项目编号： 密级：

中国人民公安大学

2021年国家级大学生创新创业训练计划

申 请 书

项目类别： 2021年大学生创新创业训练计划

项目名称：

所属一级学科： 公安技术学

项目所属单位： 信息网络安全学院

项目负责人： 钟宜均

负责人学院： 信息网络安全学院

负责人专业： 2019级网络安全与执法专业

指导教师： 高见

申报日期： 2021年12月5日

校团委制

二〇二一年五月

填写说明

一、申报书请按顺序逐项填写，填写内容必须实事求是，表达明确严谨。空缺项要填“无”。

二、封面中的项目编号由学校统一编排填写，密级由学生所在院（系、部）学生科研领导小组和项目指导教师确定，不涉密的项目留空。

三、申请参加本次学生科研项目团队的人数含负责人在内不超过5人，指导教师不超过2人。

四、对提供虚假材料或信息数据不实者，将取消申报资格，并承担相应责任。对于填写不合要求、内容含糊不清、字迹潦草者，不予受理。

五、申请书中字体务必严格遵守格式规范，页面不够时可加页，不得破坏后面表格的完整和美观。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 项目名称 | | | | | |  | | | | | | | | | | | | | | | |
| 项目级别 | | | | | | 国家级 | | | | | | | | | | | | | | | |
| 起止时间 | | | | | | 2021年 12月 至 2022年 5月 | | | | | | | | | | | | | | | |
| 项目负责人 | 基本情况 | | | 姓 名 | | 钟宜均 | | | 性别 | | 男 | | 出生年月 | | 2002年5月 | | 政治面貌 | | | | 共青团员 |
| 联系电话 | | | 13375653505 | | | | | E-mail | | | 945881066@qq.com | | | 学号 | | 202021240033 | |
| 学业  能力  、  项目经历  、  获奖  情况 | | | 本人学习能力较强，综测排名位于中队前茅。本人热衷于学习，乐于钻研，刻苦学习，崇尚真理，善于发现生活中的趣事并加以研究。本人积极与老师交流，虚心向老师请教，求取知识，力图进步，得到老师们的认可。本人身心素质良好,工作认真负责，一丝不苟，责任感强，擅长与人交往，善于团结同学。  曾在2020年获得蓝桥杯初赛二等奖；强网杯CTF竞赛“强网先锋”；美亚杯数字取证竞赛一等奖；柏鹭杯CTF竞赛优胜奖。在各项CTF赛事中获得较高的排名，目前主攻软件逆向工程和数字取证方向的内容，通过自学完成汇编语言、编译原理、Android程序设计等课程，在内存取证方面也有所学习。 | | | | | | | | | | | | | | | | | |
| 项目团队 | 姓 名 | | | | 性别 | | | 学号 | | 年级、专业、区队 | | | | | | 项目分工 | | | | | |
| 1 | | 莫中睿 | | 男 | | | 202021240021 | | 2020级安全防范工程四区队 | | | | | | 软件框架设计、软件开发 | | | | | |
| 2 | | 杨双源 | | 男 | | | 202021470042 | | 2020级网络实验班 | | | | | | 算法破解、工程实现 | | | | | |
| 3 | | 胡文强 | | 男 | | | 202121710039 | | 2021级数据警务技术二区队 | | | | | | 前期调研与文献搜集、软件开发 | | | | | |
| 4 | | 王誉霖 | | 男 | | | 202121720042 | | 2021级数据警务技术二区队 | | | | | | 文献搜集与整理、实验 | | | | | |
| 项目指导教  师 | 姓 名 | | | | 性别 | | | 年龄 | | 行政职务/专业技术职务 | | | | 研究专长 | | 所在单位 | | | 联系电话 | | |
| 1 | 高见 | | | 男 | | | 39 | | 副教授 | | | | 网络安全与执法 | | 信息网络安全学院 | | | 13401007485 | | |
| 2 |  | | |  | | |  | |  | | | |  | |  | | |  | | |
| 第一项目指导教师的业务特长与主要学术成果 | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |

