），“网络数据”（如大量数据流、动态缓存、本机 IP、网卡地址、服务器 IP、网卡地址等），“网络服务提供商服务器”（如发布内容的数据、缓存数据、网络数据中包含的数据等）。这些“巨量”数据虽然不都是可以获得或者解读的，但至少部分数据可以获得并解读，也就构成了还原海报小差错事实的电子证据基础。

那么，如何处理网络犯罪中超容或巨量的电子证据呢？这显然离不开科学理论的指导。我们认为，可以选用原子主义与整体主义证明模式的理论。它们是不同认识理论在司法领域的呈现。

依照原子主义证明模式理论，办案人员应当对电子证据尽可能地进行拆解细分，将其分解至最小单元————“原子”的程度。当然，这里的“原子”是指“逻辑认识的原子”，不是“物理分析的原子”。英国哲学家伯特兰 • 罗素说过：世界是一个由许多孤立的逻辑原子或原子事实构成的逻辑结构。逻辑原子主义虽然最早由罗素提出，但他明确表示这个思想是对维特根斯坦思想的阐明。罗素明确承认：“这些讲稿在很大程度上是关于我从我以前的学生、朋友——路德维希 • 维特根斯坦那里得到的某些观点的阐明。”在维特根斯坦的一生中，罗素是一个非常特殊的人物。他是维特根斯坦的老师，并且始终因结识维特根斯坦而庆幸。他在自己的著作中不止一次地向维特根斯坦致谢。他说，“结识维特根斯坦是我一生中最激动人心的思想遭遇之一”。有的学者认为他们之间的“情投意合”之处就在于信仰逻辑原子主义，并且都是它的创始人。逻辑原子主义是分析哲学的一个重要分支。分析哲学的基本思路是：希望分析出一个命题或事物的组成要素，再把各要素的组成要素进一步展开。也就是要追溯至最简单的组成要素。逻辑原子到底是什么？这

很难讲清楚，维特根斯坦不会告诉你什么是逻辑原子，罗素是比维特根斯坦经验主义倾向更严重的一个人，所以他说逻辑原子，就是最基本的东西，就是我们观察世界最小的那个单位，比如最小的视觉单位（色块或色点）、感觉材料。这种论述方式其实是一种经验主义论述方式。维特根斯坦不主张告诉人们逻辑原子是什么，因为他认为最小的东西是什么这个问题是由科学家去研究的，哲学就告诉人们必须抓住最小的那个东西，并从那个东西出发展开知识体系。于电子证据定案而言，当下通常可以将电子证据的内在属性、关联痕迹、复合内容析解出来，以查明、证明网络犯罪案件事实。

依照整体主义证明模式理论，办案人员应当尽可能地将不同的电子证据、电子证据与其他证据结合起来，构成一个整体，用以查明、证明网络犯罪案件事实。维特根斯坦指出：世界是由许多“状态”构成的总体，每一个“状态”都是一条众多事物组成的锁链，它们处于确定的关系之中，这种关系就是这个“状态”的结构，也就是我们的研究对象。于电子证据定案而言，当下通常可以将电子证据的组合、印证体系、鉴——数——取体系、两个空间对接拼接起来，以查明、证明网络犯罪案件事实。从理论上讲，电子证据的组合、印证体系、鉴——数——取体系、两个空间对接这几个概念可能有重叠，但在实务中已经区分开来。

假如法律工作者能够在办案中适用先进的理论指导电子证据“讲故事”，并坚持和提升形成一种行动自觉，那就会掌握很多的实务技巧。

三、技巧

电子证据的原子主义与整体主义证明模式如何落地？这里不仅要考虑证据法知识、侦查学知识与信息科学知识的有效融合，也需要同刑法学知识相结合并产生火花。

（一）原子主义证明模式的技巧

原子主义是一种暗喻的说法。在大千世界，从物质到分子再到原子，颗粒越来越细。这反映了一种解构对象以加深对客体认识的思路。电子证据最细的颗粒是 0、1 的信号，但目前尚无用于司法实践的价值。我们认为，用作电子证据证明的逻辑原子现阶段可以界定为如下三个方面。

