2023年安徽省职业院校技能大赛高职组赛项规程

一、赛项名称

赛项编号：GZ087

赛项名称：司法技术

赛项组别：高职学生组

赛项归属专业大类：公安与司法大类

二、竞赛目的

本赛项旨在落实 “坚持全面依法治国，推进法治中国建设”和国家“建设数字中国”战略，协同推动法治和数字化的深度融合，深化司法体制综合配套改革，促进司法公正，推进法治中国建设，赋能经济社会和现代职业教育高质量发展。

（一）引领教学改革

通过司法技术技能竞赛检验、展示高职院校公安与司法相关专业教学改革成果以及学生岗位通用技术与职业能力。引领职业教育“三教”改革，提高现代司法职业教育技术技能人才培养质量，促进现代信息数字化司法人才高质量就业、服务稳定社会发展。

（二）强化专业建设

赛项衔接国家司法技术类、公安技术类高职相关专业教学标准，涉及“狱侦情报工作实务”“现场勘查技术”“狱内案件侦查实务”“笔迹鉴定技术”“文件鉴定技术”“手印鉴定技术”“数字取证技术”“监所信息网络建设与维护”“计算机网络攻击与防护”“信息安全管理实务”等课程，赋能相关专业群“信息化、标准化、数字化、国际化”建设规划，实现中国特色高水平现代化专业的建设。

（三）促进产教融合

赛项基于司法技术领域主流技术设计，通过司法、公安行业专家与院校教育专家紧密合作，完成竞赛内容向教学改革的成果转化，实现以赛促教、以赛促学、以赛促改、科教融汇的教产融合的赛事创新。

三、竞赛内容

本赛项为团队赛，竞赛内容选取司法技术中网络安全运维、现场勘查与司法

鉴定等核心技术，主要包括“司法技术技能素养”“物证检验与数字取证技能”和“监所网络安全和信息系统运维技能”三大模块。

(一)考核重点

竞赛重点内容包括以下三个部分：

模块一：司法技术技能素养（分数占比 30%）

考核形式: 主要考察司法鉴定、现场勘查、安防技术、信息安全等技术等理论技能的客观题。

任务 1：单选题，考核司法鉴定、现场勘查、安防技术、信息安全等技术等理论技能。

任务 2：多选题，考核司法鉴定、现场勘查、安防技术、信息安全等技术等理论技能。

任务 3：判断题，考核司法鉴定、现场勘查、安防技术、信息安全等技术等理论技能。

模块二：物证检验与数字取证技能（分数占比 40%）

考核形式: 主要考察文件鉴定、痕迹鉴定、数字取证等司法鉴定岗位的职业技能，选取司法鉴定仿真案例，模拟办案。

任务 4：案例分析题，考核手印鉴定技术、印章印文鉴定技术、笔记文痕鉴定技术，以及考核分析研判指印、寻找发现细节特征、特征比对法、重叠比对法、画线比对法制作检验图表等技术能力。

任务 5：操作系统数字取证技术，考核依照技术标准规范进行操作系统取证分析，基于取证软件与平台进行取证操作。

任务 6：网络取证技术，考核依照技术标准规范进行网络犯罪的取证，基于网络数据的获取和分析、网络通信的追踪和定位等操作。

模块三：监所安防技能和信息系统运维技能（分数占比 30%）

考核形式：主要考察系统安全和信息系统运维岗位的实操技能，使用模拟器和虚拟机模拟真实系统安全运维操作。

任务 7：司法管理信息系统安全运维，主要考核学生在真实环境下按照等保要求安全架构、渗透测试、攻防实战、电子取证、基于 Windows 平台进行数据恢复等司法信息安全领域的核心技术技能。

任务 8：网络安全运维技术运用，主要考核网络中软硬件的安全配置，内容主要涉服务器的安全加固、防火墙的配置与维护等工作。

任务 9：监所数字安防技术运用，主要考核学生在真实环境下按照设置完成对人脸管理服务器，视频监控、门禁系统、边缘计算服务器等安防领域的技术技能配置。

(二) 赛项模块、比赛时长及分值配比如下表

表 1 竞赛具体内容表

序号	内容模块	具体内容	说明
模块一	司法技术 技能素养	司法鉴定、现场勘查、安防技术、信息安全等理论技能	单选、多选、判断； 共 200 道题。
模块二	物证检验与数字取证技能	物证鉴定技术	涵盖手印鉴定技术、印章印文鉴定技术、笔记鉴定技术、检验分析、检验图表和司法鉴定意见书的制作分析等实务操作，以及基于网络数据的获取和分析、网络通信的追踪和定位等操作。
		网络取证技术	
模块三	监所网络安全和信息系统运维技能	监所信息管理系统安全攻防	监所安防设备的配置及管理；服务器的渗透测试和系统故障数据恢复、网络取证技术、数据挖掘和关联分析、系统安全配置和防火墙配置、信息化系统项目建设与攻防等实务操作。
		监所数字安防技术运用	