|  |
| --- |
| **一、项目简介**  随着以智能手机为代表的高科技移动设备的迅速发展，微信已经成为人们日常生活必不可少的沟通工具。截至2021年第三季度，微信的月活用户已达12.62亿，微信聊天记录已经成为传递信息、记录事实的重要载体，在检察院起诉、法院审判过程中发挥着重要的作用。2020年5月1日，《最高人民法院关于修改〈关于民事诉讼证据的若干规定〉的决定》正式开始施行，这意味着微信聊天记录已经能够作为法定证据而具有法定效力，也给公安机关的电子取证能力提出了更高的要求。  本项目以软件逆向工程和密码学算法为基础，计划设计一款能够自动识别微信聊天记录是否被篡改过的取证软件，这将对我国移动设备取证发展有着积极的影响。 |
| **二、文献综述**  (一)、引言         我们团队在对微信取证的实际过程中发现，在一定情况下，可作为重要物证之一的微信聊天记录能被涉案人员轻易地篡改。根据最高人民法院《解释》第93条规定，对于电子数据应当着重审查以下内容：（3）电子数据内容是否真实，有无删除、修改、增加等情形，因此在取证时警方需设法检测聊天记录是否存在篡改痕迹以核实聊天记录的真实性。  根据前期研究发现，微信使用SQLite数据库储存聊天记录，涉案人员既能通过修改数据库中的数据实现静态篡改，也能通过设置断点劫持用户消息实现动态篡改，这两类篡改方法的成本均极低且易于实现，实际案件中会给公安机关电子取证的真实性认定带来巨大的困难。因此，一款能以高效率、高准确率的方式来检测微信聊天记录篡改痕迹的软件将能够大大减轻侦查人员的工作压力，具有很高的实用价值。  (二)、背景及技术介绍  1.相关背景  1.1检测微信聊天记录篡改痕迹的重要意义  《刑事诉讼法》第50条规定电子证据为我国诉讼证据的一种，因此电子取证也是公安机关侦查工作中极为重要的一环。实际应用中，电子证据一般从真实性、关联性、合法性三个方面进行认定。对于电子证据真实性认定，一是指确认电子证据的来源、形式、制作过程及设备情况等正常，无被修改破坏的痕迹；二是要审查电子证据的内容是否真实、有无剪裁、拼凑、伪造、篡改等。电子证据真实性的认定结果，直接决定了证据能否作为证明案件事实的材料，甚至对于案件的进展有决定性作用。考虑到微信广泛的应用范围，微信聊天记录的取证将成为侦查人员取证工作的重点，聊天记录中篡改痕迹的检测将成为取证的关键步骤。  2.技术简介  2.1 Xposed框架(Xposed Framework)         Xposed框架由XDA开发，是一套开源的、在Android高权限模式下运行的框架服务, 可以在不改变应用程序代码的情况下改变Java层代码的输出结果。(如图1)  图 1——安卓的层次结构  在这个框架下可以加载多种插件App，这些插件APP可以直接或间接劫持、篡改、伪造一些信息，理论上进行微信聊天记录真实性鉴定的插件APP可以hook到系统任意一个Java进程，如zygote、systemserver或systemui并进行相关操作。         Xposed原理：通过替换 /system/bin/app\_precesss 程序控制zygote进程，使得它在系统启动的过程中会加载Xposed framework的一个jar文件即XposedBridge.jar，从而完成对Zygote进程及其创建的Dalvik虚拟机的劫持，并且能够允许开发者独立地替代任何class，例如framework本身，系统UI或者其他任意App（如取证对象微信等）。除此之外，这种方法亦不会使ROM与App产生任何变化，一定范围内不会影响其他物证的鉴定。  2.2逆向工程（Reverse engineering）  逆向工程（又称逆向技术），是一种产品设计技术再现过程，即对一项目标产品进行逆向分析及研究，从而演绎并得出该产品的处理流程、组织结构、功能特性及技术规格等设计要素，以制作出功能相近，但又不完全一样的产品。逆向工程源于商业及军事领域中的硬件分析。其主要目的是在不能轻易获得必要的生产信息的情况下，直接从成品分析，推导出产品的设计原理。  软件逆向工程技术主要指对软件的结构，流程，算法，代码等进行逆向拆解和分析，基于某个软件，以反汇编阅读源码的方式去推断其数据结构、体系结构和程序设计信息的技术，主要用于软件维护，软件破解，漏洞挖掘，恶意代码分析。 |
