第四届“长安杯”电子数据取证竞赛
参赛手册

为促进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，推动电子数据侦查取证技术的发展，由西安电子科技大学主办的第四届“长安杯”电子数据取证竞赛拟于 **2022 年 10 月 29 日**在线上举行。参赛选手将对模拟的真实案例进行电子数据调查取证，以全面检验电子数据取证的综合素质和能力。本赛事为非营利性竞赛，旨在以赛促学、以赛代练的同时选拔优秀专业人才。

一、赛场秩序

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，请各分赛场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需全程出镜接入组委会所要求的**腾讯会议**。
2. 比赛期间每个参赛选手使用的电脑需全程录屏，并在赛后将录屏文件按要求提交组委会，录屏软件使用和设置参考详见附录。
3. 赛中和赛后会有核实成绩的电话，组委会可能会和领队老师交流并要求参赛选手回答相关问题，请注意接听。

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、公示或通知学校**

等处罚。参赛选手赛前需认真阅读诚信参赛承诺书，参与比赛即默认选手及其参赛队伍知晓并接受《**诚信参赛承诺书**》的要求。

组委会将于 10 月 28 日前将会议链接和录屏文件提交方式通过比赛相关群发送给参赛选手和指导老师。

二、 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：
    - 成员可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：每道题仅有一次提交机会！**
2. 本次竞赛题型为**填空题**，选手需要注意：
    - 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。

三、竞赛内容

包括但不限于：介质取证分析、文件隐写、服务器/网站重构分析、

数据库取证分析、应用程序功能分析、加密解密、手机取证分析。

四、赛程安排

日期	时间	内容	发布方式
10 月 25 日	12:00 前	公布**下载比赛检材镜像链接校验值**	大赛 QQ 群/官网
10 月 26 日	12:00 前	公布**参赛手册**	大赛 QQ 群/官网
10 月 28 日	12:00 前	公布比赛平台地址	大赛 QQ 群/指导教师群
	14:00-20:00	选手测试比赛平台并修改初始密码	比赛平台
	19:00-21:00	赛前会领队指导老师会	**腾讯会议**
10 月 29 日	8:00	公布检材挂载密码	比赛平台/大赛 QQ 群
	8:15	发布静态题目（pdf）	大赛 QQ 群
	8:00-8:30	开幕式/解压检材	各分赛场/在线（主）赛场
	8:00-12:00	**正式比赛**	**在线/各分赛场**
	12:00-12:30	**宣布获奖名单**	在线/b 站直播
10 月 29 日	14:00-18:00	领队填写在线问卷 确认正式获奖名单	领队微信群
	19:00-20:30	**赛后复盘**	在线/b 站直播
11 月 2 日	9:00-18:00	官网公示比赛成绩 上线证书电子版和邮寄纸质版	
备注	1. 请确保团队至少一人在大赛 QQ 群内能及时接受相关竞赛信息，若还未加入，请搜索群号 780484048 加入； 2. 请确保领队老师在领队老师微信群。 3. 比赛平台（飞客实训平台）登录方式:手机号和初始报名密码登录；ctf.changancup.com		

五、检材下载

链接：https://pan.baidu.com/s/1f9xzt0jooZ-RZylwtt3YvQ

提取码：1234

SHA256:37263f0aace3e33e7f303473e85e69ef804eb16a2500b68a6b90c895784666f5

六、案情简介

某地警方接到受害人报案称其在某虚拟币交易网站遭遇诈骗，该网站号称使用“USTD 币”购买所谓的“HT 币”，受害人充值后不但“HT 币”无法提现、交易，而且手机还被恶意软件锁定勒索。警方根据受害人提供的虚拟币交易网站调取了对应的服务器镜像并对案件展开侦查。

七、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 VeraCrypt1.25.9 （推荐此版本）、屏幕录像软件，vmware 虚拟机环境，介质取证软件，手机取证软件，服务器取证软件，程序功能分析软件，以及文本查看、十六进制查看、编解码等通用工具。

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，建议视频质量控制在 7MB/min 左右，有条件的选手建议在赛前录制 4 小时视频以进行测试。（不建议选手选择 mp4 等格式，万一录制过程遇到蓝屏、断电等异常情况，引起录制过程意外中断时，会导致所生成的视频文件损坏）。

