第五届全国计算机取证技术研讨会

程 序 册

主办单位：

中国电子学会计算机取证专家委员会

承办单位：

中央财经大学

支持单位：

《计算机科学》编辑部
《信息网络安全》编辑部
《警察技术》编辑部
公安部第三研究所
公安部第一研究所
中国政法大学电子证据研究中心

赞助企业：

厦门市美亚柏科信息股份有限公司
北京实数科技有限公司
北京天宇宁科技有限公司
上海勋立信息科技有限公司

中国 • 北京　2015 年 11 月 20 日-22 日

第五届全国计算机取证技术研讨会

中国·北京　2015 年 11 月 20 日-22 日

大会主席（以姓名拼音为序）：

丁丽萍　中国科学院软件研究所　　朱建明　中央财经大学

副主席：

王永全　华东政法大学

顾问（以姓名拼音为序）：

卿斯汉　中国科学院软件研究所　　许榕生　中国科学院高能物理研究所

组委会（以姓名拼音为序）：

畅　斌　西安政治学院　　孙国梓　南京邮电大学
陈虹宇　四川神琥科技有限公司　　陶　冶　南京海关缉私局
戴士剑　中国人民大学　　谭晓生　奇虎 360 科技有限公司
段美姣　中央财经大学　　田庆宜　重庆市公安局
范　渊　杭州安恒信息技术有限公司　　涂　敏　江西警察学院
高　胜　中央财经大学　　万　涛　IDF 互联网情报威慑防御实验室
高　翔　北京握奇数据系统有限公司　　王立梅　中国政法大学
郭　弘　公安部第三研究所　　王连海　山东省计算中心
郭英凯　上海北信源信息技术有限公司　　王秀利　中央财经大学
郭永建　北京天宇宁科技有限公司　　王永吉　中国科学院软件研究所
顾　健　公安部第三研究所　　谢君泽　中国人民大学
韩　冰　黑龙江省电力科学研究院　　谢亚龙　中国人民银行
韩马剑　河北省公安厅　　徐北明　中国电子学会
韩　晟　安世盾信息技术（北京）有限公司　　徐家力　中国政法大学
贾恒越　中央财经大学　　徐志强　厦门市美亚柏科信息股份有限公司
赖英旭　北京工业大学　　夏晓光　北京石盾科技有限公司
李　健　北京工业大学　　杨卫军　公安部第一研究所
李立中　蚂蚁金融服务集团　　杨中皇　高雄师范大学
李生红　上海交通大学　　张昌利　北京联合信任技术服务有限公司
李　洋　中央财经大学　　张宏大　沈阳市公安局
李　毅　盘石软件（上海）有限公司　　张焕国　武汉大学计算机学院
廖　鑫　湖南大学　　张　青　上海安永注册会计师事务所
刘浩阳　大连市公安局　　张　舒　北京市公安局信息中心
刘　健　信息产业信息安全测评中心　　张　璇　山东警察学院
刘品新　中国人民大学　　赵　阔　吉林大学
刘三满　山西警官高等专科学校　　赵　庸　厦门市美亚柏科信息股份有限公司
彭国军　武汉大学　　赵险峰　中国科学院信息工程研究所
石文昌　中国人民大学　　郑　辉　北京网秦天下科技有限公司
寿　步　上海交通大学　　邹锦沛　香港大学
宋　润　北京市刑事科学技术研究所