1.“内在属性”讲故事

电子证据的内在属性是数据生成、存储、传递、修改、增删而形成的时间、制作者、格式、修订次数、版本等信息。其作用在于证明数据的来源和形成过程，即讲述关于数据如何得来的“故事”，如电子邮件的制作人、发件人、收件人、传递路径、日志记录、文档本身的属性等，数码照片的拍摄机器、拍摄时间、拍摄地点、光圈快门等属性。简单地说，内在属性主要就是由鼠标点击某电子文件看到的信息。比如，在一张图片中，图片展示的是电子邮件的邮件头文件，其中就有很多属性信息，最重要的是发送邮件的 IP 地址信息等，这也能揭示出邮件发送、收到的情况和时间差等。

我们以快播公司传播淫秽物品牟利罪一案为例进行详细解读。在该案中，行政执

法人员于 2013 年 11 月 18 日查获了快播公司托管的四台服务器，后公安机关从中提取到 21 251 个淫秽视频文件（qdata 格式文件）。这些服务器和淫秽视频文件是重要的证据，案件中产生了关于视频文件真实性的争议。核心争议是这些淫秽视频文件是否是被人“移植”进服务器的，即服务器是否被污染。最后，法院委托鉴定机构进行了重新鉴定。鉴定人员得出的鉴定意见是：“经对四台服务器内现存快播独有视频格式文件 qdata 文件属性等各类信息的检验分析，没有发现 2013 年 11 月 18 日后从外部拷入或修改 qdata 文件的痕迹。”这一意见中的关键词是“qdata 文件属性”，也就是淫秽视频文件的“atime”“mtime”“ctime”等时间属性信息未发现异常。本次讲座先不讨论这一鉴定意见是否可靠，仅就其得出意见的根据来看，就是基于淫秽视频文件的“内在属性”重建其形成过程。

再看一起注入漏洞破坏计算机信息系统罪的案件。在该案中，警方通过远程勘验进入了被入侵的服务器，下载获得了该服务器记载入侵行为的日志文件等数据。这一过程是远程勘验笔录记录的，其顺序也符合一般规律，即“先登录服务器，再从该服务器中提取数据”。该次远程勘验获取的“日志文件等数据”是案件中一份重要的证据。那么，这一证据获取过程是否属实呢？有关电子证据的内在属性信息可以揭示真相。一般验证方法是，审查远程勘验笔录所附光盘记录的电子证据——远勘笔录附件，即一步一步截图形成的截屏文件（照片文件），看其属性能否反映截屏的时间及先后顺序。例如，远程勘验第七步的行为截图“图七，登录 107.jpg”的时钟为 18:31，其截图保存时间为 18:32:06；远程勘验第八步的行为截图“图八，107D 盘 .jpg”显示的时钟却为 18:30，其截图保存时间为 18:31:28。两相比较，显然“图八，107D 盘 .jpg”早于“图七，登录 107.jpg”形成。这是异常的，反映远程勘验笔录所反映的顺序不属实。这个远程勘验是否有效也会产生疑问了。这个例子给了法律工作者一个很好的启发，就是大家可以通过注意审查勘验、远勘、检查、侦查实验、鉴定所附的工作截图文件，来重建各种取证工作的全过程，审查控方取证的真实性。诚若如此，这将是倒逼警察取证规范化的一个重要举措。

在这起注入漏洞破坏计算机信息系统罪的案件中，警方还对被告人用于获利的记账数据——××× 的淘宝账户的“订单报表”数据进行了提取，使用的也是远程勘验方式。远程勘验笔录表明，警方于 2015 年 6 月 9 日远程勘验 ××× 的淘宝账户得到了“ExportOrderList 201506091451- 订单报表 .xls”。那么，事实上是不是这样呢？我们可以对所附光盘中淘宝账户“订单报表”数据——“ExportOrderList 201506091451- 订单报表 .xls”的内在属性进行核验。该“ExportOrderList 201506091451- 订单报表 .xls”的“最后一次保存时间”是 2015/6/11 15:05，尽管其“创建内容的时间”显示为“2015/6/9 14:56”。这就意味着，警方在远程勘验完成之后对该文件于 2015/6/11 15:05 实施了操作行为。一个合理的猜想是，警方或其他人很有可能进行了增、删、改。在该案中，我们要求法庭进行了当庭验证，即当庭登录 ××× 的淘宝账户重新进行远程勘验——也就是远程下载，进一步发现“利用淘宝账户的批量导出功能，仅能生成属性为 .csv 格式的数据文件”，根本不产生 .xls 格式的文件。这佐证了我们的前述猜想。