| **(三)．研究方法**  1.基于聊天记录数据库文件与索引比对实现的静态纂改痕迹取证  安卓系统基于Linux内核，使用轻量级数据库SQLite作为复杂数据的存储引擎。通过前期所进行的的安卓逆向工程（使用Jeb工具对安卓反汇编代码进行分析），本团队已确认微信进行用户数据存储的本地端SQLite的具体位置： /data/data/com.tencent.mm/MicroMsg/<usereid>/EnMicroMsg.db （如图2）。  图片 2  经分析，该数据库不仅存储了该微信用户的聊天记录，还包含了其好友列表、朋友圈记录等多种高价值信息。通过安卓逆向工程得到的反汇编代码分析，已知其数据库文件使用开源的SQLCipher作为其加密工具，加密算法为AES，并使用了CBC( Cipher Block Chaining) 加密模式和256位长度的密钥。后期工作中本团队将对该加密工具的源码与汇编代码进行分析，推出密钥对数据库文件及解密，进行纂改实验，并尝试对静态纂改及其检测原理进行探索。  2.聊天记录动态Hook篡改原理研究  此类纂改方法基于Xposed框架，由于安装Xposed框架相当于是对安卓的Kernel层进行更改，因此研究人员在使用Xposed框架之前，须先取得手机的Root权限。取得Root权限后可通过Hook技术对聊天框控件进行追踪，找到源码当中对聊天框定义的代码部分。结合之前得到的微信APK反汇编代码进行分析，编写Xposed的Hook插件对聊天信息的调用函数进行劫持，更改其中的变量内容，完成对聊天内容的更改。  3.基于逆向工程和密码学对聊天记录静态篡改取证  经前期调研发现，微信没有内置聊天记录的数据库文件的哈希计算和比对，因此当篡改者对EnMicroMsg数据库文件进行更改后我们无法通过哈希校验的方式对其是否更改进行取证。经分析，微信在保存聊天记录时使用了与EnMicroMsg.db在一个文件夹下的FTSIndexMicroMsg\_encrypt数据库文件来作为聊天信息的索引(见图3)，  图片 3  该文件与EnMicroMsg同样采用sqlcipher工具进行加密，但本团队结合APK反汇编代码进行分析发现，FTSIndexMicroMsg\_encrypt.db与EnMicroMsg.db未使用同一密钥进行加密，因此需要再次使用安卓逆向工具对反汇编代码进行分析，找出密钥对数据库文件进行解密，再将索引文件与EnMicroMsg文件中的数据进行关键字比对，并以此判断聊天记录是否被篡改。 |
| 4.基于Xposed框架实现原理的聊天记录篡改痕迹取证  Xposed框架虽基于Kernel层，但其插件还是在Java层进行实现的，所以在使用的过程中会或多或少留下痕迹。由于动态Hook篡改聊天记录是基于微信本身算法劫持实现的，所以无法像静态取证一样去分析校验数据库文件。本项目通过检测Xposed在系统中留下的痕迹来检测微信的聊天记录是否被更改过，Xposed在动态执行过程中会有很多行为可以被我们调用系统函数来检测和记录，进程执行完之后这些信息部分会以日志的形式存储到系统文件中。因此我们可通过分析不同的日志来对Xposed Hook微信的执行记录进行取证。  (四)．实验设计及结果预测  1.实验意义：  本项目实验意义在于测试所开发软件效果能否到达预期。  2.实验材料：  3部相同型号的已Root的安卓手机，测试软件  3.实验步骤：  分别对3台手机进行对应的如下操作：  1)微信聊天记录静态篡改 2)微信聊天记录动态篡改 3)不做任何篡改  然后分别用测试软件进行检验，得出检验结果进行记录  恢复手机初始化设置，重新进行多次相同实验，记录每次结果  4.