[4]武鸿浩.网络犯罪侦查课程实训体系建设[J].网络安全技术与应用，2018（10）：130-131.
[5]易艳阳.“社会调查研究方法”课程案例库建设路径探究[J].湖北开放职业学院学报，2019，32（24）：139-140.
[6]于小川．公安院校网络安全与执法专业一体化建设探索—以广西警察学院为例[J].广西警察学院学报，2019，32(4)：112-115.
[7]杨静宁，马连生，王鹏.基于案例库建设的材料力学互动教学设计与实施[J].力学与实践，2020，42（2）：237-241.
[8]刘晶晶.“全景式”案例教学法在经济犯罪侦查课程教学中的适用[J].教育教学论坛，2020（10）：234-235.

哈希算法在电子数据取证中的应用研究

◆王冠

（辽宁警察学院公安信息系　辽宁　116036）

摘要：哈希在电子数据取证中具有重要的作用，可以保证电子数据的完整性和真实性。通过分析哈希算法的特点，实验验证 Word 文件的修改时间对完整性校验的影响。提出把哈希库看作一种广义上的关键字搜索，以及哈希算法在电子数据提取与司法鉴定阶段中的作用。

关键词：哈希；电子数据取证

1　哈希算法介绍

Hash（通常翻译为散列，或音译为哈希），是把任意长度的输入数据通过散列算法，经过压缩映射变换成固定长度的输出散列值，该输出散列值也被称为消息摘要。因此，哈希是一种将任意长度的消息压缩到某一固定长度的消息摘要的算法，被广泛应用于文件校验与数字签名当中。

2016 年，两高一部颁布执行的《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》第五条明确保护电子数据完整性的方法，需要计算电子数据完整性校验值；第十二条规定在冻结电子数据时，要求计算电子数据完整性校验值；第二十三条中明确验证电子数据完整性时，需要比对电子数据完整性校验值。2019 年公安部颁布执行的《公安机关办理刑事案件电子数据取证规则》中同样也对上述问题提出了计算电子数据完整性校验值的这一要求。实际上，对于电子数据计算完整性校验值，就是将一个电子数据存储介质或一个具体的电子数据文件通过哈希算法得到一个固定长度的哈希校验值，并将该哈希校验值作为该电子数据没有被改变的完整性依据。

哈希算法之所以可以作为验证电子数据完整性的方法，是因为其独有的四个特性，即等长、雪崩、防冲突和不可逆：等长是指对于同一种哈希算法来说，任何文件不论大小（上至 TB 级的硬盘，下至几个字节的文件），都可以得到固定长度的哈希值；雪崩是指任何一个文件只要内容发生改变，哪怕只是一位二进制下 0 或 1 的改写，都会造成该文件的哈希校验值发生根本性变化，即该文件的校验值会变的完全不同；防冲突是指任何两个不同的文件得不到同一个哈希值，以经典的哈希算法 MD5 来说，其校验值固定长度为 128 位的二进制数字，因此两个不同文件得到同一个 MD5 值的概率即为 1/2128；不可逆是指由于哈希算法是单向的压缩摘要算法，与传统的文件加密算法不同，无法通过哈希校验值逆推出原文件内容。有上述四个特性可知，哈希也被称作“数字指纹”被广泛应用于电子数据取证中。

2　哈希算法实验

在电子数据取证中使用的哈希算法通常为 MD5、SHA1、SHA256 这三种，其中 MD5 算法生成的校验为 128 位二进制，SHA1 算法为 160 位二进制，SHA256 算法为 256 位二进制。算法生成的校验值长度越长，则该算法被碰撞破解的概率越低。由于 MD5 和 SHA1 算法都存在被数学破解的可能性（即对不同文件得到同样的哈希值），我国的司法鉴定和证据审查中均要求提交电子数据完整性校验值需采用 SHA256 算法来计算以保证司法严谨性。但实际操作中，即便是使用 MD5 算法，只要一个电子数据的哈希值没有发生变化，就可以认为该电子数据的完整性得到了保证。为避免工作中的误操作导致电子数据哈希值的变化破坏证据完整性，本节将设计四个 word 文档的实验来探讨对于文件修改时间对于哈希值的影响。实验首先准备一个存有文本内容的 docx 文档并计算 MD5 值 7b2cc8a7dd2c20579307818e35c8e8c5，记录下来用于比对。

实验 1：将该文档文件名进行修改，修改后重新计算哈希值与原哈希值比对，哈希值没有改变。实验分析：由于文件名属于文件属性，并没有写入文档所在数据区，而哈希值计算的是文档数据区内容，因此修改文件名并不会更改哈希值。

