工商网络交易监管及电子数据证据取证培训教材

国家工商总局网络商品交易监管司

电子数据取证分析技术

系列丛书

中国工商出版社

电子数据取证分析技术

国家工商总局网络商品交易监管司　编

中国工商出版社

责任编辑/李轶群　于成龙
封面设计/慧　子

图书在版编目(CIP)数据

电子数据取证分析技术 / 国家工商总局网络商品交易监管司编.
—北京:中国工商出版社,2014.11
ISBN 978-7-80215-755-2

Ⅰ.①电… Ⅱ.①国… Ⅲ.①计算机犯罪—数据收集—研究—中国
Ⅳ.①D924.364

中国版本图书馆 CIP 数据核字(2014)第 257565 号

书名/电子数据取证分析技术
编者/国家工商总局网络商品交易监管司

出版发行/中国工商出版社
经销/新华书店
印刷/北京海纳百川印刷有限公司
开本/680 毫米×960 毫米　1/16　印张/24.75　字数/380 千
版本/2014 年 12 月第 1 版　2014 年 12 月第 1 次印刷

社址/北京市丰台区花乡育芳园东里 23 号(100070)
电话/(010)63730074,63725178　电子邮箱/zggscbs@163.com

书号:ISBN 978-7-80215-755-2/D476
定价:48.00 元

编委名单

主　编：刘红亮　国家工商总局网络商品交易监管司司长

副主编：杨洪丰　国家工商总局网络商品交易监管司副司长

王应涛　福建省工商局副局长

编　委：刘宝恒　国家工商总局网络商品交易监管司网络商品交易规范处处长

吴东平　国家工商总局网络商品交易监管司网络商品交易监管处处长

夏　超　国家工商总局网络商品交易监管司网络商品交易规范处干部

翟　泳　国家工商总局网络商品交易监管司网络商品交易规范处干部

余　华　福建省工商局市场处副处长

肖湘华　福建省工商局市场处主任科员

王粟洋　福建省工商局市场处科员

卿斯汉　中国科学院知识创新工程项目首席科学家，北京大学、武汉大学客座教授、博士生导师

许榕生　中国电子学会计算机取证专家委员会副主任委员，中科院高能物理所计算网络安全实验室首席科学家

丁丽萍　中科院软件所基础软件国家工程研究中心研究员，中国电子学会计算机取证专家委员会秘书长

秦玉海　东北大学博士生副导师，专业技术二级警监

王永全　华东政法大学刑事司法学院副院长兼信息系主任，中国电子学会计算机取证专家委员会委员
马国富　中央司法警官学院信息系实验中心副主任
马　丁　中国人民公安大学信息安全工程系副主任、教授、理学博士
孙国梓　南京邮电大学计算机技术研究所副所长，南京邮电大学计算机学院信息安全系副主任
陈　龙　重庆邮电大学教授、博士，CAAI 智能数字内容安全专委会委员，国际期刊 IJCS 编委
陈垂聪　厦门市美亚柏科信息股份有限公司副总经理
林远近　厦门市美亚柏科信息股份有限公司培训中心技术部经理
蔡菲娜　厦门市美亚柏科信息股份有限公司培训中心培训部讲师
王　菲　厦门市美亚柏科信息股份有限公司培训中心技术部讲师

序 言

近年来，网络商品交易以其成本低、覆盖面广、使用灵活、易于参与等优势得到了广大消费者的认可和青睐，成为人们日常生活中的重要消费方式，在释放消费需求、拉动经济增长、扩大社会就业、转变经济发展方式等方面发挥了重要作用。但与此同时，由于网络的虚拟性、开放性、跨地域性的特点，网络市场在发展过程中也出现了一些不容忽视的问题，制假售假、不正当竞争、虚假宣传、网络传销等违法行为时有发生。这些问题影响了网络市场环境，扰乱了网络经济秩序，成为阻碍网络市场健康持续发展的重大瓶颈。加强网络交易监管，维护网络交易正常秩序，保障网络交易安全和消费者合法权益，是工商机关在网络时代肩负的神圣使命和重要职责。