在这起案件中，由于有较多电子文件在内在属性方面出现了异常，我们后来对疑点较大的电子文件进行了“内在属性”全梳理，特别是对前后一对电子文件（指先后取证多次形成的对应电子文件）进行重点梳理。主要技巧是用专门的取证工具（Winhex）查看 Word 文档的创建时间、修改时间、访问时间信息，查到之后可以精确到“百纳秒”级别，再行匹配找疑点。如果前后一对电子文件的创建时间、修改时间、访问时间信息在同一“百纳秒”级别是一致的，那就表明它们是同源文件，即后一 Word 文档是利用前一 Word 文档修改而来，而不是另行取证得来。在文档的内在（时间）属性特点上，胡丞同学研究较早，很早就写了一篇关于电子证据时间属性的论文，得出了许多重要的学术结论。

依靠电子证据的“内在属性”重建案件事实，几乎是每位法律工作者都能完成的任务，关键是具体工作人员是否有这一方面的意识。

2.“关联痕迹”讲故事

关联痕迹是在电子证据形成之际同时产生的一些独立“痕迹”。电子证据本身是“痕迹”，“关联痕迹”可以说是电子证据之“痕迹”边上的“专门痕迹”。通常来说，计算机等设备在生成、存储、传递、修改、增删数据时会引发信息系统环境产生新的相关的痕迹。它们包括后缀为 *.lnk、*.dat、*.identifier、*.sys、*.tmp 的各种痕迹文件，这是信息科学领域的痕迹文件；它们也包括该数据在数据磁盘层的存储规律，这是物证技术学领域的“痕迹”。后一痕迹在理解上有些困难，我可以举个简单例子进行说明。我们在电脑中编辑 Word 文档时，通常会产生快捷方式文件、临时文件、office 日志文件、软件杀毒记录文件等，但假设彻底检查一台电脑时没有发现与所编辑 Word 文档相关的任何快捷方式文件、临时文件、office 日志文件、软件杀毒记录文件等。这一“发现”就是物证技术学领域的“痕迹”，一如杀人现场的“擦拭血迹”。孙玉龙同学撰写过《基于电子痕迹的人身同一认定》一文，该文对各种电子痕迹进行了界定、归类及规律提炼，并提出可以用于对犯罪嫌疑人等进行人身同一认定。大家可以用作参考。

在我们团队中，郭树正同学对电子痕迹的研究最为专业。他曾经对各种常见电子文件的“关联痕迹”反复做过实验，如绘制电子文档的痕迹图谱，按照实体性痕迹、工具性痕迹两大类，分为网络层、应用层、操作系统层、文件系统层等层面进行过列举。如果大家感兴趣，可以仔细研读“电子痕迹图”；如果大家对此尚不熟悉，可以看看 lnk 痕迹、tmp 痕迹、office 最近访问记录。对于网络犯罪司法而言，“数据交互痕迹”“网络缓存痕迹”“网盘痕迹”“软件使用痕迹”“邮件痕迹”等值得特别关注，其中有些可能属于动态痕迹。

再来看一下 DDoS（分布式拒绝服务攻击）攻击一案。其基本案情是，嫌疑人对某网站进行 DDoS 攻击导致网站崩溃，公司因赔付数千万元而倒闭。主要证据是嫌疑人所使用的电脑硬盘；特别情节是嫌疑人使用虚拟机技术。在这起案件的办理中，为了查清犯罪嫌疑人是如何攻击、敲诈的，办案机关曾经聘请一家社会鉴定机构的鉴定专家检验，但没有发现相关痕迹。后来，办案机关委托到中国人民大学物证技术鉴定中心——我们团队的一个平台，由谢君泽同学组织开展鉴定并取得突破。他们通过取证工具分析虚拟磁盘，发现

其中存在大量的数据交互记录，证明嫌疑人向被害单位所使用的 IP 地址发动 DDoS 攻击；他们在电脑空余空间中发现嫌疑人敲诈勒索的聊天记录碎片文件，证明嫌疑人曾于发动网络攻击后向被害单位实施敲诈勒索行为；他们在电脑空余空间中发现嫌疑人所使用的 VPS（即搭建 VPN 的服务器）服务器碎片文件，证明嫌疑人发动网络攻击所使用的中转服务器……最终，我们团队基于这些痕迹制作了 DDoS 攻击与敲诈勒索案大事表，包括嫌疑人开始学习黑客攻击技术、嫌疑人锁定受害公司、嫌疑人对受害公司实施 DDoS 攻击行为、嫌疑人对受害公司实施敲诈勒索行为、嫌疑人被逮捕等环节。这个大事表就是很直接的案件事实重建了。

