

[ISS 2017]电子数据取证 议题分享二：计算机取证，科学？

[明月为临](#) / 2017-07-31 09:09:00 / 浏览数 2971 [安全技术](#) [资源分享](#) [顶\(0\)](#) [踩\(0\)](#)

小编按：邹教授总是非常风趣幽默，谈笑间发人深省。这次他通过儿童色情案例的分析，与大家探讨计算机取证的未来方向，科学的方法、重复的实验。工具各家公司都有，通常我喜欢讲一些故事、案例，讲一点能唤醒你的故事。这是09年发生在香港的案例，香港环保署助理署长因为观看色情网站面临革职。

有20%的男性承认在工作中在线观看色情作品。一周内哪一天最多人看色情？星期天。学生都看，学生是什么时候看的？做功课的时候。今天4个老师我们都没有看。

□

昨天我们看到很多CEO、COO分享了议题，你们都知道是首席执行官、首席运营官，你们听过CPO吗？首席色魔。今天我和大家讨论关于网络色情的案例。

在香港，成人色情网站并不是犯罪，而儿童色情，无疑是严重的罪行。！

香港一商会会长曾经因藏2万儿童色情照被判刑。如果你的电脑里面、手机里面有儿童色情照，这就是犯罪。

什么也不用解释，持有儿童色情物品就是犯罪，但问题是什么是“有”？

嫌犯往往辩称他不知道儿童色情作品存在，同时如果嫌犯在合理期限内已经将作品删除，恢复出来的不算。这就是今天我跟大家讲的两个问题：

第一个问题是他自己知道不知道儿童色情作品的存在？

第二个问题他在合理的期限内删除了。有没有科学的方法来证明其罪？

另一个案例。如果在疑犯电脑里找到5万儿童色情照片，没有人会相信他什么也不知道。那只有一个我们怎么算？他知道不知道？两个、五个、十个、二十个呢？有科学模型

如果只有一个，他知道就是犯罪，但是好多时候他们都是不知道，好多时候他们都没有修改，他的儿童色情照片有一个，我们怎么知道他知道还是不知道。去法庭，被告承认

法医DNA的问题，在犯罪现场发现了一根头发，数学模型会计算出头发不是被告的概率值，重复的实验，第二是子弹轨迹，数学模型，重复的实验。在计算机取证领域，有

法医学是应用在刑事跟民事案，观察和实验对物理和自然界的结构和行为进行系统研究的智力和实践活动。

科学的方法是什么？系统的观察、测量和实验，以及对假设的表述、检验和修正。

计算机的取证，科学，有科学的方法吗？你们有没有做实验？刚刚丁老师说了好多工具，取证，但有些工具什么取证方法，有没有什么实验？这就是科学，一个简单的问题

可以看两个案例，2010年香港一个儿童色情案例，有一个电脑里面有上万个图像，其中248个是儿童色情的，他说什么也不知道，我们用我们数学模型可以算出来随机浏览活

还有一个案例，被告有超过714430个下载图像文件，其中有84个儿童色情图像文件，我们算出来随机浏览活动的结果几率是不超过4%的。

我们的论文An approach to quantifying the plausibility of the inadvertent download defence供大家参考

我们常常听到一些工具，我的工具比他工具多，我的工具找不到，你的工具找到吗？其实问题是法庭需要的是可重复的实验。

除了在香港大学做科研，还有其他人在做吗？NIST他们这个科研中心主要就是几个方向，就是专注于改善指纹，枪械，工具痕迹，牙科及其他模式的统计基础实证分析。还

他们的工作不仅限于传统法医学，还包括计算机、视频、音频等数据证据分析。

法医学在解决犯罪、使犯罪者绳之以法、保护无辜者免受错误定罪方面发挥着关键作用。卓越的法医科学中心将侧重于模式证据和电子证据。

计算机取证，我们有重复的实验吗？

NIST里面有一个项目，叫CFTT，是通过制定是通用工具的规范、测试程序、测试标准、测试集和测试硬件，建立一种测试计算机取证工具的方法。测试项目也可以用来确保forensics tool testing handbook都可以在网上下载。

因此计算机取证的发展，下一步是科学的方法、重复的实验。谢谢各位！

点击收藏 | 0 关注 | 1

[上一篇：威胁情报与安全智能PPT](#) [下一篇：\[ISS 2017\]电子数据取证 ...](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)