(四)学生组竞赛分值权重和时间分布

表 2 竞赛分值权重和时间分布一览表

序号	具体内容	比赛阶段	权重	竞赛时间
模块一	技能素养	阶段一	30%	120 分钟
模块二	物证鉴定技术	阶段二	20%	240 分钟
	网络取证技术		20%	
模块三	监所信息管理系统安全攻防		20%	
	监所数字安防技术运用	阶段三	10%	20 分钟/组

四、竞赛方式

（一）学生组竞赛组队

本赛项为团体赛，以院校为单位组队参赛，不得跨校组队，同一学校报名参赛队不超过4支。每支参赛队由3名选手（设队长1名）和不超过2名指导教师组成。

（二）竞赛赛卷

1.由专家组长提名，报大赛组委会办公室通过，组建命题专家组。

2.命题专家组负责本赛项的命题工作。

3.本赛项为非公开赛卷。

4.本赛项通过安徽省职业院校技能大赛指定的网络信息发布平台公布竞赛学生组样卷。

五、竞赛流程

（一）日程安排

比赛限定在1天半内进行,比赛场次为2场,赛项竞赛持续时间约为8小时，时间为竞赛第一日上午9：00-11:00，下午13:00-17:00，第二日上午08：10-11：50。具体安排如表3所示。