网络商品交易通过电子数据传递信息，网络商品交易及相关服务的全过程也以电子数据的形式来记录和保存。虚拟的电子数据具有分散性、隐匿性、易被篡改的特点，电子证据通常具有外在实体上的无形性、表现形式的多样性和易灭失破坏性。因此，收集固定网络交易的电子数据证据，是网络交易监管执法的重要前提。如何科学规范地收集、固定电子数据证据并确保其证据效力，成为工商机关切实履行网络交易监管职责时不可回避的重大课题。

国家工商总局于2011年专门下发了《关于工商行政管理机关电子数据证据取证工作的指导意见》（工商市字[2011]248号），对电子证据的定义、取证原则、取证方式、取证程序，以及询问笔录和检查查封的具体要求作出了规定。但基层工商机关在电子取证执法实践中仍然面临电子证据提取手段匮乏、办案人员技术水平有待提高等诸多困难，在办理网络案

件时难以在第一时间提取和固定网络违法证据，经常陷入“看得到”却“拿不到”，甚至因法律无法认定而导致证据失效，让违法者逍遥法外的窘境。

为进一步加大电子数据证据取证相关业务知识的普及和培训力度，增强并规范工商行政管理机关电子数据证据取证工作，国家工商总局网络商品交易监管司组织编写了工商网络交易监管及电子数据证据取证培训系列教材。系列教材由《网络交易规范和监管》、《电子数据检查及证据固定》、《电子数据取证分析技术》、《移动互联网及手机取证技术》组成，系统介绍了网络商品交易监管特别是电子数据取证工作的理论背景、法律依据与实践经验，为各级工商网监机构开展业务培训提供了有益范本。以系列教材的出版为契机，大力开展网络商品交易监管业务培训，打造一支熟练掌握相关法律法规、信息网络技术、工商行政管理实践经验的工商网络交易监管复合型人才队伍，将会有力地提升工商机关网监队伍的履职能力和监管效能，实现从传统实地市场巡查模式向利用现代信息技术“以网管网”的转变，以更加规范有力的网络商品交易监管执法工作，为中国网络市场健康持续发展保驾护航。

甘霖

2014 年 10 月

前 言

伴随着企业无纸化办公和电子商务的产生与发展，计算机成为企业在经营过程中不可或缺的办公工具，越来越多的证据以电子数据形式存放在办公电脑中。以“天津第一口奶事件”为例，记者就是以某奶粉供应商记账明细电子表格为突破口，调查出奶粉供应企业与所有医院医生之间的商业贿赂往来。所以，分析涉案电子数据，获得相关电子数据证据对于案件的办理显得尤为重要。

电子数据取证分析技术，是从海量数据中获取与计算机违法经营或犯罪有关的证据，进行相关性分析与研究，借助高效率的搜索算法、完整性检测算法、数据挖掘算法等技术快速有效进行数据分析和取证。国内外的取证分析软件也是围绕这些取证技术方向进行探索和研究。

本书立足电子数据取证实用分析技术，首先介绍电子数据取证的相关基础概念、常见国内外取证分析工具，然后分别阐述实用分析技术，包括Windows 取证技术（主要介绍自动取证分析）、文件分析技术（文件签名及散列值在取证中的应用）、内容匹配技术（文件过滤与关键词搜索）、Web 服务器取证分析、数据恢复及关联分析技术，以典型案例形式介绍了取证分析的实战经验，力求深入浅出地向读者阐述取证分析思路与技巧。

全书共分七章，主要内容如下：

第一章　介绍电子数据取证基础，主要包括文件系统及取证专业术语解释、国内外常见取证分析工具、电子数据取证分析方法及注意事项。

第二章　介绍 Windows 取证技术，包括注册表分析、上网痕迹分析、电子邮件分析、即时通信软件分析、日志分析及回收站分析、加密文件检测、反取证软件检测、打印脱机文件分析等。

第三章　介绍文件分析技术，主要包括文件签名及散列分析应用，动态仿真技术。

第四章　介绍了内容匹配技术，包括文件过滤技术、关键词搜索技术，重点阐述 GREP 语法表达式在实战中的分析与应用。

第五章　Web 服务器取证分析，包括服务器取证的基础知识、VmWare 虚拟机应用、数据库基础及 Web 环境搭建、RAID 重组技术、IIS 网站取证、常见 Web 日志分析等技术。重点阐述了常见 RAID 模式、重组方法，分析思路与经验技巧。以实战案例方式详细阐述了 IIS 网站取证系统仿真、数据库分析及关联分析。以 IIS 日志为例阐述日志格式含义以及在入侵案件分析中的综合运用。