实验 2：将该文档进行复杂粘贴到另一个磁盘分区中，计算该复制文档的哈希值与原哈希值比对，哈希值没有改变。实验分析：复制后文档的创建时间发生变化，但修改时间没有变化，创建时间并不影响文件数据区内容，因此复制文件的副本并不会更改哈希值。

实验 3：将该文档打开，不做任何改变直接点击保存按钮。完成后关闭该文档，重新计算哈希值，对比后发现没有改变。实验分析：当对文档内容没有任何操作的情况下，点击保存按钮，并不会造成 docx 文档的修改时间变化。由于修改时间没有变化，因此哈希值不变。

实验 4：打开该文档，在文字中输入一次空格，然后删除该空格。点击保存按钮，关闭文档。重新计算该文档哈希值 369a132900749fa2989b3522a6f998e8，对比后发现与原文档哈希不一致，发生改变，操作结果如图 1 所示。实验分析：对文档加减空格后保存的操作，虽然对实际文本内容没有修改，但由于 word 文档的特性会对每一次操作进行格外记录，以便于撤销恢复。这些记录会写入文件中，也会造成文档修改时间的改变，因此该文档对应的哈希值也会发生变化。在实际工作中应当避免对于文件误操作后撤销且点击保存的操作，以免造成哈希值的变化而改变文件完整性。

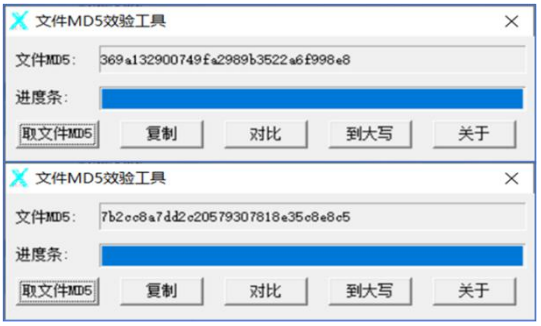

图 1　word 文件加减空格后保存改变 MD5 值

3　哈希算法在电子数据取证应用

3.1 勘查阶段

在公安工作中，不论在现场提取电子数据或是通过网络在线提取电子数据阶段，都需要对提取的电子数据进行固定，并计算完整性校验值。此外，若需要通过录像的方式记录提取过程时，也同样需要将该录像文件计算完整性校验值。通过提取电子数据时计算哈希值并做好记录的操作，在证据审查阶段，只需确定电子数据的哈希值与提取时的哈希值一致，即可以判断该证据的真实性和完整性。

3.2 司法鉴定

在对电子数据进行分析和司法鉴定工作中，通常要求对原始电子数据存储介质进行备份或镜像，并通过只读保护设备来对该备份进行分析。为保证电子数据的完整性，首先需要计算该原始电子数据存储介质的哈希值，然后在做完位对位的备份后，同样计算该备份介质的哈希值进行比对，两者一致才能证明是同样的电子数据。分析完成该备份介质后，需要再次对该分析备份介质计算哈希值并证明一致，以此来验证分析过程没有对电子数据造成任何破坏或更改。

此外，在司法鉴定过程中，还经常需要做同一性或相似性鉴定的鉴定报告，这也需要比较双方送检文件的哈希值是否一致来直观判断是否存在同一性问题。对于数据库或软件相似性的司法鉴定，往往也需要比较双方数据库文件或服务器文件中，具有相同哈希值的文件数目，以此来确定是否存在同样的文件，判断存在相似性的可能。

3.3 哈希库

在电子数据分析过程中，通常会将一类已知的特定文件（如操作系统文件，常用软件文件，病毒和恶意代码文件以及犯罪图片等）进行哈希值计算，然后将这些特定类型的文件的哈希值记录下来，并进行分类成为一个库的概念，即为哈希库（hashsets）。在分析一台嫌疑人的电脑时，可以通过计算该电脑中所有文件的哈希值，并与已知登记的哈希库进行碰撞，当发现存在同样哈希值的文件后，即可以快速明确该电脑中存在的文件内容。比如，该电脑的操作系统文件，安装的办公文档软件，是否存在病毒或恶意代码程序以及是否存有相关犯罪图片文件等。采用哈希库这一技术进行快速的文件搜索，实际上非常类似于我们平时使用的关键字搜索技术。关键字搜索技术，是通过将字转换为二进制编码匹配的过程，而哈希库是通过将文件转换为哈希值进行匹配的过程。因此也可以把哈希库看作是是一种广义上的关键字搜索技术。实战中通过特定文件的哈希库进行比对，而不需要一个个的比较文件内容，可以快速发现一类的涉案证据文件，起到事半功倍的效果。