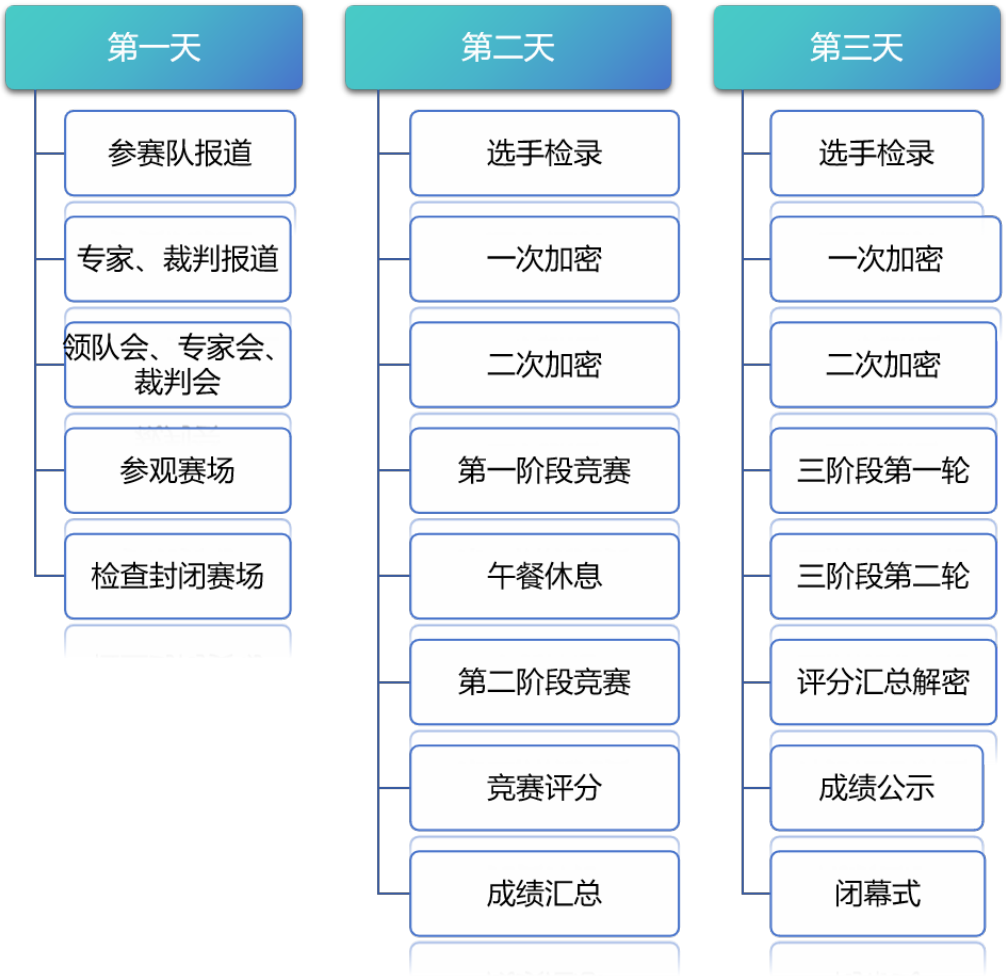
表 3 学生组竞赛日常安排表

日期	时间	事项	参加人员	地点
1 月 5 日	09:00-12:00	参赛队报到 安排住宿，领取资料	工作人员、参赛队	住宿酒店
	14:30-15:30	裁判工作会议、领队会	裁判长、领队 裁判员、监督组	会议室
	15:30-16:00	参观赛场	各参赛队领队	竞赛场地
1 月 6 日	08:00	裁判、选手进入比赛现场	选手、裁判长、现场裁判	竞赛场地
	08:10-08:20	选手检录	检录裁判	竞赛场地
	08:20-08:45	选手抽签 一次加密确定参赛号 二次加密确定工位号	参赛选手、加密裁判	竞赛场地
	08:45-08:50	裁判长宣读比赛纪律	参赛选手、现场裁判	竞赛场地
	08:50-09:00	选手检查比赛环境 现场裁判发放赛题	参赛选手、现场裁判	竞赛场地
	09:00-11:00	第一阶段正式比赛	参赛选手、现场裁判	竞赛场地
	11:00-11:30	一阶段成绩汇总报送	评分裁判、解密裁判、裁判长、专家、监督	竞赛场地
	11:30-12:30	午餐	裁判、志愿者	竞赛场地
	12:30-12:50	选手抽签 一次加密确定参赛号 二次加密确定工位号	参赛选手、加密裁判	竞赛场地
	12:50-13:00	现场裁判发放第二阶段赛题	参赛选手、现场裁判	竞赛场地
	13:00-17:00	第二阶段正式比赛	参赛选手、现场裁判	竞赛场地
	17:00-17:30	二阶段成绩汇总报送	评分裁判、裁判长、专家、监督仲裁	竞赛场地
		第二天比赛顺序抽签	参赛选手、加密裁判	竞赛场地
1 月 7 日	07:30-08:00	1-11 号选手检录、抽签确定参赛编号与工位	参赛选手、加密裁判	竞赛场地
	08:00-09:50	第三阶段（1-11 号）正式比赛	参赛选手、现场裁判	竞赛场地
	09:30-10:00	12-22 号选手检录、抽签确定参赛号与工位号	参赛选手、加密裁判	竞赛场地
	10:00-11:50	第三阶段(12-22 号)正式比赛	参赛选手、加密裁判	竞赛场地

备注：1 月 7 日赛程分两组进行，第二组进场检录后，第一组才能离场。

（二）学生组比赛流程

图 1 竞赛流程图



六、竞赛规则

（一）竞赛报名

1. 各高职院校按照大赛组委会规定的报名要求，通过“安徽省职业院校技能大赛网络报名系统”报名参赛。

2. 高职学生组参赛对象为全日制普通高等职业院校在校生（含职教本科）和五年制高职四至五年级在校生（1999 年 5 月 1 日以后出生）。已经在国赛和省赛中获得过一等奖的选手不得参加同项目、同组别比赛。每组可报 1-2 名指导教师。

3. 不得跨校组队，同一学校报名参赛队不超过 2 支。

4. 参赛选手和指导教师报名，获得确认后不得随意更换。比赛前参赛选手和

指导教师因故无法参赛，须由学校在本赛项开赛前 10 个工作日出具书面说明，并按参赛选手资格补充人员并接受审核，经省大赛组委会办公室同意后予以更换。

（二）熟悉场地规则

1.各参赛队统一有序的熟悉场地，熟悉场地时限定在指定区域，不允许进入比赛区。

2.熟悉场地时严禁与现场工作人员进行交流，不发表没有根据以及有损大赛整体形象的言论。

3.熟悉场地时严格遵守大赛各种制度，严禁拥挤，喧哗，以免发生意外事故。

（三）入场规则

1. 参赛选手按规定的时间准时到达赛场检录区集合。

2. 裁判将对各参赛选手的身份进行核对。参赛选手须提供参赛证、身份证、经学校注册的学生证，证件上的姓名、年龄、相貌特征应与参赛证一致。

3. 裁判检验参赛选手的工具、量具及书写物品，不允许携带任何通讯及存储设备、纸质材料等物品，检查合格后进入赛场抽签区。

4. 上午和下午分别的一次加密选手按检录顺序号依次抽取参赛编号，二次加密凭参赛编号抽取比赛工位号，然后在相应的比赛工位号区域外等待；在裁判长的指令下统一进入抽取的比赛工位号区域内就位。

