听《Automated forensic analysis of mobile applications on android devices》有感

2019年5月20日，学校邀请了Xiaodong Lin教授就Android设备上移动应用程序的自动取证分析进行技术分享。Xiaodong Lin教授获中国北京邮电大学信息工程博士学位，加拿大滑铁卢大学电气与计算机工程博士学位（研究生成绩优异）。他目前是加拿大圭尔夫大学计算机科学学院终身副教授。他的研究兴趣包括无线通信和网络安全、计算机取证、软件安全和应用密码学。他是许多国际期刊的副主编。他曾担任或正在担任IEEE、Elsevier和Springer期刊的许多特刊的客座编辑，以及IEEE/ACM会议的研讨会主席或轨道主席。他还曾在许多项目委员会任职。他是通信和信息安全技术委员会（ICTC）的主席，IEEE通信协会（2016-2017年），他同时也是IEEE的研究员。

讲座中以手机参与犯罪活动为背景，这在现实生活中并不罕见，例如秘密收集信用卡信息。因此移动应用程序的法医分析对于收集犯罪证据至关重要。然而，传统的基于人工调查的取证方法无法扩展到大量的移动应用程序。另一方面，由于建立适当的运行时环境以适应操作系统差异和依赖库并激活所有可行的程序路径，动态分析很难实现自动化。在讲座中，Xiaodong Lin教授介绍了一个全自动的工具，ForDroid，用于在Android上对移动应用程序进行取证分析。Fordroid对Android APK进行组件间静态分析，并构建控制流和数据依赖关系图。此外，Fordroid还通过污染分析来识别在本地存储中写入的信息的内容和位置。通过遍历图来定位数据。这解决了几个技术难题，包括组件间字符串传播、字符串操作（例如append）和APL调用。此外，ForDroid还通过解析SQL命令（即数据库表的结构）来标识如何存储信息。最后，我们从四个类别中选择了由2841个组件组成的100个随机Android应用程序进行评估。对所有应用程序的分析花费了64小时。Fordroid在36个应用程序中发现了469条路径，这些应用程序将敏感信息（如GPS）写入本地存储。此外，Fordroid成功地定位了458（98%）条路径的信息写入位置，并确定了所有（22个数据库表）的结构。

事实上，移动设备取证已经有了相当多的成果。移动设备上本地存储的数字取证需要回答以下三个问题：存储的信息是什么（例如，GPS）；存储的信息在哪里（例如，文件路径）；以及如何存储信息（例如，数据库表的结构）。过去进行了大量的研究，以识别和分析各种应用程序生成的工件。动态分析是最常见的实践。更具体地说，应用程序安装在测试电话或模拟环境中。在一段时间内手动播放应用程序以生成法医痕迹。不幸的是，这种方法有几个缺点：首先很难出发所有的程序路径，从而无法发现犯罪行为；其次手动解析相关工件的文档是一项艰巨而漫长的任务。

Xiaodong Lin教授正是解决了上述现有技术的局限性，实现了移动设备的自动取证，在高效、自动化的同时保证了取证的准确性。