2024 第四届
全国网络空间取证竞赛

<参赛手册>

FORENSIX IN CYBERSPACE

指导单位：中国刑事科学技术协会

主办单位：FIC网络空间取证峰会组委会

承办单位：浙江警察学院 上海弘连网络科技有限公司

2024年4月

FORENSIX IN CYBERSPACE

FORENSIX >>>
IN CYBERSPACE

目 录

一、竞赛目标

为推动电子数据取证相关专业人才培养工作，提高电子数据取证能力和水平，促进电子数据侦查取证技术的发展，由中国刑事科学技术协会指导、FIC网络空间取证峰会组委会主办、浙江警察学院和上海弘连网络科技有限公司承办的第四届全国网络空间取证竞赛（简称“FIC竞赛”）定于2024年4月27日举行线上赛，参赛选手将对模拟的真实案例进行电子数据调查取证，全面验证选手电子数据取证的综合素质和能力。

二、竞赛时间

2024年4月27日 13:00-17:00

FORENSIX >>>
IN CYBERSPACE

三、赛程安排

第四届全国网络空间取证竞赛 日程表			
日期	**时间**	**内容**	**发布地点**
4月20日	18:00前	公布检材镜像文件下载地址 公布《参赛手册》	大赛QQ群/FIC官网
4月26日	12:00	公布比赛平台地址	大赛QQ群/教师群
	12:00-20:00	选手测试比赛平台 并修改初始密码	大赛QQ群
	19:00-21:00	赛前会议（仅领队/指导老师参加）	腾讯会议
4月27日	12:30-12:45	开幕式	直播平台
	12:45-13:00	公布检材挂载密码/解压检材	大赛QQ群/直播平台
	13:00-17:00	正式比赛	比赛平台
4月28日	全天	成绩复核 答辩环节(组委会将从拟获奖队伍中抽查10支队伍进行答辩)	腾讯视频会议
4月29日	13:00	公布线上赛获奖名单	FIC官网
		单项定点通知决赛入围名单	官方邮件
	19:00-20:30	赛后复盘	直播平台
备注	1.请确保团队所有成员均在大赛 QQ 群内能及时接收相关竞赛信息，若还未加入，请搜索群号647746302加入。 2.请确保高校领队老师在微信沟通群。 3.比赛平台(飞客实训平台)首次登录信息：用户名为报名手机号，初始密码为报名学生证号。		

四、竞赛秩序

为了维护良好的比赛秩序，请各队选手诚信参赛、独立解题。同时，请各高校领队/指导老师安排好监考工作，保证比赛公平、公正地进行。

1、比赛期间每个参赛选手使用的电脑需**全程录屏**，如果对成绩有异议，录屏将作为赛后提出申诉或申辩的重要依据，直接影响申诉或申辩的成功与否。

2、比赛结束后，组委会将会第一时间在大赛QQ群发起问卷统计，各参赛选手须在**赛后2小时内将录屏文件的Hash（SHA256）值提交到问卷统计表单中，便于组委会进行成绩复核工作**，录屏软件使用和设置参考详见附录。

特别提醒，在系统重启后请重启录屏软件。

3、如发现有选手恶意攻击比赛平台、交换答案或解题思路等违规情况，视情节严重程度可能会被处以通报批评、禁赛、取消成绩、公示或通知学校等处罚。

4、参赛选手赛前需认真阅读并签署**《诚信参赛承诺书》**，参与比赛即视为认可并同意其中全部条款。

五、竞赛形式

1、本次比赛的考试形式为线上团队赛答题，团队内成员共同参与作答同一套比赛题目，具体流程为：

- 成员登录各自账号进行答题；
- 各参赛队伍根据题目要求，结合案情简述对检材进行分析，提交结果；
- 比赛时间未结束时，若参赛队伍需提前交卷可点击结束答题，**但结束后不可再继续作答任何比赛题目或修改答案。**
- **请特别注意：三名队员共享一张电子试卷，每道题仅有一次提交机会！任意队员作答并提交过答案的题目，三名队员均无法进行修改。**

2、本次竞赛题型为填空题/选择题，选手需要注意：

- 务必使用不低于109版本的Chrome浏览器或Edge浏览器进行答题，因使用低版本浏览器或其他浏览器导致的题目提交失败/错误等问题，组委会将不予追溯。

请务必仔细阅读题干，**关注答案格式要求和示例，特别是大小写、全半角符号；**

强烈建议：尽量不要在比赛接近结束时集中提交答案，以免因网络波动造成不必要的损失。

六、竞赛内容

包括但不限于：计算机取证分析、手机取证分析、虚拟化平台分析、服务器分析、网站重构、数据库分析、文件隐写分析、AI痕迹分析、软路由分析、数据恢复、密码破解等。

七、检材下载

链接：https://pan.baidu.com/s/1pJDwwNy14o-kAstHkndWPg?pwd=1234

提取码：1234

八、案情简介

2024年4月，卢某报案至警方，声称自己疑似遭受了“杀猪盘”诈骗，大量钱财被骗走。卢某透露，在与某公司交流过程中结识了员工李某。李某私下诱导卢某参与赌博游戏，起初资金出入均属正常。但随后，李某称赌博平台为提升安全性，更换了地址和玩法，转为通过群聊抢红包形式进行赌博。随着赌资不断增加，卢某投入巨额资金后，发现无法再访问该网站，同时李某也失去联系，卢某遂意识到自己被骗。在经济压力下，卢某选择报警，并承认参与赌博活动，愿意承担相应法律后果。