（四）赛场规则

1.选手进入赛场后，必须听从现场裁判的统一布置和指挥。

2.分发比赛任务书后，选手可分析比赛任务，摆放工具、清点检查器材，但不可进行比赛任务的操作。

3.裁判长宣布比赛开始，参赛选手才能动手进行竞赛比赛任务的操作。

4.比赛过程中，参赛选手必须严格遵守安全操作规程，确保人身和设备安全，并接受现场裁判和技术人员的监督和警示。

5.比赛过程中若有任务书字迹不清问题，可示意现场裁判，由现场裁判解决。若认为比赛设备或元器件有问题需更换或耗材需要补充，应在赛场记录表的相应栏目填写更换设备或元器件、耗材名称、规格与型号、更换原因、更换时间等并签比赛工位号确认后，由现场裁判和技术人员予以更换。更换后经现场裁判和技

术人员检验并将结果记录在赛场记录表的相应栏目中并由选手签比赛工位号确认。

6.需要通电检查或调试设备时，应先报告现场裁判或技术人员，通电前的安全检测合格、获允许并派人监护后，才能通电检查或调试。

7.经现场裁判和技术人员检验，确因设备、元器件故障或损坏而更换设备或元器件者，从报告现场裁判到完成更换之间的用时，为比赛补时时间（控制在30分钟以内）。

8.比赛过程中选手不得随意离开工位，除本队参赛选手外，不得与其他参赛选手和人员交流。因故终止比赛或提前完成比赛任务需要离场，应报告现场裁判，在赛场记录表的相应栏目填写离场时间、离场原因并由现场裁判签名和选手签工位号确认。

9.第一阶段比赛结束，选手应停止操作并退到工位区域外。

10.第一阶段比赛结束，需要补时的选手在现场裁判宣布补时操作开始后，补时选手开始操作；现场裁判宣布补时时间到，选手应停止操作。

11.比赛过程中，严重违反赛场纪律影响他人比赛者，违反操作规程不听劝告者，越界影响他人者，有意损坏赛场设备或设施者，有意关闭/删除比赛服务器软件者，经现场裁判报告裁判长，经大赛组委会办公室同意后，由裁判长宣布取消其比赛资格。

（五）离场规则

1.比赛结束前15分钟，裁判长提示一次比赛剩余时间。

2.比赛结束信号给出，由裁判长宣布终止比赛。

3.裁判长宣布终止比赛时，选手应停止竞赛任务的操作。竞赛任务书、图纸、赛场记录表等整齐摆放在工作台上，不能带出赛场；工具、试题作答的文具等，保持现状，不需整理。

4.裁判长宣布终止比赛后，现场裁判组织、监督选手退出工位，站在工位边的过道上。

5.裁判长宣布终止比赛后，参赛队长按比赛工位号顺序向现场裁判提交比赛的答案，并由现场裁判和选手双方确认及将文件的数量和总的大小记录在提交答案记录表的相应栏目中，然后由选手签比赛工位号确认。

