## 信息安全及取证研讨班

**主持人：**伏晓

**时间：**2016年11月至2017年4月

**理论内容：**计算机取证、信息安全。

**上课实践：** (上课时间另行通知)

**实践内容：**（根据学生实际情况，选择合适的最优实践）

1. 基础理论：计算机取证、信息安全。
2. 深入研讨：计算机及互联网技术的迅猛发展也带来了计算机犯罪率的飞速增长。打击犯罪的关键在于获得充分、可靠和强有力的证据。计算机取证（computer forensics）即是专门研究如何按照符合法律规范的方式收集、处理计算机犯罪证据的新兴学科。本研讨班将探讨针对各种环境下（例如：网络、单机、云平台、移动平台等）面临的安全问题，以及针对各类犯罪行为（例如：黑客入侵、散步非法信息、违法下载等）的不同取证技术，例如：如何从内存信息中自动识别犯罪线索、如何自动重现犯罪过程、如何从海量候选数据中自动筛选出与犯罪相关的证据。
3. 实际开发：结合上述理论和技术研究，开发一些相关的软件工具。

**组织方法：**

1. 充分地研讨充分地交流。同学们可以根据自己的兴趣，选择相应的子主题开展更加深入的研究和开发工作。
2. 每次讨论约2小时。
3. 交流方式除了会议外，建立Email group，交流相关问题。