结果预测  筛选掉无用数据之后结果应趋近于100%准确。  (五)．存在的问题与未来展望  1.可能存在的问题  由于微信是腾讯公司所开发的闭源通信软件，难以得知某些功能的具体实现与技术细节，且微信的更新频率较高，本团队难以无法预测微信未来更新对聊天记录在本地端的存储方式和加密方式作出的改变，因此本项目只对微信5.0至8.0版本的聊天记录纂改取证鉴定有参考意义。未来随着微信的版本更新，本团队还得继续跟踪相关技术细节的更新。  2.对于未来的展望  智能手机等移动设备的兴起和不断发展，给人民生活带来许多便利之处，但也给许多不法分子带来了可乘之机。因此，移动设备取证技术也在近几年迅速发展。自最高人民法院宣布微信聊天记录可以作为法定证据之后，我国公安机关愈加重视针对微信的取证技术的研究。目前的研究大多数是基于对微信证据的提取与分析，随着科技的不断进步，不难猜测将会有越来越多的不法分子依靠科技手段对证据进行破坏和篡改，这就将会给取证人员提取完整而有效的证据带来越来越多的阻力。因此，对于证据完整性和真实性性的取证技术研究也将会是未来取证技术研究的一个重点方向。  (六)．结语  在国内来看，微信以其他软件无可比拟的便利性和实用性，成为了我国人们使用频率最高的移动通信软件之一。许多不法分子利用微信牟取私利，甚至利用一些科技手段销毁自己违法犯罪的证据。为响应国家打击网络违法犯罪的号召，公安机关和取证人员必须要不断提升以智能手机等移动设备为代表的高科技产品的取证本领，特别是在现在犯罪分子犯罪的科技水平不断提高的大社会背景下，一些证据的真实性和完整性难以得到确认。因此公安机关和取证人员在继续开展证据提取的研究之外，逐步开展对证据真实性和完整性验证的相关研究，全面确保证据真实、完整、充足。 |
| **三、申请理由**  团队优势：  本团队成员平日学习刻苦仔细认真，编程能力较强，具有较为扎实的知识功底。团队搭配合理，成员大部分拥有Java编程和取证经验对项目的研究有帮助，同时也有善于搜索资料、撰写论文的成员，团队成员都对科研具有强烈热情，希望能够在项目中发挥所学，为做出贡献。  项目负责人钟宜均，2020级安全防范工程专业本科生。曾自学C++、Python、Java等多种语言，有过多次逆向工程项目经验，能较为熟练的进行Android项目开发，曾协助黑龙江省哈尔滨市反诈中心在案件侦办取证部分中做出重大贡献并收到感谢信，在校期间多次参加计算机类竞赛，目前取得过2020蓝桥杯二等奖，2021美亚杯电子取证竞赛一等奖，2021柏鹭杯CTF竞赛优胜奖，参加过祥云杯CTF，NCTF等多场CTF竞赛并进入决赛，已通过计算机三级考试，NISP一级考试等。现在主要专攻方向是逆向工程和数字取证，希望能通过这次机会为科研事业贡献一份自己的力量。  项目参与人莫中睿，2020级安全防范工程专业本科生，连续两次获得校级一等奖学金，对科研有着浓厚的兴趣，自学了有关Python和自然语言处理方面的知识，自学C++、Java等编程语言且有过相关软件开发经验，积极参加校内外学生竞赛并多次取得优异成绩，获得全国大学生数学竞赛全国三等奖、北京市二等奖。  项目参与人杨双源，2020级网络安全与执法专业本科生，在CTF竞赛中主攻Web方向，对SQL，Oracle等数据库较为熟悉，能独立进行网站开发与维护，具有较强的代码分析和编写能力，熟练掌握C、Python、PHP、Java、Go、Javascript和css等编程语言，具有丰富前后端开发和网站渗透经验，在2021年美亚杯电子取证竞赛中取得三等奖，参加过祥云杯CTF，NCTF等多场CTF竞赛并进入决赛，同时参加过科研项目，具有一定的科研经验。  项目参与人胡文强，2021级数据警务技术专业本科生，高中起学习C、C++、Java并多次参加竞赛，掌握一定的数据库操作方法，对Linux操作系统的操作与结构较为熟悉，能进行一些网络服务器搭建和维护工作，曾在KDE Plasma 桌面开源项目中贡献过自己的力量。