6.裁判长宣布离场时，现场裁判指挥选手统一离开赛场。

7.选手离场后，到指定的休息场所用餐、休息、等待评定比赛成绩。

（六）成绩评定与管理规则

1.成绩管理的机构及分工

成绩管理机构由裁判组、监督组和仲裁组组成。裁判在大赛裁判库中随机抽取，监督组和仲裁组由大赛组委会办公室指派。

（1）裁判组实行“裁判长负责制”，设裁判长 1 名，全面负责赛项的裁判分工、裁判评分审核、处理比赛中出现的争议问题等工作。

（2）裁判员根据比赛需要分为检录裁判、加密裁判、现场裁判和评分裁判。

检录裁判：负责对参赛队伍（选手）进行点名登记、身份核对等工作；（检录裁判可由承办校的工作人员来承担，但需要接受监督组的监督）

加密裁判：负责组织参赛队伍抽签，对参赛队信息、抽签代码等进行加密；

现场裁判：按规定做好赛场记录，维护赛场纪律，进行现场执裁的工作；

评分裁判：负责按评分细则评定成绩。

（3）监督组对裁判组的工作进行全程监督，并对竞赛成绩抽检复核。

（4）仲裁组负责接受由参赛队领队提出的对裁判结果的申诉，组织复议并及时反馈复议结果。

2.成绩管理流程

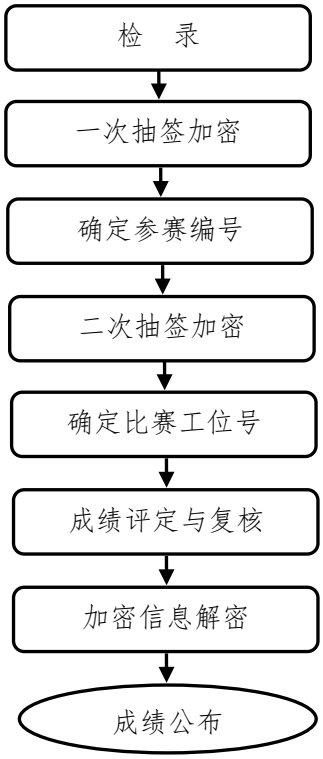


图 2 成绩管理流程图

3.比赛成绩评定

（1）结果评分

由评分裁判依据评分表，对参赛队所提交的答案（结果性评分）和系统自动统计的数据（机考评分）进行评分。

（2）违规扣分

选手有下列情形，需从比赛成绩中扣分：

在完成比赛任务的过程中，因操作不当损坏比赛设备，不影响他人比赛，从比赛成绩中扣 10 分；影响他人比赛，从比赛成绩中扣 20 分。

4.解密

裁判长正式提交工位号评分结果并复核无误后，加密裁判在监督人员监督下对加密结果进行逐层解密，形成成绩表，并由裁判长、监督员签字确认。

5.成绩公布

将解密后的各参赛队得分结果汇总，经裁判长、监督员和专家组长及巡视员签字后，在成绩发布会上公布。

七、竞赛环境

竞赛工位内设有操作平台，每工位配备 220V 电源，工位内的电缆线应符合安全要求。每个竞赛工位面积≥5 ㎡，有≥1.4m 高度的分隔装置，确保参赛队之间互不干扰。竞赛工位标明工位号，并配备竞赛平台和技术工作要求的软、硬件。环境标准要求保证赛场采光(大于 500lux)、照明和通风良好；每支参赛队提供一个垃圾箱。

八、技术规范

本赛项涉及主要有以下 11 项国家标准，参赛队在实施竞赛项目中要求遵循如下规范。

表 4 技术规范一览表

序号	标准号	中文标准名称
1	GB/T 37231-2018	《印章印文鉴定技术规范》

2	GB/T 37234-2018	《文件鉴定通用规范》
3	GB/T 37239-2018	《笔迹鉴定技术规范》
4	GB/T 37238-2018	《篡改（污损）文件鉴定技术规范》
5	SF/Z D0202001-2015	《文件上可见指印鉴定技术规范》
6	GB/T 29360-2012	《电子物证数据恢复检验规程》
7	SF/T 0014-2017	《全国监狱信息化应用技术规范》
8	GB/T 36643-2018	《信息安全技术—网络安全威胁信息格式规范》
9	GB/T 22239-2019	《信息安全技术—网络安全等级保护基本要求》
10	GB/T 20272-2006	《信息安全技术操作系统安全技术要求》
11	GB/T 20271-2006	《信息安全技术信息系统通用安全技术要 求》

九、技术平台

（一）竞赛设备一览表

表 5 竞赛设备一览表

序号	设备名称	数量	参考型号
1	明镜数字司法技术竞赛平台	1	米好信安 MJDJ-TCS
2	PC 机	3	2 台：多核 CPU，主频 ≧ 3.4GHZ，≧四核心八线程，内存 ≧ 16GB，具有串口或者配置 USB 转串口的配置线，支持硬件虚拟化; 1 台：多核 CPU，主频 ≧ 3.4GHZ，≧四核心八线程，内存 ≧ 8GB，具有串口或者配置 USB 转串口的配置线，支持硬件虚拟化;

（二）竞赛软件

提供个人计算机（安装 Windows 操作系统），用以组建竞赛操作环境，并安装 Office 等常用应用软件。

表 6 竞赛应用软件一览表

序号	软件	介绍
1	Windows 10	操作系统
2	Microsoft Office 2016/2019	文档编辑工具
3	VMware 15 或以上版本	虚拟机运行环境

4	Visio	2010 及以上版
5	Winhex	V16.0
6	Photoshop	CS6
7	Parrot Security Edition	5.2
8	超级终端 SecureCRT/putty	设备调试连接工具

提供渗透测试机和靶机虚拟机环境。

表 7 渗透测试机与靶机一览表

序号	软件	介绍
1	Windows 7 \Windows 10	Windows 客户机操作系统
2	Windows Server 2003\2008\2010\2012\2016\2018	Windows 服务器操作系统
3	Ubuntu\Debian\Kali	渗透测试机操作系统
4	Linux CentOS	Linux 服务器操作系统

十、成绩评定

（一）评分文件

1.学生组评分标准

竞赛评分严格按照公平、公正、公开的原则，评分标准注重考查参赛选手以下各方面的能力和水平。

表 8 学生组竞赛评分标准表

竞赛阶段	竞赛任务	考核内容	分值	评分方式
第一阶段	司法技术技能素养	单选、多选、判断	30%	自动评分
	物证检验与数字取证技能	物证鉴定技术	20%	结果评分-客观人工评分
		网络取证技术	20%	
第二阶段	监所安防和信息系统运维技能	监所信息管理系统安全攻防	20%	依据评价标准验证结果正确性自动评分
		监所数字安防技术运用	10%	结果评分-客观人工评分