主办单位：中国电子学会计算机取证专家委员会

承办单位：中央财经大学

支持单位：

《计算机科学》编辑部　　公安部第三研究所
《警察技术》编辑部　　公安部第一研究所
《信息网络安全》编辑部　　中国政法大学电子证据研究中心

赞助企业：

厦门市美亚柏科信息股份有限公司　　北京天宇宁科技有限公司

北京实数科技有限公司　　上海勋立信息科技有限公司

温馨提示

尊敬的各位代表：

您好！

欢迎您来到北京参加第五届全国计算机取证技术研讨会！为保证会议的有序进行和您在此期间生活、交流的便利，敬请注意以下事项：

1. 请熟悉会议日程，按照会议日程的安排准时参加。若议程的时间、地点安排有临时调整变化，会务组将及时通知。

2. 为方便服务和管理，请各位代表在开会和就餐时随身佩戴代表证，并妥善保管，不得转借。

3. 进入会场后，请关闭手机或保持在静音状态，尽量不要在会场内走动，以免影响会议正常进行。会场内请勿吸烟。

4. 开会、住宿、就餐、乘车时请妥善保管个人财物。会议期间正值中央财经大学学院南路校区内施工，进出学校请注意安全。

5. 大会在中央财经大学（学院南路校区）西侧融金中财大酒店设有会议注册处，遇有问题请及时和会务组工作人员联系。

6. 融金中财大酒店、中央财经大学专家宾馆每天最晚退房时间为 12:00。

7. 本次会议如有服务不周之处，敬请谅解。

祝您在第五届全国计算机取证技术研讨会会议期间身体健康，心情愉快，一切顺利！

第五届全国计算机取证技术研讨会会务组

2015 年 11 月 11 日

日程概况

11 月 20 日（星期五）全天 （融金中财大酒店）	
09:00 - 21:00	报到、注册
18:30 - 20:00	晚餐（凭代表证在融金中财大酒店就餐）
11 月 21 日（星期六）上午 （中央财经大学学院南路校区学术会堂 202）	
08:30 - 09:00	开幕式
	领导致辞
09:00 - 09:20	全体代表合影留念
09:20 - 09:55	大会主题报告：电子取证—一个越来越被关注的研究领域 报告人：丁丽萍（中国科学院软件研究所）
09:55 - 10:30	大会主题报告：移动取证软件的设计与实践（Design and Implementation of Mobile Forensic Software） 报告人：杨中皇（高雄师范大学）
10:30 - 10:50	茶歇
10:50 - 11:25	大会主题报告：互联网时代的电子数据保全与鉴定 报告人：叶　红（国家信息中心）
11:25 - 12:00	大会主题报告：电子支付取证方法研究 报告人：朱建明（中央财经大学）
12:00 - 13:00	午餐（中央财经大学专家宾馆）
11 月 21 日（星期六）下午	
13:30 - 17:00	论文宣讲论坛（中央财经大学学院南路校区学术会堂 202）
18:00 - 19:30	晚餐（由北京天宇宁科技有限公司赞助）
11 月 22 日（星期日）上午 （中央财经大学学院南路校区学术会堂 706）	
08:30 - 08:50	优秀论文评选
08:50 - 09:15	大会主题报告：大数据取证技术的定位与规制 报告人：刘品新（中国人民大学）
09:15 - 09:50	大会主题报告：互联网金融犯罪及数字取证 报告人：孙国梓（南京邮电大学）
09:50 - 10:25	大会主题报告：苹果系列产品的取证难点及一些新思路 报告人：尹文基（上海势炎信息科技有限公司）
10:25 - 10:50	茶歇
10:50 - 11:25	大会主题报告：综合各种时间属性开展深层次调查和鉴定 报告人：郭永健（北京天宇宁科技有限公司）
11:25 - 12:00	大会主题报告：第六代电子数据取证模式 报告人：吴少华（厦门市美亚柏科信息股份有限公司）
12:00 - 13:00	午餐（中财大厦）

大会主题报告

主题报告 1：电子取证——一个越来越被关注的研究领域

报告人：丁丽萍　研究员

报告简介：

电子取证是一个法学与计算机科学的交叉领域。随着电子技术的普及和应用，犯罪和违法行为涉及电子证据的情形越来越多。大数据、物联网、移动互联网等诸多领域出现了很多新技术新场景，给电子取证带来了前所未有的挑战。本报告将重点介绍电子取证涉及的研究领域，发展现状，与其他学科的关系，以及近年来面临的热点难点问题。