再举一起破坏计算机信息系统的案件。这次我们要讨论的主要证据是一张光盘，即警方对嫌疑人账号文件远程下载而制作的光盘。一般来说，办案实践中很多人不看数据光盘。但是，假如我们查看光盘，会发现什么痕迹呢？我想至少可以看到刻盘痕迹、刻盘记录。我们通过侦查实验发现，刻录光盘的文件系统多为 UDF 文件系统。在这个案件中，警方也是使用 UDF 文件系统刻制光盘。该文件系统存在如下特征：在十六进制下进行分析，发现“根目录”的“修改时间”信息即光盘刻录的时间，光盘内存在的文件其“修改时间”信息即该文件被修改时的时间信息，该信息并未因光盘刻录而变化，且该文件原来的修改时间会将其他时间信息覆盖。请大家注意两个时间信息，其中“根目录”的“修改时间”为 2014/11/20 09:12:33，表明该光盘刻制于 2014/11/20；（网监）勘［2014］006 号“附件光盘”文件的“修改时间”为 2014/10/28 14:52:00，表明该笔录成稿于 2014/10/28。经核对该案中远程勘验笔录后发现，警方进行远程勘验的文字记录时间为 2014/10/23 21:30。这些“关联痕迹”解释出了一个十分不正常的过程：警方于 10 月 23 日进行远程勘验，之后 5 天内（到 10 月 28 日）还对提取的电子证据进行过修改操作，之后又过了近一个月才刻制光盘。这是严重违反取证规则的，严重影响了电子证据的真实性。

我们再看一起提供侵入、非法控制计算机信息系统程序、工具罪的案件。这个案件是我和徐菲同学合作的成果。这个案子中的主要证据也是一张光盘，是关于警方在线提取电子证据的光盘。笔录表明，在线提取证据工作的完成时间是 2018-5-17 9:10；“在线提取数据”光盘显示“× × 数据库远程勘验 .zip”文件的“修改时间”为“2018-05-23 10:05:11”，远远晚于在线提取时间。那么，这张光盘中的电子证据还有法律效力吗？

还有一起侵犯公民个人信息罪的案件。现场勘验记录的勘验时间是 2018 年 1 月 10 日 16:53，而勘验光盘制作的时间是 2018 年 2 月 1 日 16:50:34。这一反常也是令人生疑的！检察官因为注意到勘验光盘文件中的修改时间反常，决定自行对警方提取的数据库文件进行审查。幸亏警方在进行远程勘验时提取了涉案服务器的镜像文件，这给检察官事后补证提供了基础。

依靠警方光盘留下的“关联痕迹”重建取证过程，虽然一个很简单的技巧，但足以揭示一种常见的违法现象。我们在一些地区调研时发现，实务中警方几乎都是在事后刻制取证光盘，甚至是到了必须将案件移交检察院的时候才刻制，这与法律要求的同步刻制是背离的。我提醒听课的警察群体纠正这个“潜规则”，提醒听课的检察官、法官、律师注意识别这个“潜规则”。总之，网络犯罪司法中，“光盘”容易“惹祸”，不可不察！

3.“复合内容”讲故事

“复合内容”是受“复合文档”的启发而形成的一个概念。复合文档不仅包含文本，还包括图形、电子表格数据、声音、视频图像以及其他信息。这是当前电子证据内容的普遍承载方式。例如，大家审视一封电子邮件，看到的只是类似传统信件内容的“书信”吗？当然不是！电子邮件证据，除了邮件正文，还有封装的内容。