警方依据卢某提供的线索和手机数据，迅速锁定犯罪团伙，并在一藏匿地点成功抓获犯罪嫌疑人李某和赵某。警方对嫌疑人持有的物品进行了证据固定：李某手机被标记为检材1，窝点内服务器为检材2，赵某使用的计算机为检材3。

接下来，请取证工作者根据案情和这些检材进行深入分析，并解答后续问题。

九、取证工具

参赛队伍根据比赛内容各自准备，建议包含如下类别：

容器软件，推荐VeraCrypt1.25.9版本；镜像挂载软件，如FTKimager等；虚拟机环境，如VMware等；屏幕录像软件；介质取证分析软件；手机取证分析软件；服务器取证分析软件；程序功能分析软件；文本查看、十六进制查看、编解码等通用工具。

FORENSIX >>>
IN CYBERSPACE

附录一

视频录制要求

请设置好录屏参数，保证录制的视频区域为所有显示器的全部区域。录制视频对帧率和质量不作强制要求，能清晰展现出解题主要过程即可。

录制视频格式保存时选择flv格式，参赛选手务必在赛前提前录制4小时视频以进行测试。比赛结束后2小时内，按前文所述要求，将视频Hash（SHA256）值提交至QQ群中发布的问卷统计中，如有多段视频，则打包后计算压缩包SHA256值并填入。

所有参赛队员的屏幕录像需保存至4月30日。入围决赛的队伍视频需保存至决赛结束后方可删除。

推荐录屏软件的使用方式参考附录二。

附录二

ForensicRecorder 软件安装及使用说明

一 安装包下载

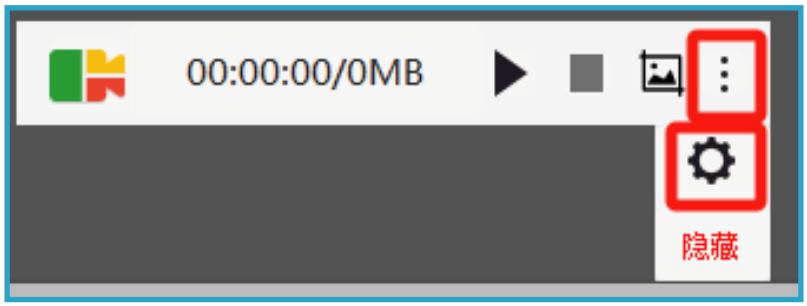
下载链接：

https://update.forensix.cn/api/download/ForensixRecorder/63969c986897479aee27bf63/?fast=true

通过链接弘连取证录像软件即可下载ForensicRecorder软件安装包，安装完成后双击打开。

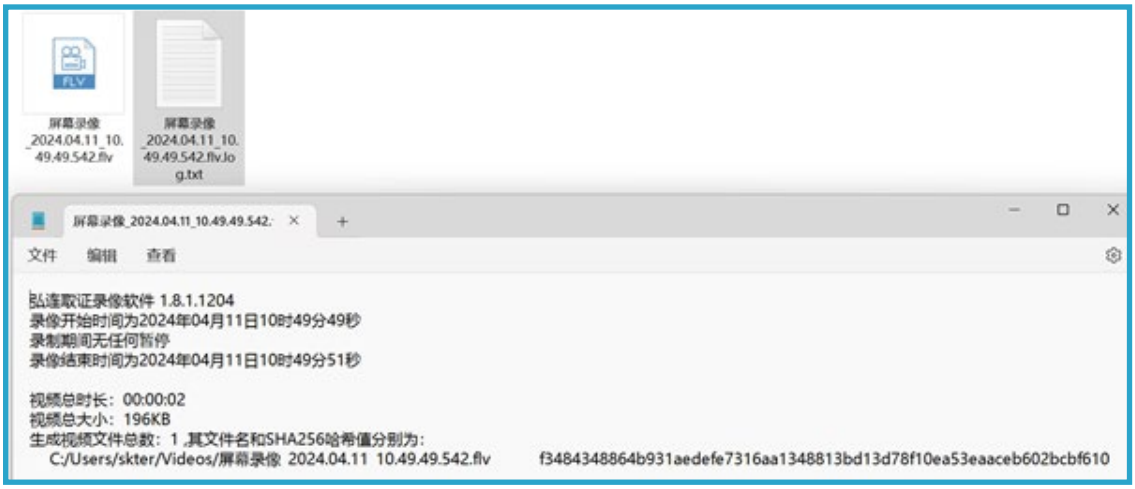
二 软件介绍

1、软件运行后将出现在屏幕上方，整个界面主要由左侧软件LOGO、中间录制时间/大小、右侧操作区域组成；



2、点击右侧操作区域的设置按钮可以打开设置菜单，菜单中主要包括了基础设置、音视频设置、快捷键设置及关于；

3、点击上方的开始按钮，选择“整个屏幕”并开始录制。录制结束后点击结束，将自动生成哈希值。



扫一扫 了解更多FIC资讯