报告人简介：

丁丽萍，中国科学院软件研究所研究员，博士生导师；兼任中国电子学会计算机取证专家委员会主任委员，中央财经大学信息学院兼职教授，中南理工大学软件学院兼职教授，北京工业大学计算机学院兼职教授，北京航空航天大学金融安全联合实验室技术顾问。她的主要研究领域包括电子数据取证、系统安全和可信计算。

主题报告 2：移动取证软件的设计与实践（Design and Implementation of Mobile Forensic Software）

报告人：杨中皇　教授

报告简介：

2014 年全球智能手机用户达 13 亿，智能手机销售量远超过个人电脑。移动智能终端(包含智能手机、智能手表、平板电脑等) 已成为现代人不可或缺的随身设备，越来越多的个人资料不可避免地存放在此设备中。2013 年斯诺登(Snowden)揭露美国国家安全局(NSA)的“棱镜”（PRISM）监控计划，明显美国与英国等国家的情治单位通过攻击智能手机应用软件来搜集情报资料。所以移动终端的资料保护，已经成为信息安全与网络空间安全的重要课题。移动取证可让用户了解终端内部的隐私资料，从而采取加强措施保护资料。由于移动智能终端操作系统的版本更新快、终端隐私资料也常存于云平台、iOS 终端的越狱与 Android 终端的刷机，这些特色使得移动取证面临很多挑战。本报告从学术单位的角度探讨移动取证软件的设计与实践，我们介绍过去几年针对 iOS 终端与 Android 终端进行取证雏型软件开发所碰到的问题与解决的方式。

报告人简介：

杨中皇教授 1958 年生于台湾台北，1990 年美国 University of Louisiana at Lafayette 计算机工程博士(由中科院曾肯成教授访问美国期间指导博士论文)，曾任美国 RSA Data Security, Inc.软件研发工程师(1991)、日本电信电话公司(NTT)博士后研究员(1991-1993)、台湾的中华电信研究所“信息安全与密码技术”项目主持人(1996-1997)。此外，杨教授担任过 SCI 期刊 IEICE Trans. Communications 副编辑(Associate Editor) (2004-2005)、Asia Joint Conference on Information Security 国际会议大会共同主席(2013- 2015)、韩国信息安全学会(KIISC)访问理事(2011)、台湾的信息安全学会理事长(2012-2015)等，并负责举办第二届海峡

两岸信息安全研讨会(2013 年 9 月台湾高雄召开)、第四届海峡两岸信息安全研讨会(2015 年 1 月台湾南投召开)。目前杨教授是高雄师范大学教授、西安邮电大学特聘教授、西安电子科技大学 ISN 国家重点实验室客座教授。详细学经历及著作请参见 http://security.nknu.edu.tw/

主题报告 3：互联网时代的电子证据应用实践探讨

报告人：叶红　高级工程师

报告简介：

在实施互联网+行动计划和国家大数据战略的背景下，信息化已经深度融合在国民经济和社会生活中。国家安全、电子政务，电子商务以及百姓的社交生活都离不开网络，离不开数据，同时，各种法律问题不断出现，在涉网案件中电子证据作为最直接、最具证明力的证据形式，发挥着越来越重要的作用。但是，电子证据作为新型的证据形式，由于自身的电子属性，具有可复制、易修改、易删除的特点，如何证实其真实性、原始性？在电子数据成为电子证据的生成链条中，信息系统（平台）的所有者是否具有举证能力？谁可以出具的电子证据合法？可靠的电子证据应该具有什么特征？法庭应该怎样认定？等等问题有待探讨和解决。需求推动发展，针对上述问题，大量应用实践提供了可供研究和应用的范例，对其加以分析和讨论，将有利于电子证据的发展，使其成为为信息化社会提供法律保障的有力支撑。

