学校编码：10384
学号：X2012231205

分类号____密级___
UDC___

厦门大学

工 程 硕 士 学 位 论 文

计算机取证实验室管理系统设计与实现

Design and Implementation of Computer Forensic Lab Manager System

张艺宝

指 导 教 师： 林 坤 辉 教 授

专 业 名 称： 软 件 工 程

论文提交日期： 2015 年 6 月

论文答辩日期： 2015 年 7 月

学位授予日期： 年 月

指 导 老 师：_____

答辩委员会主席：_____

2015 年 6 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果,均在文中以适当方式明确标明,并符合法律规范和《厦门大学研究生学术活动规范（试行)》。

另外,该学位论文为(　　)课题(组)的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。(请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。)

声明人（签名)：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（ √ ）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

进入 21 世纪以来，计算机和网络技术为主导的信息技术正在发生着革命性的变革。伴随着信息技术的飞速发展，越来越多的信息化管理系统已经进入各行各业，为其提供了包括审计、管理、信息归档等各方面的服务，可以说信息技术已经改变了人们的工作、生活甚至是思考方式，与此同时，计算机犯罪和网络违法犯罪案件也变得非常普遍。存在电子设备中的电子证据逐步成为司法部门的重要诉讼依据。因此，计算机取证作为一门新兴的学科正逐步被人们所重视。计算机取证技术是一门涉及法律学、证据学、刑事侦查学、计算机及网络技术的综合性学科。在美国 70%的法律部门拥有专门的计算机取证实验室。目前，我国也在各地公安部门中逐步建立计算机取证实验室。针对这一发展，开发一套规范化、信息化程度较高的计算机取证实验室管理系统，对电子证据的获取、管理等系列操作，具有较高的实用性。本文针对案件管理部门对于电子取证系列操作的管理需求，设计一个计算机取证实验室管理系统，为电子取证操作提供自动化、流程化、规范化、高效化服务。

本文设计的计算机取证实验室管理系统（CFLMS，Computer Forensic Lab Manager System）基于现代化 WEB 开发技术，采用 B/S（Browser/Server，浏览器/服务器）框架结构，使用基于 JavaScript 实现 RIA 技术进行系统前台开发，同时后台数据库采用了 SQL Server 进行开发，完成对数据的存储、管理和日常维护，与服务器交互采用异步方式，减少了用户等待的时间。CFLMS 主要功能包含：送检单位管理，委托单管理，检材管理，设备管理，图表统计以及系统设置，上级单位可以对下级单位进行管理，并查看其所接受案件情况。设计过程中利用统一建模语言(UML，Unified Modeling Language)对 CFLMS 系统进行需求分析、概要设计、详细设计，并设计测试用例完成系统测试。实际应用后证明，CFLMS 能够优化计算机取证实验室的工作流程，提高实验室日常工作管理效率。

关键词：计算机取证；软件设计；数据库应用

Abstract

Since the 21st century, computer and network technology as the leading information technology is undergoing a revolutionary change. Along with the rapid development of information technology, more and more information management systems have entered into all walks of life, which provided auditing, management, information archiving and so on. At the same time, Computer Crime and Internet Crime are growing up. The electronic evidences become so important in judical field that the electronic forensics received more attention. The electronic forensic is a comprehensive technology which combines with jurisprudence, science of evidence, science of criminal investigation , science of computer and technology. In America, 70% of justice department are supported by Computer Forensic Labs(CFL).In China, CFLs are also growing up. A kind of standardized and informationized manager system for CFL is badly needed, which is helpful to improve the CFL's daily work. For this requirement, we designed a Computer Forensic Lab Manager System to provide the automatized, standardized, streamlined and highly-efficient service for electronic forensic works.

In this thesis, a Computer Forensic Lab Manager System(CFLMS) will be designed. We will use B/S(Browser/Server) technology, rich Internet application , JSP technology .The database is developed by SQL Server, which complete the data storage, management and daily maintenance. The main functions of CFLMS include: inspection agency management, case management, inspection material management, equipment management, graphical statistic and system settings. Superior unit can manage the subordinate units and view their accepted cases. Using UML(Unified Modeling Language) to describe CFLMS's requirement analysis, system design, and designing cases for system testing. It is approved that CFLMS can optimize the computer forensic working flow and speed up the CFL's daily work.

Key Words: Electric Forensics; Software Design;Database Application

目 录

Contents

第一章 绪 论

1.1 课题研究背景和意义

早在大约 5 万年前，语言的出现为信息的传播提供了有效的载体，这给人类进化和文明的传播带来了契机。从大约公元前 3500 年文字的出现，到公元 1040 年活字印刷技术的使用，到 19 世纪电报、电话、广播的发明，20 世纪计算机技术以及其与网络技术的有机结合，再到 21 世纪海量数据存取技术的发展及其应用，人类已经进入到了信息时代。计算机技术的普及使得人们可以方便的利用其提高自己的生活质量以及工作效率，结合互联网技术，人们在信息时代的生活以及工作方式更是得到了革命性的改变。