我们来看一起破坏计算机信息系统罪的案件。这起案件中最重要的电子证据是警方在抓获嫌疑人之后，使用嫌疑人账号、密码登录其邮箱获得的几百封电子邮件。它们能够证明嫌疑人推广流氓软件及获利的情况。对于这样一份电子邮件证据，我们要注意其内容不仅包括每封邮件的正文，也包括邮箱收件夹、发送夹等文件夹中有多少邮件（即邮件列表），还包括该邮箱反映的“最近登录”（也称为“上次登录”）形成的时间、地点信息。本案中邮箱显示“上次登录”时间为“11/03 17:20:18”，显示“上次登录”地点为“湖北省”（这里是纸质版，如果有电子版还能够进一步查清楚上次登录的 IP 地址等）。这些附带的“复合内容”就揭示了警方违规取证的过程。为什么呢？经过核对笔录，发现警方远程勘验结束的时间早于这里显示的“上次登录”时间“11/03 17:20:18”。这说明，警方远程勘验笔录记录不实，或者警方反复多次进入该邮箱而没有如实记录，也没有如实保全证据。这个案子在开庭时，我向法庭说明了这封邮件的“复合内容”——“上次登录”时间信息异常。公诉人回应说，可能远程勘验笔录写错了“远程勘验结束的时间”。我作为辩护律师回击说：不可能是这样的，因为这张图还显示了“上次登录”地点为“湖北省”，而被告人是外地人，被抓之前没有到过湖北。法官当时问被告人：那一天你在哪里？是否到过湖北上网？被告人回答：那时我已经被关在湖北的看守所了。可见，电子文件的内容不像我们看到的一张纸那么简单。对其内容挖掘越多、越深，我们的收获就越大。

我再补充一起关于电子邮件转发的案件。邮件转发是司空见惯的事情，一封邮件被转发后，就会一环套一环，形成多封邮件合一的效果。对于这样的邮件，大家要挖掘其中所附的原发邮件、回复邮件、转发邮件等，包括内容正文、发件人、收件人、回复人、转发人、抄送人等内容。在这里，我会特别提醒大家可以从中挖掘出所附的“广告信息”。该案件的转发邮件中有个完全一样的“广告信息”，这是不正常的。我们在法庭上要求当庭登录有关邮箱账号进行查看，结果发现涉案邮件对不上，邮件证据涉嫌重大造假。法庭最终排除了相关电子邮件。

回到前述提供侵入、非法控制计算机信息系统程序、工具罪一案。其中有一份电子证据是远程勘验笔录及数据。我们发现笔录的复合内容不仅写明了何人、何时、何地进行了勘验，而且注明了是使用密码“××××wangan2018”进行在线提取。这一密码显然指代网安警察，说明警方改了嫌疑人的密码，这就可能产生警方先进入嫌疑人服务器账号，后提取证据的怀疑。这一做法违反了公安部《公安机关办理刑事案件电子数据取证规则》第 33 条的规定：“网络在线提取或者网络远程勘验时，应当使用电子数据持有人、网络服务提供者提供的用户名、密码等远程计算机信息系统访问权限。”我们挖掘出来的这一点内容，使得有关电子证据的真实性、合法性受到质疑。

以上就是原子主义证明模式的办案技巧。也就是说，我们要尽量“细化”“揉碎”电子证据，“挖掘”不为人知的微观信息用于还原案件事实。那么，具体能够将电子证据“细化”“揉碎”到什么程度？我的理解是进行二进制数据查看：对每一个电子文件都要分析文件头、文件中间、文件尾；对每一存储介质都要分析各个分区，特别是未分配空间。这是一种理想状态，实现这一点还有很长的路要走。但是，当下司法实践中法律工作者漠视电子文档、光盘、硬盘等介质的属性（往往只看笔录或打印出来的纸面材料），是极不合理的。

（二）整体主义证明模式的技巧

整体主义证明模式的逻辑要求：一个特定证据作为分析对象的证明价值，从根本上取决于其他所有证据。这一理论很容易同我国的证据组合、体系、锁链和印证等说法勾连起来。这一联想是有道理的。但是，电子证据遵循整体主义证明模式的改造，也会产生独特的火花。

1.“证据组合”讲故事

“证据组合”是将能够支撑或反驳某一个案件事实的不同来源的证据结合在一起的思路。例如，为了证明犯罪目的，可以将相关口供、证人证言、书证同有关电子证据（主要是聊天类电子证据）汇总起来。这是不同形式证据的组合。对于电子证据而言，构成证据组合还有新的优势和切入点。这是因为同一份电子证据往往在不同层面呈现，人们可以打造不同层面证据的组合。

我们团队技术导师戴士剑是我国数据恢复学科的奠基人。他在早年帮助我办理的一起案件中展示了这种新方法。那是一起通过电子邮件获取商业秘密的案件，主要证据是一些带有扫描合同的电子邮件。为了还原通过电子邮件获取商业秘密的案件事实，戴老师绘制了网络行为图，表明一个完整的电子邮件行为会在网络层、应用层、操作系统层、文件系统层、物理层等留下证据，分别是电子邮件、PDF 合同文件、操作系统日志、文件操作日志、纸面合同证据或履约证据，从各层进行遴选组合就能完成任务。现在看来，虽然这种“网络行为图”的细节还有需要完善的地方，但是这一思路本身的确具有宝贵的价值。当时，我们顺着这个新思路扩大寻找证据的空间，确实收集到了足以构成“组合”的、丰富的电子证据。