比赛结束后组委会将通过在线方式收集录屏文件（视频文件命名：**学校+队伍名称+选手姓名.flv**），届时会给出提交视频的方法。

附录二和附录三给出了两种视频录制软件的使用方法和推荐设置，以供参考。

附录二：

ForensicRecorder 软件安装及使用说明

一、安装包下载

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、界面介绍

1、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；

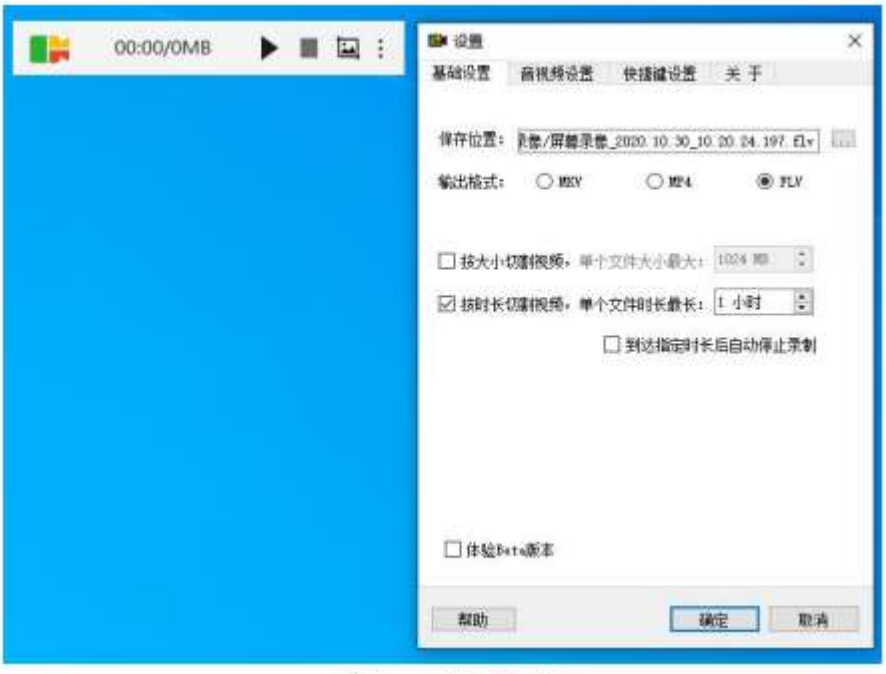


图 1 界面介绍

三、功能介绍

- 指定需要录制的屏幕，可以单独指定某一个屏幕或者多块屏

幕合并录制。

1、点击右侧操作区域的【▸录制】按钮，软件会在下侧自动显示出屏幕列表；