随着信息技术的飞速发展，数据越来越多的以电子形式存储，伯克利大学研究报告就指出，以电子形式存储的数据量占数据总量的 92%以上，这个比例还在不断增加。与此同时，在司法领域中涉及到电子证据的案件也日渐增多，而这些证据的获取涉及到了证据学、刑事侦查学、计算机等多种学科，人们针对这些问题进行研究，也就出现了电子取证这门新兴的学科。所谓“电子取证”，既恢复已被破坏的计算机数据及提供相关的电子资料证据，因其涉及学科较多，因而电子取证往往缺少规范化，目前针对电子证据的管理出现了诸多问题亟待解决[1]，这其中包括：

1、计算机取证实验室[2]管理方式相对落后，以至于实验室管理工作效率相对较低。这种落后的管理方式体现在国内大部分的同类型实验室管理主要依赖人工管理，缺少专业管理软件对实验室信息和业务流程进行整合。现存的大多数的软件仅是利用计算机完成信息的录入、存储等功能，不得不说对于强大的网络以及现代计算机系统是一种资源的浪费，同时这种管理方式的后果导致了管理系统的混乱，进而致使管理工作者的工作效率较低。

2、现行计算机取证实验室管理系统开发所用技术相对落后，扩展性、可移植性较差。目前被广泛使用的管理系统依然采用传统的 C/S（Client/Server,客户机/服务器）模式进行开发，这种模式开发的系统受到客户机（Client）以及原有程序的制约，其可移植性及其扩展性都受到很大限制，通常其扩展、维护都需要

专业人员进行操作，使得其长期使用受到一定限制，无法满足日益变化的功能需求。另一方面，这种技术开发的软件因为偏重功能性，通常其界面并不友好，这导致管理机构需先对其员工进行一定培训才能投入使用，一定程度上增加了使用成本。

3、管理信息结构化混乱。案件委托单的管理通常包括了收领、预检、受理审核、检测、报告审核、结案等过程，而这其中涉及了关于案件的各种信息，另外包含了检材管理员、审核员、检验鉴定员、授权签字人、文件管理员、设备管理员、超级管理员等角色信息，管理系统信息结构化程度不高，导致了各个模块、各个角色之间配合难度加大。随着信息量的增大，后续管理越来越复杂和困难，这致使后续工作中由于管理人员操作失误导致信息流逝，给管理机构带来不必要的麻烦和损失。

4、管理系统数据时效性较低。案件委托单管理工作环环相扣，由于缺乏统一的管理，数据的组织分散无规则，致使下一环节的工作无法及时得到上一环节数据而不能正常进行，这就导致工作流无法顺利进行，一定程度上影响了管理机构办事效率。

5、信息交互性较差。现行管理系统流程之间缺少信息交互，业务中途处理失败，不能时回退。各个人员之间的工作的交互缺少规范化管理。

利用便捷的网络构建先进的计算机取证实验室管理系统对鉴定流程进行监管以及对产生的委托方信息、案件信息、委托单信息数据进行管理，对进一步提高电子取证的效率，提高系统数据的安全性和可靠性，有着广泛的发展应用前景和较高的实用价值。

鉴于实验室管理中所遇到的问题，结合现代软件技术的发展与广泛应用，利用计算机和当代计算机网络，本文意在设计一套计算机取证实验室管理软件，用于规范实验室操作，通过该系统高效、便捷的对实验室进行统一的管理。拟设计的模块主要包含：送检单位管理模块、案件管理模块、检材管理模块、设备管理模块、报表统计模块、系统模块，通过这些模块的配合作用，完成既定的规范化管理目标。架构方面，本系统将采用 B/S（Browser/Server，浏览器/服务器模式）架构，客户端使用浏览器通过网络对系统进行访问，以此提高系统的扩展性和移植性。另一方面，系统中集成扫描枪、条码打印机、光盘刻录打印机、检材柜、

预检工作台等设备，使系统功能更加完善，实验室管理形成一套规范化、合理化的工作流程[3]。系统在实现鉴定流程规范化的前提下，通过合理的布局、结合已经集成的自动化设备来有效减少工作量，对于提高管理单位工作办事效率有着极其重要的意义[4]。

1.2 国内外研究现状

电子取证源自于美国 FBI 的计算机分析相应组（CART），上世纪八十年代，工作人员结合实际工作中遇到的案件对计算机取证技术进行了研究，电子取证的概念正式形成。依托计算技术的发展，电子取证技术在九十年代中期得到了飞速发展，各种计算机取证（Computer Forensic）技术层出不穷，然而这一时期的电子取证技术缺少统一的标准对其进行规范，一定程度上限制了其推广和规模化。电子取证的规范化研究和基本方法的完善大概在 2000 年左右，出现了较多较为优秀的电子取证产品，这其中包括美国 GUIDANCE 公司开发的 Encase、德国 X-Ways 公司开发的 X-Ways Forensics、美国计算机取证公司开发的 FTK 等一系列的计算机取证系统。国内对于电子取证的研究起步相对较晚，但近十年依赖发展速度较为迅速。首先是国家各项法律法规的支持，这些法规包括了 1999 年的《中华人民共和国合同法》、2002 年的《中华人民共和国电子签名法》、2002 年的《最高人民法院关于民事诉讼证据的若干规定》、2013 年正式实施的新修订的《中华人民共和国刑事诉讼法》和《中华人民共和国民事诉讼法》以及公安部起草发布的各项检查规则和检测方法。在产品方面也有美亚柏科信息股份有限公司的 ForensicsMaster、上海盘石公司的 SafeAnalyzer 等产品。