报告人简介：

叶红，国家信息中心信息与网络安全部副主任、电子数据司法鉴定中心常务副主任，中国信息协会信息安全专业委员会秘书长，北京市司法鉴定业协会副会长，长期从事信息安全、灾难恢复、网络应急救援，电子数据司法鉴定等方面的研究和具体工作。具有丰富的理论知识和实践经验。参与研制全国第三次人口普查数据处理系统，并作为主要参加者获得国家科技进步一等奖；主持制定《应用级防火墙安全技术要求》，《存储介质数据恢复服务规范》等国家标准；主持起草司法部技术规范《电子数据司法鉴定通用实施规范》及北京市司法鉴定业协会标准《电子数据司法鉴定操作规范》；负责实施国家信息安全专项《存储介质数据恢复服务》、《国家重要信息系统安全可控性验证服务》和《信息系统个人信息保护标准体系建设及关键标准研究验证》以及国家 863 计划《智能终端的电子取证关键技术研究及应用示范》等项目。所负责的鉴定中心多次承担重大疑难案件的电子数据鉴定任务，协助公检法及政府部门在一些具有重大社会影响力的案件中发挥重要作用。

主题报告 4：电子支付取证方法研究

报告人：朱建明　教授

报告简介:

电子支付是电子商务的重要环节。针对电子支付过程，分析了电子支付中的取证要素，研究了电子支付取证的主要方法，提出了基于大数据的电子支付取证方案，为计算机取证提供了新的思想。

报告人简介：

朱建明，博士、教授、博士生导师，现任中央财经大学信息学院院长，2013 年获第九届北京市高等学校教学名师奖，美国 University of Texas at Dallas 访问学者。兼任教育部互

联网应用创新开放平台联盟常务理事，中国计算机学会理事、信息保密专业委员会委员、体系结构专业委员会委员，中国通信学会高级会员。主要从事信息安全、数据挖掘与隐私保护、互联网金融等方面的教学和科研工作。近年来，主持国家自然科学基金项目 4 项、省部级科研项目 4 项，出版著作和教材 11 部，发表学术论文 70 多篇。

主题报告 5：大数据取证技术的定位与规制

报告人：刘品新 教授

报告简介：

一、大数据取证的司法实践

（一）大数据挖掘

（二）大数据碰撞

（三）大数据搜索

（四）其他应用

二、大数据取证技术的法律定位

（一）侦查机关的职权行为

（二）大数据公司的协助行为

（三）其他性质

三、大数据取证技术的司法规制

（一）隐私保护

（二）令状制度

（三）收费制度

报告人简介：

法学博士，教授，硕士研究生导师，中国人民大学法学院证据学研究所副所长，中国人民大学刑事法律科学研究中心研究员，兼任中国行为法学会理事，中国电子学会计算机取证专家委员会委员，北京市刑事侦查学研究会常务理事，《证据学论坛》、《公安学论丛》副主编，中国人民大学物证技术鉴定中心鉴定人，北京市地石律师事务所律师，长期从事证据学、网络法、侦查学、物证技术学等领域的研究。近年来，代表性科研项目有国家社会科学基金年基金、最高人民检察院 2008 度检察理论研究课题、数据工程与知识工程教育部重点实验室（中国人民大学）开放课题、教育部人文社会科学研究等，出版著作 8 部，发表学术论文 50 余篇。曾获《中国电子证据立法研究》获首届全国信息化研究优秀成果奖三等奖 1 项，《中国电子证据立法研究》获第二届全国法学教材与科研成果三等奖 1 项，《证据法学》获第二届全国法学教材与科研成果一等奖 1 项。

主题报告 6：互联网金融犯罪及数字取证

报告人：孙国梓 教授

报告简介：

针对当前出现的互联网金融犯罪现象，分析互联网金融犯罪的基本特征，从数字取证的视角探讨互联网金融犯罪过程中可能涉及的相关技术、法律问题，针对互联网金融犯罪，从数据采集、数据存储、数据分析、证据生成等多层次对相关技术进行分析，为互联网金融犯罪取证提供必要的理论、技术基础，探讨可能存在的法律问题，为打击互联网金融犯罪提供基本支撑。