2021年入校以来曾参与过某科研项目的数据分析工作，自行学习逆向工程等相关知识，在网络特警队的新生赛中获得第一名。  项目参与人王誉霖，项目参与人王誉霖，2021级数据警务技术专业本科生，高中起学习Python编程语言并多次参加竞赛。本人2021年入校以来曾参与过某科研项目分析工作。成员们熟练掌握本软件开发时所需要的各种技术。本着能学能干、吃苦耐劳、不怕输不认输的优良作风，本团队一定能够在项目进展中攻坚克难并取得最终的胜利。  已具备条件：  前期团队为了了解项目的意义，成员与指导老师积极沟通，已经把握项目研究方向和创新点，力求在该研究方向有所突破；后又咨询多个相关领域的研究人士，了解项目的实用意义与领域研究现状。  项目已经规划了具体的实施方案，将具体任务落实到相关负责人上，  在项目开展之前，团队内成员均预先通过学习掌握了项目所需技术和知识，也都有过取证实践或竞赛相关经历。 |
| **四、项目实施方案及进度安排**  计划、技术路线、人员分工等，按月份或季度列出。  时间安排  1、现状调研阶段（2021年12月）持续1个月  准备阶段（2021.12.5-2021.12.10）  项目组全体成员通过视频会议讨论研究，制定详细的研究计划和人员分工安排。  调研与环境搭建阶段（2021.12.10-2021.12.31）  在知网上搜寻微信等取证研究的文献资料；通过网络渠道了解相关软件逆向工程思路和密码学算法；搭建研究所需要的开发环境。  2、理论研究与实现阶段（2021.1.1—2021.3.1）持续2个月  理论研究阶段(2021.1.1—2021.1.31)  通过文献资料以及项目组自身实践对原理进行研究，结合编程知识和最终程序设计提出合理的解决方案和软件结构框架。  实现阶段(2021.2.1—2021.2.28)  对原理进行复现，在工程上实现和验证解决方案，结合具体情况对解决方案做出调整。  3、软件设计与调试阶段（2021.3.1-2021.3.31）持续1个月  软件设计阶段(2021.3.1—2021.3.20)  结合工程实现的具体情况和前一阶段的软件结构框架，进行软件的开发.  软件调试阶段(2021.3.21—2021.3.31)  在不同的环境中对软件的兼容性和稳定性进行软件调试。  4、实验和反馈阶段（2021.4.1—2021.4.30）持续1个月  实验阶段(2021.4.1—2021.4.15)  通过设计多组对照实验的形式对软件效果进行测试，统计并记录实验结果。  反馈改进阶段(2021.4.16—2021.4.30)  分析实验数据，为软件和解决方案作出合适的调整，完善软件设计。  5、项目定稿结题，撰写论文（2021.5.1—2022.5.31）持续1个月  完成设计方案，并撰写论文，定稿，结题。 |
| 人员分配  钟宜均：逆向研究、工程实现  莫中睿：软件框架设计、软件开发  杨双源：算法破解、工程实现  胡文强：前期调研与文献搜集、软件开发  王誉霖：文献搜集与整理、实验开展 |
| **五、特色与创新**  1.当前移动设备取证研究的主流方向为证据提取，本项目创新性的提出对移动设备证据的完整性和真实性进行检测，可以为以后取证研究方向提供新的思路。  2.本项目基于实际出发，考虑当前公安取证工作的具体情况，开发了可视化的软件来解决问题，可以大大节省公安取证工作的人力和物力，提高取证工作的效率，更符合公安在实战取证工作的需要。  3.当前已经被广泛使用的一些取证工具综合性更强，体量大，但严重缺乏专一性，且受制于平台和设备环境的限制。本项目开发的工具更加轻量化，专一性强，更具有针对性，可以不受制于设备环境。 |
| **六、预期成果**  结项论文（一份）：关于上述微信聊天记录篡改痕迹取证软件搭建的技术细节的报告  软件（一件）：微信聊天记录篡改痕迹取证软件 |