实验室信息管理系统(LIMS)[5]，Laboratory Information Management System，它是由计算机硬件和应用软件组成，能够完成实验室数据和信息的收集、分析、报告和管理的系统[6]。

早在上世纪 60 年代末期，美国的一些高校并开始使用计算机处理化学实验数据[7]，这被认为是 LIMS 的雏形。随着局域网技术发展，出现了更加完善的解决实际问题的个性化方案，然而这些方案针对不同客户的实际需求解决问题，尚未形成完善的体系结构，因而其推广和发展受到了极大的制约。进入 90 年代后，随着网络技术的发展以及计算机的普及，C/S 结构，即 Client/Server(客户机/服务

器)结构，通过将任务合理分配到 Client 端和 Server 端，降低系统的通讯开销，充分利用两端硬件环境的优势，成为了早期的软件系统多以此作为首选设计标准。

互联网技术的飞速发展改变了诸多人们的工作与生活方式，人们的出行、居家、购物都可以通过互联网使其更加方便。开发者们更是顺应时代的潮流，将 LIMS 系统的 Client 用浏览器的方式进行实现[8]，使得需要专门在客户机上的软件变成了用于统一规范的网页标准，其兼容性、可移植性大大提高，这也就是当下最为主流的 B/S 框架结构，即 Browser/Server(浏览器/服务器)结构。较小的开发维护成本体现了一种节约资源的环保意识，并且极大的提高使用单位的办事效率。

在中国，基于 C/S 的 LIMS 在上世纪 90 年代便以不同的形式引入中国。然而，限于科技发展的滞后性，这种系统的引入往往需要高额的费用，LIMS 在中国各行各业的使用、普及收到了极大的限制和影响。进入 21 世纪以来，随着国家信息产业的不断推动与发展，很多高校、企业、政府部门纷纷开发自主知识产权的管理系统[9]，中国的各行各业也正在大踏步的迈入信息化时代[10]。在科教、卫生、通讯服务等各行各业出现了各式各样的实验室管理系统[11]，这些改变着人们的工作、生活方式，当然相对于国外发达国家，中国的信息化普及程度仍然有待提高[12]。

1.3 本文主要工作及结构

1.3.1 主要工作

本文对实验室管理系统的发展做了深入的剖析，通过对相关技术的对比分析、需求分析，确定了使用 B/S 框架结构结合 ASP、SQL 等技术进行系统开发，尝试实现用于计算机取证实验室的管理系统开发。本文主要工作具体如下：

1、介绍了实验室管理系统（LIMS）的发展，详细分析了实验室管理系统存在的问题，并结合国内外研究现状以及案件管理特点，讨论了系统的可行性，并最终确定了本文的主要工作，拟实现计算机取证实验室管理系统（CFLMS）。

2、通过对比介绍相关技术，确定了基于 B/S 框架的系统开发方案；进行了详细的需求分析，并使用相关技术进行实际的系统开发，最终完成了 CFLMS 的

开发，实现了既定的送检单位管理、委托单管理、检材管理、设备管理、图表统计、系统设置等功能。

3、进行了实际功能测试，验证了系统功能的完备性。

1.3.2 组织结构

第一章：绪论，主要介绍课题的研究背景以及选题意义，分析了国内外实验室管理系统研究现状，并论证了开发一套专门性的计算机取证实验室管理系统的必要性。同时对本文主要工作进行了总结，对文章的章节安排做了介绍。

第二章：相关技术介绍，本章介绍了系统开发架构，包括两种开发模式以及其对比分析；数据库相关技术，包括数据库概述以及访问等技术；介绍了包括 www、HTML、CSS 在内的相关 Internet 技术；系统开发技术，包括 ASP 技术以及系统开发的脚本语言。

第三章：需求分析，本章首先从操作可行性、技术可行性两方面对 CFLMS 的开发进行了可行性分析，然后对计算机取证实验室管理流程进行了介绍，并以此为基础，针对系统要实现的功能，分别从案送检单位管理、委托单管理、检材管理、设备管理、图表统计、系统设置等方面进行了功能需求分析。最后对系统进行了性能需求分析。

第四章：系统设计，本章根据开发需求完成了本系统各项功能的设计，利用面向对象的设计方法给出了系统静态类图、关键模块时序图、系统部署图以及数据库的逻辑设计和物理设计方案。

第五章：系统实现，本章将系统各个功能模块的具体实现情况做了详细描述，并给出每个功能模块的实现界面及操作方法。

第六章：系统测试，本章对所设计系统进行了功能性测试，包括测试环境搭建、设计测试用例、测试评估等方面的内容。

第七章：总结与展望，针对本文设计中存在的优缺点进行总结，并对系统的扩展研究工作进行了展望。