2.评分表

评分表根据赛项评分标准，由命题专家在拟定比赛任务书时拟定，裁判根据评分表对选手的比赛成绩进行评定（评分表见样题）。

（二）评分方法

评分裁判评分过程中，对第一阶段比赛答案进行背对背评分，成绩一致方可进行统计，产生答案提交文档号的各项成绩；并导出系统自动统计的第二阶段和第三阶段机考评分成绩。

（三）成绩审核与产生

1.评分裁判小组应统计各个比赛工位每个评分项目中的得分，对项目成绩进行复查审核。并连同系统自动统计的机考评分成绩一并提交裁判长。

2.裁判长统计各个比赛工位上午比赛的各个评分项目得分，产生每个工位的上午比赛的得分。

3.裁判长分别对上午和下午比赛成绩经复核无误，由加密裁判在监督员的监督下解密。

4.裁判长按参赛队合并上午和下午的比赛得分，得出各参赛队的总得分（竞赛成绩）。

5.为保障成绩评判的准确性，监督组将对赛项成绩抽检复核，如发现成绩错误以书面方式及时告知裁判长，由裁判长更正成绩并签字确认。

6.最终成绩经复核无误，由裁判长、监督人员签字确认，并公示。

十一、奖项设定

（一）参赛选手奖

学生组根据竞赛成绩，从高到低排序，按实际参赛队数量的10%设一等奖，20%设二等奖，30%设三等奖。

（二）指导教师奖

对获得一、二、三等奖参赛队的指导教师颁发指导教师奖。

十二、赛场预案

承办院校负责编制车辆安全措施应急预案、食品安全措施应急预案、火灾安全事故紧急处理预案、伤害事故紧急处理预案、设备事故紧急处理预案，电力供应事故紧急处理预案等。对处理各种可能出现的突发状况进行事先演练，确保赛项顺利进行。

各参赛院校赛前要对选手进行计算机、网络设备、工具等操作的安全培训，进行安全操作的宣讲，确保每个队员能够安全操作设备后方可参加比赛。裁判长

在比赛前，宣读安全注意事项，强调用电安全规则。

（一）消防预案

承办院校负责赛场、师生入住酒店的消防环境等检查，做好赛场和酒店的应急疏散预案，确保竞赛期间师生安全。

封闭赛场前，由赛点领导小组成员带队（含安保组成员）进行一次全面的现场消防检查，包括消防栓方位、配备灭火器的检查，在使用上是否进入良好状态，不许出现消防隐患，确保消防安全。

竞赛期间，任何人发现火情，选手等在现场工作人员的引导下进行有序疏散，并迅速使用现场的消防器材控制火情，争取消灭于火灾初级阶段。

如不能及时控制、扑灭火灾，在场工作技术人员要立即采取切断电源等措施妥善处理，防止火势蔓延。

在场工作人员要以最快的方式向赛点领导小组成员、安保组成员汇报，尽快增加援助人员，协力救火。

赛点领导小组成员接到报告后，要立即达到火情现场，并视火情拨打“119”报警求救。

为更好地应对紧急情况，所有人员必须一切听从现场指挥员的指挥。

（二）供电预案

安装在线 UPS：采用 UPS 防止现场因突然断电导致的系统数据丢失，额定功率 3KVA，后备时间 2 小时，输出电压 230V±5%V；市电采用双路供电。

（三）医疗预案

承办院校须安排专职医护人员做好比赛期间的医疗保障工作，做好救护地点、医疗器械、药物，休息床等的准备工作。

在比赛场地的适当位置设置急救医疗点，救护用器械及设施、药品和医护人员，并有醒目标志，确保通讯畅通（通过裁判长）。

当赛场内有人员发生病情时，场内医护人员要及时采取救治措施进行现场救护；如需送医院救治的，应立即就近送医院继续治疗，并通知领队和指导教师。

疫情防控常态化形势下，按照承办院校的各类突发情况预案和应对工作，做好比赛期间的各类突发情况预案和应对工作。

（四）设备预案

预留至少 10%的备用 PC 和各种设备，当出现设备掉电、故障等意外时经现场裁判确认后由赛场技术支持人员予以更换。

竞赛过程中出现设备掉电、故障等意外时，现场裁判需及时确认情况，安排技术支持人员进行处理，现场裁判登记详细情况，填写补时登记表，报裁判长批准后，可安排延长补足相应选手的比赛时间。