试举一起破坏公用电信设施罪的案件。案情是，犯罪嫌疑人于 12 月 8 日至 10 日，在公众场所使用短信群发设备进行短信群发，向周围手机用户强行推送短信。嫌疑人于 12 月 10 日下午 2 点被刑事拘留。证明这样一种伪基站犯罪行为主要依靠电子证据。警方将其微基站设备（电脑）送检后，发现其系统时间归零了，无法确定哪些或哪一推送短信记录是嫌疑人在案发过程中留下的。通常，微基站设备中推送短信记录有很多条，要排查哪些是嫌疑人的行为产生的，哪些是其他人如电脑上家的行为产生的。对于这样重要的案件事实，无法依靠电子证据（日志文件）及相关鉴定意见证实，那怎么办？承办人员一方面对嫌疑人进行补充讯问，问清楚嫌疑人推送短信的精确内容是什么；另一方面调整鉴定请求，改为鉴定微基站设备中推送上述内容短信的日志记录“造成多少部手机通信中断”。

这样一来，电子证据、鉴定意见与讯问笔录（口供）就构成了一个有效的证据组合。

2.“印证体系”讲故事

“印证体系”指的是同一网络行为产生了若干份电子证据，特别是不同网络节点的多份电子证据，它们相互印证构成虚拟空间中的一种独特证据锁链。这些电子证据往往是同一行为或关联行为产生的。我们常说，发送电子邮件会在发件人电脑、发件人邮件商的服务器、收件人电脑、收件人邮件商的服务器等多点留下电子邮件；同理，发送短信、微信等都会产生可以相互印证的网络证据。将这些网络证据匹配起来，审查其内容是否一致，特别是审查相关时间信息、地址信息等是否正常，就可以还原整个网络行为事实。

试举一起网络诈骗罪的案件。该案是熟人之间的微信诈骗案件，在这一案件中，究竟该如何判断发生了什么？最有效、最简单的方法就是将不同手机中的微信聊天记录进行对照，按照逐条微信的发送时间、收到时间编排大事表，必要时还要查看微信登录日志（“登录设备管理”信息等）。我们查看这起案件的微信记录后，很快判断出嫌疑人通过编造“算命先生”等虚假身份进行诈骗，诀窍就在于制作了“基于微信印证体系构建大事表”。我们团队还在其他案件中制作过基于系列照片印证体系的大事表、基于电子邮件印证体系的大事表等。这些工作很多是毛自荐老师协助的。她的感受是，难倒不难，但很有意义。

再举一起通过网络泄露国家秘密罪的案件。案情是，嫌疑人通过互联网将一份重要的“国家秘密”文件传送到境外。侦查开始前嫌疑人对电脑进行了擦写。最后，专案组除了获取了泄密文档，还在电脑中获取了嫌疑人将泄密文档敲打成电子版本留下的输入法碎片文件、发送短信留下的碎片、跟同事进行 QQ 聊天留下的碎片，后来还顺藤摸瓜向邮件服务商调取了涉案期间的电子邮件。它们构成一个良好的印证体系，特别是系列 QQ 聊天记录（碎片）证明了嫌疑人的犯罪主观方面。

3.“鉴——数——取体系”讲故事

司法实践中，从来没有一起案件中只有孤立的电子证据的情况。我们观察，网络犯罪司法的主打证据体系往往表现为一种独特的电子证据结构，即由电子证据、“来源笔录”与鉴定意见组成的三位一体构造。在这里，“数”指的是电子证据，通常不是孤立地发挥证明作用；“取”指的是各种“来源笔录”；“鉴”指的是电子数据司法鉴定意见等，用于证实案件争议事实。三者结合形成一个稳定的架构，用于证明网络犯罪的主要案件事实。其中，直接证明案件事实的往往是“鉴”，而“鉴”是否可靠有效取决于“取”的支撑和“数”的验证。