第六章　数据恢复技术，主要包括数据恢复基础知识，常见的软、硬件恢复工具以及数据恢复方法（包括删除文件恢复、分区格式化恢复、丢失分区恢复）。

第七章　数据关联分析技术，主要介绍实际取证分析中常见的两种数据分析：人员组织结构分析、银行账单关联分析。

工商机关在办理涉及计算机和互联网的案件中，常常会因为缺乏相应证据且无第三方见证，导致案件证据不足，面临“疑罪从无”最终销案的局面。因此，我们必须清醒地意识到运用电子数据取证分析技术是查办涉及计算机和互联网案件的有力手段，也是开辟调查途径、解决查办难点、完备证据体系的迫切形势，更是大力加强工商执法信息化，工商创新发展的重要支撑。本书采用理论结合实际案例的方式对电子数据取证分析技术进行全面剖析，内容由浅入深、条理清晰，力求让执法人员能学为己用、学有所得，为执法部门的电子数据分析调查实践工作提供有益参考。

笔者期待与广大读者进行交流，共同探讨电子数据取证分析相关技术问题。

目 录

第1章 电子数据取证分析概述

本章学习目标：

1. 熟悉常见文件系统、国内外取证分析工具；
2. 掌握电子数据取证常用术语、电子数据取证分析方法及注意事项。

1.1 电子数据取证分析基础

电子数据取证工作涉及较多的计算机技术，因此要求分析人员掌握足够的相关基础知识，如磁盘的存储原理、操作系统基础、应用程序相关常识，以及各种专业取证分析软件的应用等。

1.1.1 FAT 文件系统

FAT 文件系统的名称来源于“文件分配表(File Allocation Table)”，文件分配表用于记录 FAT 文件系统中簇的使用情况。“FAT”后面的数字，如 FAT12、FAT16、FAT32，表示用于记录对应逻辑卷上的簇的数据位数(8 位为一个字节)。

高密度软盘使用 FAT12 文件系统，即使用 12 个数据位记录逻辑卷上可用的地址，该位数限制了簇的数量不能超过 4 084。尽管 212 的结果是 4 096，但其中保留了 11 个值用于表示特殊值，1 个值被舍弃，剩下 4 084 个值可用作地址。大家可以很快明白为什么 FAT12 不能够用于硬盘分区上，因为 4 084 个簇地址无法管理上百万个扇区。

FAT16 使用了 2 个字节(16 位)表示地址，其簇地址个数为 65 524(与 FAT12 类似，65536 个地址减去 12)。FAT32 使用了 4 个字节(32 位)表示地址，然而，高 4 位保留未被使用，因此 FAT32 实际使用了 28 位，其簇地址数为 268 435 445。

在 DOS/Windows 下，对于 FAT16 和 FAT32 文件系统，硬盘上的数据按照

其不同特点和作用大致由 MBR 区、DBR 区、FAT 区、FDT 区和 DATA 区这 5 个部分组成。其中，MBR 由分区软件创建，而 DBR 区、FAT 区、FDT 区和 DATA 区由高级格式化程序创建。文件系统写入数据时只是改写相应的 FAT 区、FDT 区和 DATA 区。FAT 分区的数据存储区域分布，如下图所示。

图 1-1　FAT 分区的数据存储区域

1.1.1.1 DBR

DBR(DOS Boot Record)，操作系统引导记录区，国外也常称之为 VBR(Volume Boot Record)。第 1 个分区的 DBR 通常位于硬盘 0 柱面 1 磁头 1 扇区，是操作系统可以直接访问的第一个扇区。它由以下 5 个部分组成：

1. 跳转指令，占用 3 个字节，它将程序执行流程跳转到引导代码的位置。

2. 厂商标识和 DOS 版本号，该部分总共占用 8 个字节，其内容随 DOS 版本不同而略有变化。

3. BPB(BIOS Parameter Block，BIOS 参数块)，BPB 从第 12 字节起占用 52(0B ~ 3E，FAT12/FAT16)或 80(0B ~ 5A，FAT32)个字节。BPB 参数记录着本分区的起始扇区、结束扇区、文件存储格式、硬盘介质描述符、根目录大小、FAT 个数、簇大小等重要参数。该部分的内容随磁盘类型的不同而变化。