（五）赛题预案

采取比赛试题 AB 卷，内容、题量及其难度和得分权重基本相当。

比赛前日，在领队会上，监督员的监督下，裁判长随机抽取采用试卷；在监督员的监督下，命题专家组打印装订比赛试题，并由监督员保密存放。

未被抽取到的比赛试题卷则为备用试题卷。

（六）疫情防控

为切实推进与落实疫情防控常态化条件下省高职赛项组织工作，确保参赛师生生命安全与身体健康，比赛期间疫情防控要求如下：

1.承办院校

各赛项承办院校为疫情防控主体责任单位，科学落实属地疫情防控要求，成立相关组织机构，统一负责疫情防控组织工作。赛事组织过程中，要加强与当地疫情防控指导机构的沟通联系，制定好各赛项疫情防控实施方案，将防控要求落实到办赛全过程，并在大赛指南中明确。安排专人与各参赛院校对接，主动告知赛务安排、人员报到等具体要求。对参赛人员做好体温检测，健康码核查、提供必要防疫物资等相关疫情防控工作，确保竞赛顺利实施。

2.参赛院校

各参赛院校加强参赛人员统一管理，精简随行人员，除领队、选手和指导教师外，减少其他工作人员数量。安排专车点对点接送参赛人员，确保参赛选手安全抵离。

指定专人落实参赛人员的疫情防控准备工作，提前准备好参赛人员（含领队及指导教师等）相关防疫资料，报到现场须提交《参赛人员健康状况排查承诺书》和《个人健康状况承诺书》，提供健康通行码“绿码”和手机漫游地查询结果(通信大数据行程卡)，在测温正常下完成报到，入住承办院校指定酒店。比赛期间

应注意做好个人防护，备足一次性医用口罩，避免在人员密集、通风不良的场所逗留。参赛人员须服从承办学校疫情防控检查，如果出现发热、乏力、干咳、呼吸困难等症状，请立即与承办院校疫情防控工作小组取得联系，视病情及时就医，确保竞赛安全举办。

十三、赛项安全

赛项安全是技能竞赛一切工作顺利开展的先决条件，是赛项筹备和运行工作必须考虑的核心问题。采取切实有效措施保证大赛期间参赛选手、指导教师、裁判员、工作人员及观众的人身安全。

（一）比赛环境

在赛前组织专人对比赛现场、住宿场所和交通保障进行考察，并对安全工作提出明确要求。赛场的布置，赛场内的器材、设备，应符合国家有关安全规定。如有必要，也可进行赛场仿真模拟测试，以发现可能出现的问题。承办单位赛前须按照赛项规程要求排除安全隐患。

赛场周围要设立警戒线，防止无关人员进入发生意外事件。比赛现场内应参照相关职业岗位的要求为选手提供必要的劳动保护。在具有危险性的操作环节，裁判员要严防选手出现错误操作。

承办单位应提供保证应急预案实施的条件。对于比赛内容涉及高空作业、可能有坠物、大用电量、易发生火灾等情况的赛项，必须明确制度和预案，并配备急救人员与设施。

承办单位制定开放赛场和体验区的人员疏导方案。赛场环境中存在人员密集、车流人流交错的区域，除了设置齐全的指示标志外，须增加引导人员，并开辟备用通道。

大赛期间，承办单位应在赛场管理的关键岗位增加力量并建立安全管理日志。

参赛选手进入工位、赛事裁判工作人员进入工作场所，严禁携带通讯、照相摄录设备，禁止携带记录用具。如确有需要，由赛场统一配置、统一管理。赛项可根据需要配置安检设备对进入赛场重要部位的人员进行安检。

（二）生活条件

比赛期间，统一安排参赛选手和指导教师食宿。承办单位须尊重少数民族的信仰及文化，根据国家相关的民族政策，安排好少数民族选手和教师的饮食起居。

比赛期间安排的住宿地应具有宾馆/住宿经营许可资质。以学校宿舍作为住宿地的，大赛期间的住宿、卫生、饮食安全等由提供宿舍的学校负责。

大赛期间承办单位须保障比赛期间选手、指导教师和裁判员、工作人员的交通安全。

各赛项的安全管理，除了可以采取必要的安全隔离措施外，应严格遵守国家相关法律法规，保护个人隐私和人身自由。

（三）参赛队责任

1.各学校组织参赛队时，须安排除参赛选手、指导教师、领队以外的随行人员购买大赛期间的人身意外伤害保险。

2.各学校参赛队组成后，须制定相关管理制度，并对所有选手、指导教师进行安全教育。

3.各参赛队伍须加强对参与比赛人员的安全管理，实现与赛场安全管理的对接。

（四）应急处理

比赛期间发生意外事故，发现者应第一时间报告赛项专家组长，同时采取措施避免事态扩大，立即启动预案予以解决并报告组委会。赛项出现重大安全问题可以停赛，应向组委会报告详细情况。