2、指定您想要录制的屏幕（例如：屏幕 #1、屏幕 #2、所有屏幕等）；

3、单击后，录制任务即会开始；

4、点击右侧操作区域的【■结束】按钮，录制即会结束，软件会自动打 开录制视频的保存位置。

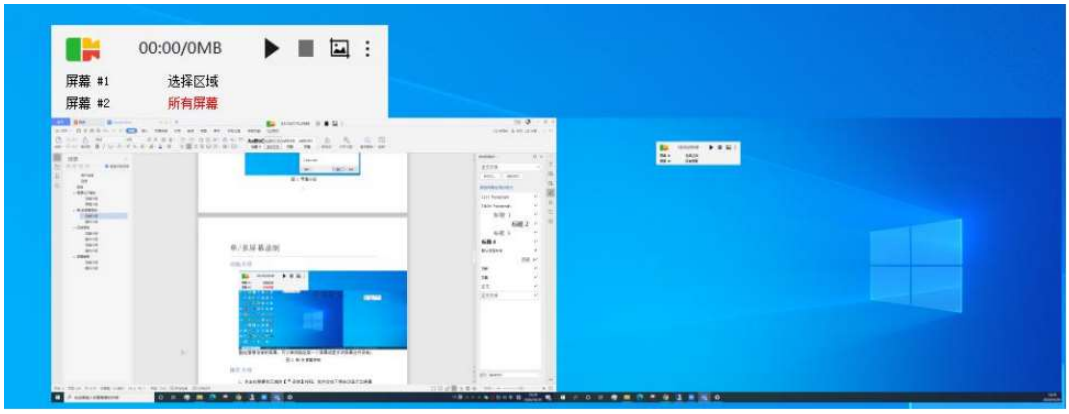


图2 单/多屏幕录制

- 选择指定区域或者窗口，只录制这个区域或者窗口中的内容；

1、点击右侧操作区域的【▸录制】按钮，软件会在下侧自动显示出【选择区域】选项（可设置快捷键）；

2、鼠标画出您需要录制的区域大小，如果是窗口的话，软件会自动吸附出对应窗口的大小；

3、单击【录制】按钮后，录制任务即会开始；

4、点击右侧操作区域的【■结束】按钮，录制即会结束，软件

会自动打开录制视频的保存位置

图3 区域录制

- 选择有滚动条的窗口，比如浏览器、word 文档、qq 微信聊天窗口等等， 软件会自动帮您缓慢拖动滚动条进行录制；