报告人简介：

孙国梓，博士，教授，南京邮电大学计算机技术研究所副所长，中国计算机学会、中国电子学会高级会员，香港 ISFS 会员，中国电子学会计算机取证专家委员会、中国人工智能学会智能数字内容安全专业委员会、江苏省计算机学会计算机安全专业委员会、计算机与通信专业委员会、嵌入式系统及设备专业委员会、江苏省电子学会信息安全专委会、江苏省微型电脑应用协会嵌入式系统专业委员会）委员（，全国计算机继续教育研究会江苏委员会理事。多年来一直从事电子数据取证、计算机网络及信息安全、云计算、智慧城市、企业信息化工程与电子政务工程的总体规划等相关理论和应用研究，在该领域具有较强的科研及实践能力。作为项目负责人或主要完成人先后参加过国家"973"计划、"863"计划、十五科技攻关计划、十一五科技支撑计划、国家自然科学基金、江苏省青年科技基金等多项科研项目。负责完成近 20 项与企业合作的科研项目。曾获省科技进步二等奖 1 项，市科技进步三等奖 1 项，发表科技论文 90 余篇，合作编写 2 部数字取证方向的专著。

主题报告 7：苹果系列产品的取证难点及一些新思路

报告人：尹文基　上海势炎信息科技有限公司总经理

报告简介：

随着 iPhone 等苹果公司的电子产品的流行，针对苹果公司电子产品的取证也逐渐发展成为一个独立的取证领域，形成了一系列的取证手段和产品形态，也出现了一些技术性难点。在本次演讲中作者将通过梳理苹果电子产品上取证的一些手段和方向的同时，针对 Mac 电脑固件密码，FileVault 全盘加密技术等一些技术性难点问题提出了新的思路，并将演示最新的研究成果。

报告人简介：

尹文基，资深的信息安全专家，上海势炎信息科技有限公司总经理，CISA、等级保护测评师，具有十多年行业经验。

主题报告 8：综合各种时间属性开展深层次调查和鉴定

报告人：郭永健　北京天宇宁科技有限公司 CEO/CTO

报告简介：

在不同的操作系统、Windows 注册表、应用程序的相关痕迹、元数据和系统日志，包含有各种不同的时间信息。如果能够充分挖掘、有效地利用时间属性，可以对电子数据的分析

和鉴定起到至关重要的作用。本报告，将针对不同数据类型的时间属性的手动和智能化分析技术进行探讨。

报告人简介：

郭永健，资讯保安及法证公会(ISFS) 中国大区联络官，中国电子学会计算机取证专家委员会委员，北京天宇宁科技有限公司 CEO/CTO。郭永健先生从 90 年代初即开始从事电子数据取证分析的研究，至今已有二十五年从业经验。郭先生于 2005 年创办了“CCFC 计算机法证技术峰会”，迄今为止已举办十一届，对推动国内计算机取证技术行业的发展作出了应有的贡献。郭先生在其二十多年的职业生涯中，测试、翻译并引进了大量国外优秀取证分析工具，他是德国 X-Ways Forensics，澳大利亚 Nuix Desktop，韩国 FinalData、FinalForensic，俄罗斯 BelkaSoft IM Analyzer、俄罗斯 Passware 等知名软件的汉化作者，也是各国际公司授权的培训讲师。他先后翻译出版了《iOS 取证分析》，参与撰写了《电子数据取证》MacOS 取证分析章节。此外，他围绕取证软件国产化发展趋势，主持开发了“星云邮件分析系统”、“星云手机取证系统”、“鉴证大师”、“MacOS 智能分析系统”。他是资讯保安及法证公会(ISFS)中国大区联络官，中国电子学会计算机取证专家委员会委员，中国政法大学法务会计研究中心客座研究员、辽宁警院公安信息系客座教授，取证中国论坛 MacOS 取证版主。

主题报告 9：第六代电子数据取证模式

报告人：吴少华　厦门美亚柏科第二研究院计算机取证研发中心副总监

报告简介：

简要回顾历代电子数据取证模式的发展历程和特点，并指出第五代取证模式面临的主要问题，介绍第六代电子数据取证模式的特性，并对镜像分析同步、数据预处理、分布式计算、全文检索、数据挖掘等模式特性进行展开介绍，最后介绍新取证模式在实战中如何运用，并对未来的发展方向进行展望。