回到前述提供侵入、非法控制计算机信息系统程序、工具罪一案。该案需要证明的基本事实是，被告人提供的软件是否属于侵入、非法控制计算机信息系统的程序、工具。案件中控方委托鉴定机构出具的一份鉴定意见书表明，该“×× 软件利用 ×× 服务器实现 ×× 登录，具有获取 ×× 相关信息、上传设备信息和用户账号密码的功能，这个功能突破了计算机信息系统的安全保护措施，未经授权获取了计算机信息系统的相关信息，属于侵入 ×× 系统的程序”。这些鉴定意见言之凿凿，是否就足以证明案件事实呢？

本案必须审查对应的“数”证据，即鉴定意见所使用的检材。经核查发现，上述鉴

定意见书使用了 9 份检材，可以分为四大类，包括压缩文件“××V8085.rar”、证人手机中的文件“××1.rar”、侦查实验文件及被害人提供的“480800××apk.rar”文件。其中，最重要的指控证据是压缩文件“××V8085.rar”，它被认为是被告单位对外提供的。从表面来看，这些检材不是一个“软件”，那就要判断它们与被告单位的关系以及来源等真实性问题。

这就提示本案要配合审查对应的“取”证据。经核查发现，虽然鉴定意见书表明最重要的证据“××V8085.rar”源自被告单位的一位技术员工的个人电脑，但勘验笔录反映不出来这一事实（只反映出有另一个名为“××_kks.rar”的文件，而经过解压缩没有发现前述文件）；同时，虽然鉴定意见书表明“480800××apk.rar”文件是被害人提供的，但案卷中无任何笔录证明这是被告单位的软件。

在本案中，将这三者————“鉴”“数”“取”结合起来，就发现它们根本构不成证据体系。换个角度来说，它们至多构成一个千疮百孔的证据体系。我们在开庭过程中，询问鉴定人“送检程序”跟被告单位的关系，鉴定人说“我不清楚，也不管”；我们问出庭的警察，“送检程序”是哪里来的？警察回答，不是从被告单位扣押的完整软件，也不是来自第三方从被告单位接收的完整软件，主要是源自被告单位的一位技术员工的个人电脑。对于勘验笔录中没有记载这一程序，警方表示是疏忽，但确实是有这样一份文件。后来，控方竟然补充提交了一份新的勘验笔录，表明重新勘验到了这样一份文件。这次重新勘验合法有效吗？我们仍然从“鉴”“数”“取”进行体系性审查，结果发现并没有重新勘验，更发现这个硬盘自第一次勘验后没有封存，存在数据植入的可能。这个案子的庭审质证很精彩，大家可以看看庭审录像，领略我和徐菲同学的交叉询问艺术（http://tingshen.court.gov.cn/live/9719853）。最后，一审法院作出认定：“本案中司法鉴定意见书不应作为定案的根据。”

4.“两个空间对接”讲故事

一般来说，电子证据对应信息空间，传统证据对应物理空间。如果我们能够基于电子证据还原虚拟空间的轨迹，基于传统证据还原物理空间的轨迹，将两个空间的人员轨迹对接起来，就能神奇地还原案件事实。这就是“两个空间对接”的技巧。我们团队中张杨杨同学一直钻研各种数据库记录定位的方法，他很早就发现淘宝等各种购物 App 获取用户轨迹的数据。当然，这些数据均可以用于查明和证明网络犯罪，解决证明网络犯罪行为究竟是谁实施的难题。

回到前述破坏计算机信息系统罪一案。该案的重要指控证据是一份鉴定意见，能够用于证明被告人获利达到 70 多万元。这份证据证明的事实准确吗？当时，我们进行了简单的“两个空间对接”：一是查到案件中有一份“情况说明”，表明被告人使用 ADSL 连接互联网犯罪共使用了 100 多个“×× 市”的相关网络 IP，比对鉴定意见书记载的检材发现“使用 SQL 语句注入漏洞的行为共涉及 3 440 个 IP 地址，其中被告人住所地 IP 地址 1 805 个，外地 IP 地址 1 603 个”。这就说明，虚拟空间的位置信息证据表明有其他人作案的可能性。二是核查言词证据等，确定被告人在案发期间没有离开当地。这样一来，电子证据反映的作案人轨迹同传统证据反映的被告人轨迹不一致，一大一小，就说明存在其