1、点击右侧操作区域的【录制】按钮，软件会在下侧自动显示出【选择区域】选项；

2、鼠标画出您需要滚动录制的窗口，软件会自动吸附出对应窗口的大小；

3、单击【滚动录制】按钮后，自动滚动窗口录制任务即会开始；

4、点击右侧操作区域的【结束】按钮，录制即会结束，软件

会自动打 开录制视频的保存位置。

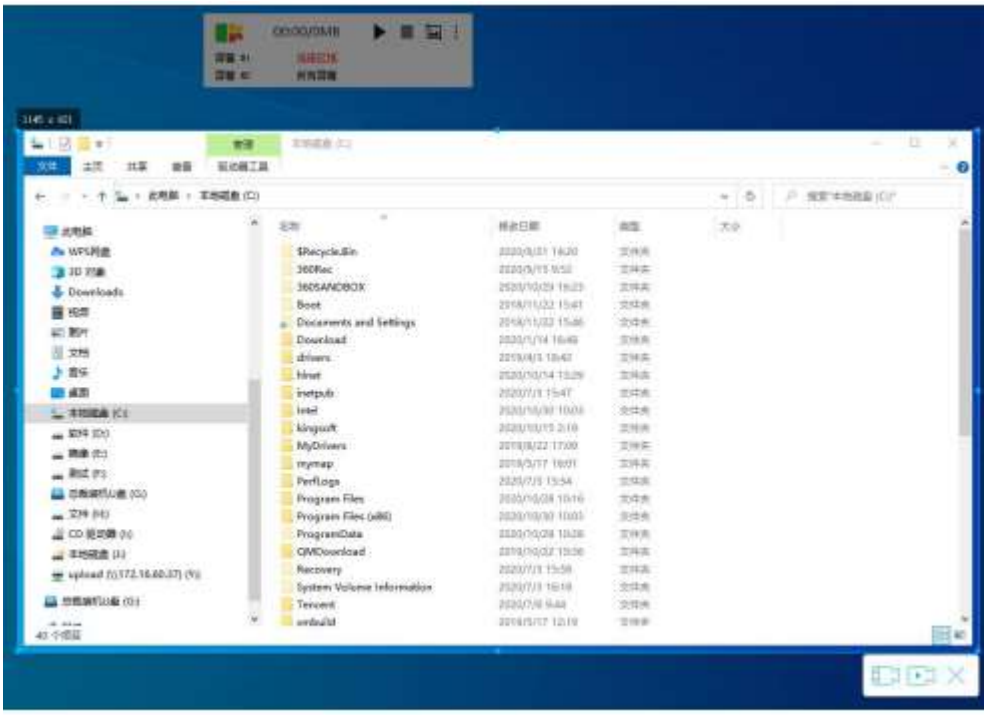


图4 自动滚动窗口录制

- 选择区域进行截图操作，可以保存到文件，也可以保存到剪贴板(可通过双 击右键快速复制)；

1、点击右侧操作区域的【▸录制】按钮，软件会在下侧自动显示出【选择区域】选项；

2、鼠标画出您需要截图的区域，如果是窗口，软件会自动吸附出对应窗口的大小；

3、单击【✓确定】按钮后，截图会保存到剪贴板中；单击【✕取消】按钮后，放弃本次操作；单机【保存】，截图会保存到默认目录。

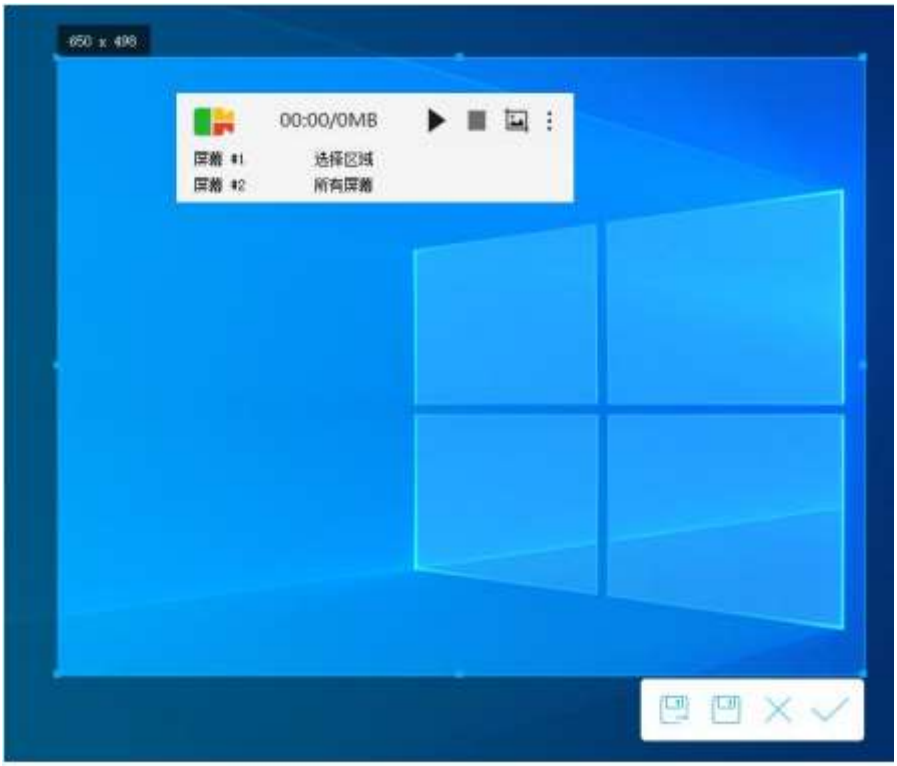