报告人简介：

吴少华，现任厦门美亚柏科第二研究院计算机取证研发中心副总监、产品经理，有着 8 年 IT 领域技术及项目管理经验，熟悉国内外计算机取证技术，负责多款计算机取证装备及系统的研发工作，具有丰富的计算机取证经验。

日程详细

11 月 20 日（星期五）

09:00 - 21:00　报到、注册

18:30 - 20:00　晚餐（凭代表证在融金中财大酒店就餐）

11 月 21 日（星期六）上午

08:30 - 09:00　会议开幕式（中央财经大学 学术会堂 202）

主持人：中央财经大学 信息学院院长 朱建明 教授

主持人介绍与会嘉宾

中科院高能物理研究所网络安全实验室首席科学家许榕生研究员致词

09:00 - 09:20　全体代表合影留念（中央财经大学 校门口）

09:20 - 12:00　大会主题报告（中央财经大学 学术会堂 202）

大会主题报告（一） 主持人：朱建明 教授		
时间	**报告题目**	**报告人**
09:20 - 09:55	电子取证——一个越来越被关注的研究领域	丁丽萍（中国科学院软件研究所研究员、中国电子学会计算机取证专家委员会主任）
09:55 - 10:30	移动取证软件的设计与实践（Design and Implementation of Mobile Forensic Software）	杨中皇（高雄师范大学教授）
10:30 - 10:50	茶歇	
大会主题报告（二） 主持人：丁丽萍 研究员		
10:50 - 11:25	互联网时代的电子数据保全与鉴定	叶　红（国家信息中心信息与网络安全部副主任、高级工程师）
11:25 - 12:00	电子支付取证方法研究	朱建明（中央财经大学教授、中央财经大学信息学院院长）

12:00 - 13:00　午餐（中央财经大学专家宾馆）

11 月 21 日（星期六）下午

13:30 - 17:00　论文宣讲论坛

论坛概览

时间	论坛专题	地点
13:30 - 14:30	网络取证	中央财经大学学院南路校区 学术会堂 202
14:30 - 15:10	智能终端取证	
15:30 - 16:10	电子证据鉴定技术和规范	
16:10 - 16:50	取证与反取证	

论坛详细

论文宣讲论坛（一）　主持人：李洋 副教授		
时间	**报告题目**	**报告人**
13:30 - 13:50	一种基于 URL 语法规则的欺诈网站识别方法	孙国梓
13:50 - 14:10	网络取证技术研究	夏东冉
14:10 - 14:30	基于增量学习和主动学习的垃圾邮件识别新方法	王友卫
14:30 - 14:50	网络传销的电子证据分析	刘志军
14:50 - 15:10	电子数据取证中 windows 系统下的时间属性鉴定讨论	李　毅
15:10 - 15:30	茶歇	
论文宣讲论坛（二）　主持人：廖鑫 博士		
15:30 - 15:50	基于 Android 智能终端微信应用的数字取证分析模型的研究	何　月
15:50 - 16:10	移动恶意代码攻击数字证据取证调查处理程序之研究	张志宋
16:10 - 16:30	两款隐写软件信息隐藏的取证	李金才
16:30 - 16:50	AES 密钥隐藏方法研究	吴紫鹏