4　结语

本文介绍了哈希算法的特点，对哈希算法的等长、雪崩、防冲突和不可逆四个特性进行了分析。明确了哈希在电子数据取证中对于完整性和真实性的作用。并进行了 word 文档的哈希实验，以此确定了修改时间对于哈希值的影响。最后对于哈希在电子数据取证工作中的应用进行了介绍，提出了哈希库是广义上的一种关键字搜索技术这一观点。

参考文献：

[1]王聪,饶智韬,刘满果.MD5 值的电子取证应用研究[J].中国公共安全(学术版),2020(01):146-149.

[2]王鸣远．电子数据完整性证明研究[D].重庆邮电大学,2019.

[3]尹鹤晓．电子数据侦查取证程序研究[D].中国人民公安大学,2019.

论跨国网络犯罪给我国刑法管辖原则带来的冲击与挑战

◆魏祎远

（北京外国语大学法学院　北京　100089）

摘要：随着互联网技术发展和用户不断增多，网络犯罪日益突出，新的犯罪形式不断涌现。互联网作为一项重要的媒介，已成为跨国犯罪的重要工具，我国刑法的管辖原则已不能准确适应跨国网络犯罪发展所带来的冲击与挑战，给国家、社会和个人都造成了严重影响，给我国刑法传统的管辖原则理论带来了巨大冲击，各国的刑事管辖权也因此受到了重要影响。

关键词：网络空间；跨国网络犯罪；刑法管辖原则

1　跨国网络犯罪的界定

1.1 网络犯罪

网络犯罪是随着社会进步、科技发展而形成的一种犯罪类型，它深刻体现了社会生产力发展水平，使许多传统型犯罪皆可利用网络进行实施。从整体上看，“网络”与犯罪的关联目前有“工具说”“对象说”“空间说”和“关联说”。

第一种学说是“工具说”，该学说把网络视为同传统犯罪一样的犯罪工具。如果行为人使用网络实施危害国家安全、社会法益和个体法益的犯罪行为就应视为网络犯罪。第二种学说是“对象说”，该学说是把网络作为一种犯罪对象来看待。即把网络作为犯罪行为所侵害的具体人或具体物，通过对网络实施侵害达到危害信息网络秩序、社会公共秩序的目的。第三种是“空间说”，即把网络作为犯罪空间，主要是依据网络在该类犯罪中的地位和作用来划分，正如劳尔·昆兰蒂罗所说“网络空间是一个与现实世界有些相似的世界，是一个既存在于现实世界，又存在于现实世界之外的无法界定的地方。”[1]第四种学说是“关联说”，是目前占据主流的观点，主要是以犯罪行为是否与网络有所关联进行判断，无论是犯罪主体、客体抑或是犯罪对象、犯罪工具等，凡是有网络与其相关联就视为网络犯罪。当前，将网络作为“犯罪对象”“犯罪工具”和“犯罪空间”的网络犯罪，三者共存而案发比例各不相同：“犯罪对象”类网络犯罪逐渐减少，“犯罪工具”类网络犯罪占据上风，“犯罪空间”类网络犯罪不断攀升[2]。

中国司法大数据研究院 2019 年 11 月发布的司法大数据专题报告之网络犯罪特点和趋势（以下简称“网络犯罪报告”）给网络犯罪的定义是指以互联网为工具或手段实施的危害社会、侵害公民合法权益的行为，或是对计算机系统实施破坏的行为，可见其采用的是“工具说”和“对象说”。

综合不同学说观点，结合各类型网络犯罪的发展趋势，本文认为网络犯罪是指行为人利用网络技术，把网络作为犯罪工具或攻击对象，或以网络空间为主要犯罪场所，从事直接危害网络安全和秩序以及其他严重危害国家、公民和社会利益的犯罪行为。

1.2 跨国网络犯罪

跨国网络犯罪是在网络犯罪基础上所形成，是指符合网络犯罪的构成要件，并且由具有组织性的犯罪团伙通过互联网这一媒介实施的犯罪行为，通常表现为跨国诈骗、色情、盗窃、赌博、诽谤、洗钱、传播计算机病毒、侵犯知识产权等犯罪行为。其构成可以表述为：网络犯罪+犯罪主体跨国/犯罪工具跨国/犯罪结果跨国/犯罪目的跨国=跨国网络犯罪，其中犯罪主体、犯罪工具、犯罪结果、犯罪目的只要有一样具有跨国成分，就可构成跨国网络犯罪。