图5 屏幕截图

四、推荐视频输出设置

点击视频录制软件图标，点击“设置”。在“基础设置中”设置输出格式为 FLV；在“音/视频设置”中视频的帧率设置为 5，质量设置为 1。

附录三：

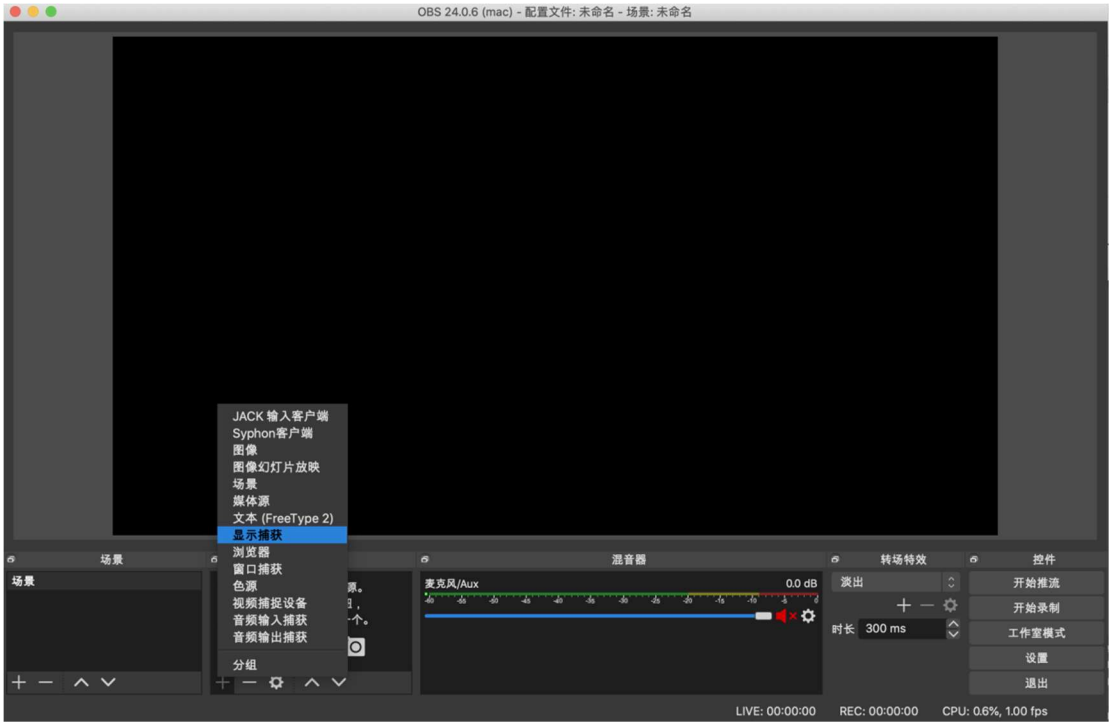
OBS 软件安装及设置说明

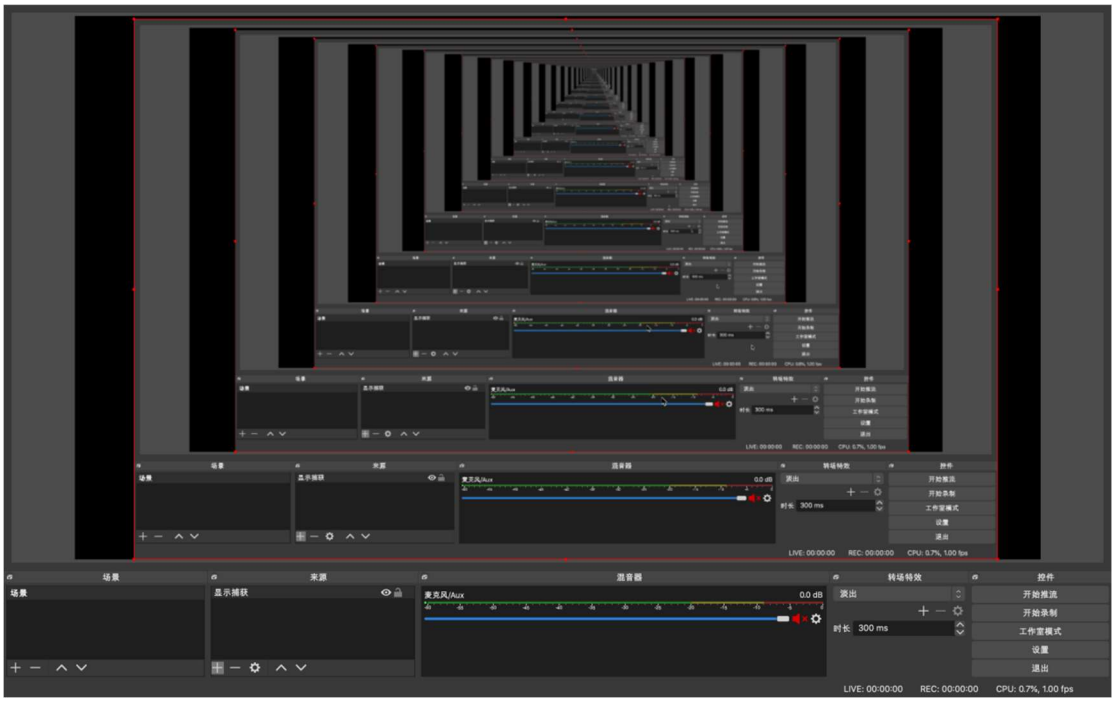
一、软件安装

前往 https://obsproject.com/ 下载对应系统的安装包并安装，安装完成后双击打开。

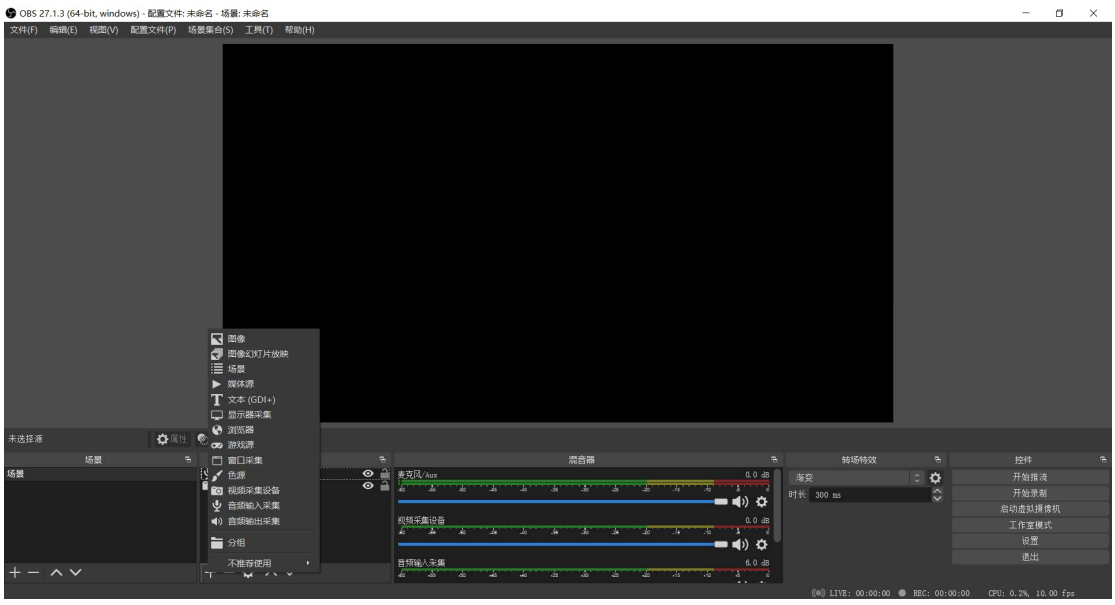
二、设置来源

- 在主界面“来源”处点击加号，选择“显示捕获”并确定。此时在工作区显示屏幕捕捉的内容，然后通过**拖动视频四周的红色边框调整捕获视频大小，使屏幕内容全部显示在工作区中。**