他人犯罪的极大可能。相应地，鉴定意见书将获利 70 多万元全部归到被告人头上，也是错误的。

我在许多场合称赞过最高人民检察院发布的第 39 号指导性案例——朱炜明操纵证券市场一案。这是一个非常有价值的“两个空间对接”案例。2013 年 2 月 1 日至 2014 年 8 月 26 日，被告人朱炜明在任国开证券营业部证券经纪人期间，先后多次在其担任特邀嘉宾的《谈股论金》电视节目播出前，使用其实际控制的三个证券账户买入多只股票。于当日或次日在《谈股论金》节目播出时，以特邀嘉宾身份对其先期买入的股票进行公开评价、预测及推介，并于节目首播后一个至两个交易日内抛售相关股票，人为地影响前述股票的交易量和交易价格，获取利益。经查，其买入股票交易金额共计人民币 2 094.22 万余元，卖出股票交易金额共计人民币 2 169.70 万余元，非法获利 75.48 万余元。审查起诉阶段，朱炜明辩称：（1）涉案账户系其父亲朱某实际控制，其本人并未建议和参与相关涉案股票的买卖……检察机关审查认为，犯罪嫌疑人与涉案账户的实际控制关系，公开推介是否构成“抢帽子”交易操纵中的“公开荐股”以及行为能否认定为“操纵证券市场”等问题，有待进一步查证。针对需要进一步查证的问题，上海市人民检察院第一分院分别于 2017 年 1 月 13 日、24 日两次将案件退回上海市公安局补充侦查，要求公安机关补充查证犯罪嫌疑人的淘宝、网银等 IP 地址、MAC 地址（硬件设备地址，用来定义网络设备的位置），并与涉案账户证券交易 IP 地址做筛选比对；将涉案账户资金出入与犯罪嫌疑人个人账户资金往来做关联比对；进一步对其父朱某在关键细节上做针对性询问，以核实朱炜明的辩解。

简单地说，两种证据表明，在朱炜明出差期间涉案账户使用了其出差城市 IP 地址做证券交易，在朱炜明不出差期间涉案账户使用了其办公室 IP 地址做证券交易；而这些地址是其父不可能使用的。

以上就是整体主义证明模式的办案技巧。也就是说，我们要尽量将电子证据与其他证据进行整合，搭配搭建各种有效的证据组合、印证体系、“鉴——数——取”体系、两个空间对接等结构，以宏观的视角还原案件事实。当下，司法实践中对电子证据如何整理探索不多，经验不够，值得反思。

四、结论

网络犯罪是当今各国面临的时代挑战，电子证据是科技催生的秘密武器。本次讲座初步展示了网络犯罪司法借助电子证据进行重塑的实务经验、支撑理论和现实规律。归结起来，如图 1-1 所示，我们称之为“以电子证据切入改进网络犯罪司法”的知识图谱（或一把钥匙）。希望读者能够产生钻研的兴趣或者批判的冲动。

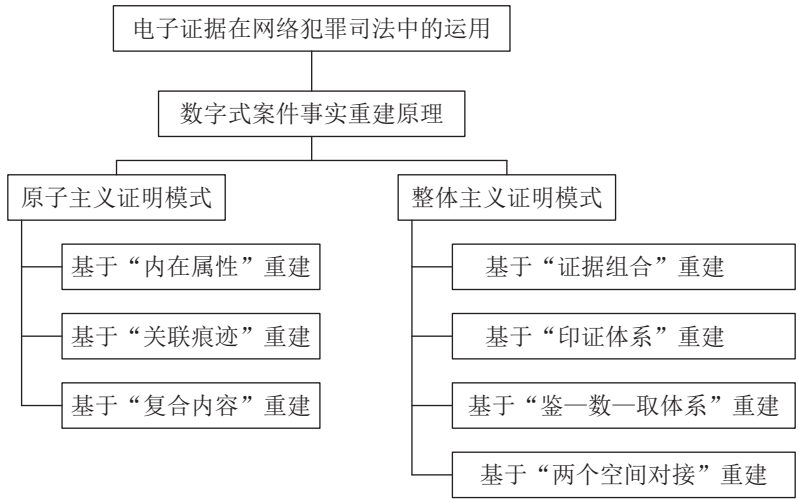

图 1-1　以电子证据切入改进网络犯罪司法

20 多年来，我研究电子证据的心得是：尽量弥补不同专业知识之间的沟壑。在向网络犯罪研究转型过程中，我更感受到寻找跨界桥梁的重要性。其中道理，只可意会，不可言传。我建议，主管部门（高检院）可以在这一方面做更多更好的推动，像美、加、英等国出版的《网络犯罪公诉指引》等手册，中国也该酝酿推出自己的版本了，并不时更新。