4. DOS 引导程序。DOS 引导程序是占用 448 字节(3E ~ 1FD)或 420 字节(5A ~ 1FD)的 BOOT 代码，负责完成 DOS 的 3 个系统文件的装入工作。这部分内容随 DOS 版本不同而变化。

5. 结束标志，结束标志占用 2 个字节，与分区表的结束标志相同，其值为“55 AA”。

以上 5 个部分共占用 512 个字节，正好是一个扇区，因此，称它为 DOS

引导扇区或 BOOT 区。该区间的内容,除了第 5 部分结束标志固定不变之外,其余 4 个部分都是不确定的,第 1,2,4 部分都因 DOS 版本的不同而不同,第 3 部分的内容也随 DOS 版本及磁盘的逻辑盘参数的变化而变化。

下表所示为 FAT32 文件系统 DOS 引导扇区的详细结构:

表 1-1 FAT32 文件系统的 DOS 引导扇区结构

偏移地址	字节数	标识符	注释
00H	3	跳转码	包含短转移指令(1 字节),引导区代码的偏移地址(1 字节)和一个空指令(NOP)
03H	8	OEM 名称	格式化分区的操作系统的名称
0BH	2	每扇区字节数	每个扇区包含的字节总数
0DH	1	每簇扇区数	每个簇包含的扇区总数
0EH	2	保留扇区数	为引导记录保留的扇区总数
10H	1	FAT 数	FAT 的总数,一般为 2 个(原始的 FAT 及其备份)
11H	2	根目录数	根目录中可能的最大目录数。允许设置根目录的子目录数目
13H	2	扇区总数	扇区总数。用于小于 32MB 的分区和软盘驱动器
15H	1	介质类型	软盘驱动器用“F0”,硬盘驱动器用“F8”
16H	2	每个 FAT 的扇区数	每个 FAT 上包含的扇区总数,用于 FAT12/16
18H	2	每个磁道的扇区数	每个磁道上包含的扇区总数
1AH	2	每个柱面的磁头数	驱动器磁头的总数
1CH	4	隐藏扇区数	引导记录前,主引导记录 MBR 中的扇区总数
20H	4	扇区总数	大于 32MB 的分区中的扇区总数
24H	4	每个 FAT 的扇区数	在每个 FAT 上的扇区总数。用于 FAT32
28H	2	标志	为确定 FAT 镜像状况而保留的。允许将备份 FAT 作为主 FAT32 系统

续表

偏移地址	字节数	标识符	注释
2AH	2	版本	文件系统版本号
2CH	4	根目录簇	根目录的起始簇号
30H	2	信息扇区	文件系统信息区的扇区号
32H	2	引导备份位置	驱动器上引导记录的备份位置的扇区号
34H	12	保留	为将来使用保留
40H	1	驱动器 ID	软盘驱动器用“00”,硬盘驱动器用“80”
41H	1	NT 保留	当驱动器格式化时,被 NT 设置为“00”
42H	1	扩展驱动签名	设置为“29”表示当前的序号,分区名称和 FAT 类型存在
43H	4	卷序列号	格式化时分配给分区的唯一序号。快速分区和完全格式化都会重新分配一个序号
47H	11	卷/分区名	在格式化驱动器时给卷的一个 11 个字符的名称
52H	8	FAT 类型	FAT12、FAT16 或 FAT32。这是给一些工具使用,而不是操作系统使用
5AH	420	可执行的引导程序	引导系统本身开始的第一个文件
01FEH	2	可执行的签名	格式化时设置为“55AA”,否则操作系统将不能被当前的 BIOS 识别

DBR 的主要功能:

DOS/Windows 系统在引导的时候,DBR 是第一个(除硬盘的 MBR 之外)需装载的程序段。DBR 装入内存后,即开始执行引导程序段,其主要任务是装载 DOS 的系统隐藏文件 IO. SYS。

它包括一个引导程序和一个被称为 BPB(BIOS Parameter Block)的本分区参数记录表。引导程序的主要任务是,当 MBR 将系统控制权交给它时,判断本分区根目录前两个文件是不是操作系统的引导文件。以 DOS 为例,即是 IO. SYS 和 MSDOS. SYS。低版本的 DOS 要求这两个文件必须是前两个文件,即位于根目录的起始处,占用最初的两个目录项,高版本已经没有这个限制。