- 如若在主界面“来源”处点击加号后没有“显示捕获”，如下图，请点击“显示器采集”，点击两次确定即可（按照默认设置即可）。

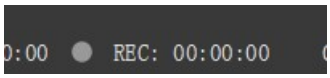


三、使用说明

- 开始录制：点击主界面“开始录制”后开始进行屏幕录制。当

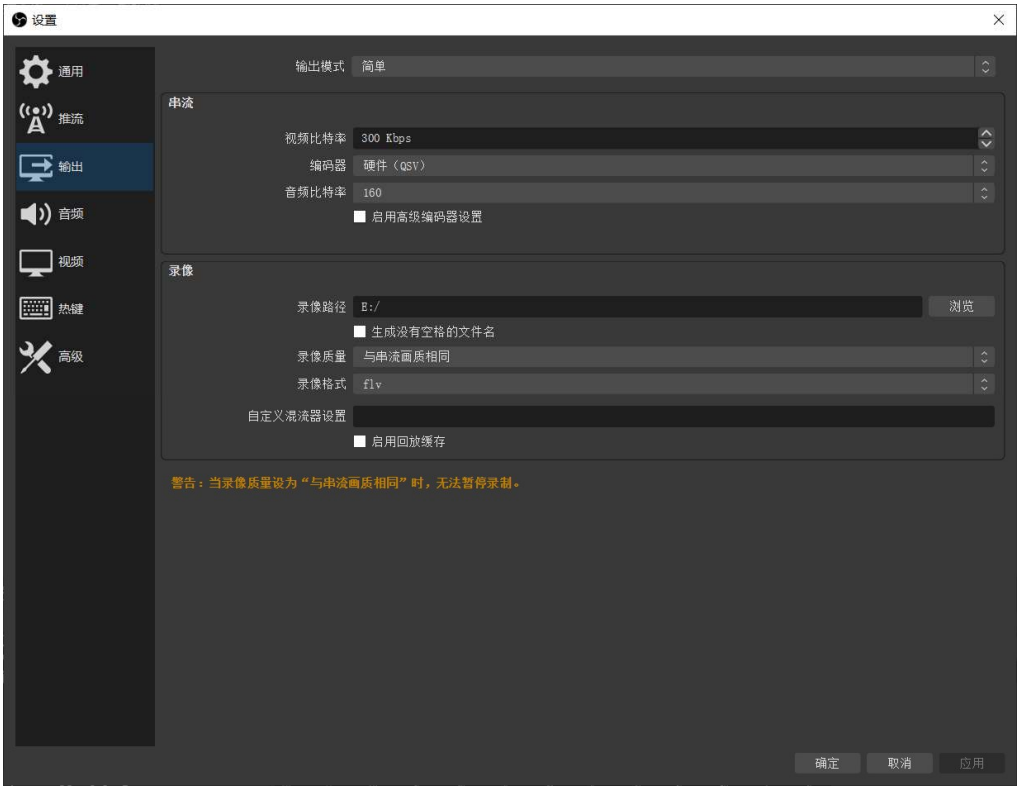
右下角 REC 旁为红灯时即开始了录制：

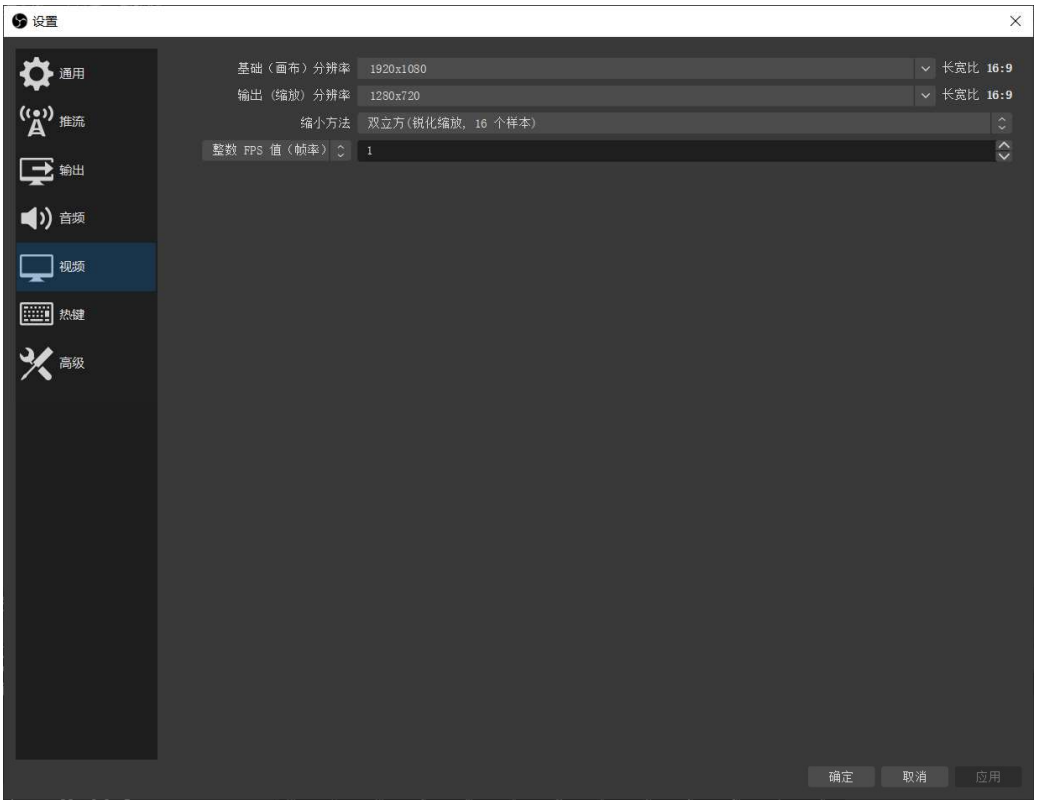
- 结束录制：点击主界面“停止录制”后，若右下角 REC 旁灯仍为红灯时，需要再次点击“停止录制”，当 REC 旁为灰色时，说明录制结束：



四、推荐视频输出设置

点击主界面“设置”->“视频”（Windows 是“文件”->“设置”），调整输出分辨率为 **1280x720**，基础画布分辨率不变。在下拉菜单中选择设置整数 **FPS 值（帧率）为 1**。在“设置”->“输出中”设置视频比特率为 **300kps**，设置录像路径（即视频保存路径），设置录像格式为 **flv**，录像质量为**与串流画质相同**。




设置
通用
推流
输出
音频
视频
热键
高级
基础（画布）分辨率
1920x1080
长宽比 16:9
输出（缩放）分辨率
1280x720
长宽比 16:9
缩小方法
双立方（锐化缩放，16 个样本）
整数 FPS 值（帧率）
1
确定
取消
应用