18:00 - 19:30　晚餐（北京天宇宁科技有限公司赞助）

11 月 22 日（星期日）上午 中央财经大学学术会堂 706

08:30 - 08:50 优秀论文评选

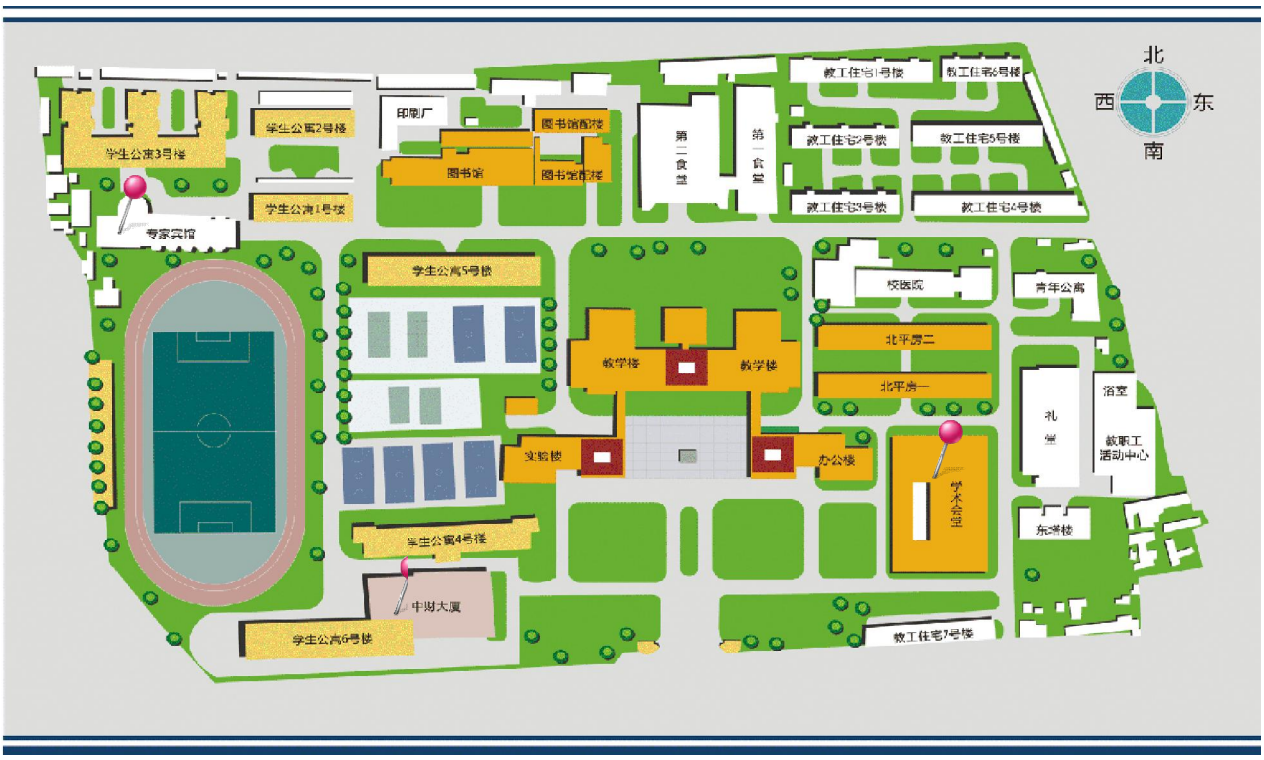
08:50 - 12:00 大会主题报告

大会主题报告（三） 主持人：石文昌 教授		
时间	报告题目	主讲人
08:50 - 09:15	大数据取证技术的定位与规制	刘品新（中国人民大学教授、中国人民大学法学院证据学研究所副所长）
09:15 - 09:50	互联网金融犯罪及数字取证	孙国梓（南京邮电大学教授、南京邮电大学计算机技术研究所副所长）
09:50 - 10:25	苹果系列产品的取证难点及一些新思路	尹文基（上海势炎信息科技有限公司总经理）
10:25 - 10:50	茶歇	
大会主题报告（四） 主持人：王立梅 副教授		
10:50 - 11:25	综合各种时间属性开展深层次调查和鉴定	郭永健（北京天宇宁科技有限公司 CEO）
11:25 - 12:00	第六代电子数据取证模式	吴少华（厦门市美亚柏科信息股份有限公司第二研究院计算机取证研发中心副总监）

12:00 - 13:00 午餐（中财大厦）

会议地点（中央财经大学学院南路校区）

会场示意（中央财经大学学院南路校区）



联系会务

会议总负责：段美姣　13581986862

会务联系人：胡鸿雁　13810689983，　廖鑫　18674388210

住宿餐饮联系人：李洋　13691119321