（五）处罚措施

1.因参赛队伍原因造成重大安全事故的，取消其获奖资格。

2.参赛队伍有发生重大安全事故隐患，经赛场工作人员提示、警告无效的，可取消其继续比赛的资格。

3.赛场工作人员违规，按照相应的制度追究责任。情节恶劣并造成重大安全事故的，由司法机关追究相应法律责任。

十四、竞赛须知

（一）参赛队须知

1.参赛队名称统一使用规定的代表队名称。

2.参赛队员在报名获得审核确认后，原则上不再更换，如筹备过程中，选手因故不能参赛，所在学校需出具书面说明并按相关规定补充人员并接受审核；竞赛开始后，参赛队不得更换参赛队员，允许缺员比赛。

3.参赛队按照大赛赛程安排凭大赛组委会颁发的参赛证和有效身份证件参加比赛及相关活动。

4.各参赛队统一安排参加比赛前熟悉场地环境的活动。

5.各参赛队准时参加赛前领队会，领队会上举行抽签仪式抽取场次号。

6.各参赛队要注意饮食卫生，防止食物中毒。

7.各参赛队要发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。

（二）指导老师须知

1.各指导老师要发扬良好道德风尚，听从指挥，服从裁判，不弄虚作假。指导老师经报名、审核后确定，一经确定不得更换。

2.对申诉的仲裁结果，领队和指导老师应带头服从和执行，还应说服选手服从和执行。

3.指导老师应认真研究和掌握本赛项比赛的技术规则和赛场要求，指导选手做好赛前的一切准备工作。

4.领队和指导老师应在赛后做好技术总结和工作总结。

（三）参赛选手须知

1.参赛选手应遵守比赛规则，尊重裁判和赛场工作人员，自觉遵守赛场秩序，服从裁判的管理。

2.参赛选手应佩戴参赛证，带齐身份证、注册的学生证。在赛场的着装，应符合职业要求。在赛场的表现，应体现自己良好的职业习惯和职业素养。

3.进入赛场前须将手机等通讯工具交赛场相关人员保管，不能带入赛场。未经检验的工具、电子储存器件和其他不允许带入赛场物品，一律不能进入赛场。

4.比赛过程中不准互相交谈，不得大声喧哗；不得有影响其他选手比赛的行为，不准有旁窥、夹带等作弊行为。

5.参赛选手在比赛的过程中，应遵守安全操作规程，文明的操作。通电调试设备时，应经现场裁判许可，在技术人员监护下进行。

6.比赛过程中需要去洗手间，应报告现场裁判，由裁判或赛场工作人员陪同离开赛场。

7.完成比赛任务后，需要在比赛结束前离开赛场，应向现场裁判示意，在赛场记录上填写离场时间并签工位号确认后，方可离开赛场到指定区域，离开赛场

后不可再次进入。未完成比赛任务，因病或其他原因需要终止比赛离开赛场，需经裁判长同意，在赛场记录表的相应栏目填写离场原因、离场时间并签工位号确认后，方可离开；离开后，不能再次进入赛场。

8.裁判长发出停止比赛的指令，选手（包括需要补时的选手）应立即停止操作进入通道，在现场裁判的指挥下离开赛场到达指定的区域等候评分。需要补时的选手在离场后，由现场裁判召唤进场补时。

9.赛场工作人员叫到工位号、在等待评分的选手，应迅速进入赛场，与评分裁判一道完成比赛成绩评定。在评分过程中，选手应配合评分裁判，按要求进行设备的操作；可与裁判沟通，解释设备运行中的问题；不可与裁判争辩、争分，影响评分。

10.遇突发事件，立即报告裁判和赛场工作人员，按赛场裁判和工作人员的指令行动。

（四）工作人员须知

1.工作人员必须服从赛项组委会统一指挥，佩戴工作人员标识，认真履行职责，做好服务赛场、服务选手的工作。

2.工作人员按照分工准时上岗，不得擅自离岗，应认真履行各自的工作职责，保证竞赛工作的顺利进行。

3.工作人员应在规定的区域内工作，未经许可，不得擅自进入竞赛场地。如需进场，需经过裁判长同意，核准证件，有裁判跟随入场。

4.如遇突发事件，须及时向裁判长报告，同时做好疏导工作，避免重大事故发生，确保竞赛圆满成功。

5.竞赛期间，工作人员不得干涉及个人工作职责之外的事宜，不得利用工作之便，弄虚作假、徇私舞弊。如有上述现象或因工作不负责任的情况，造成竞赛程序无法继续进行，由赛项组委会视情节轻重，给予通报批评或停止工作，并通知其所在单位做出相应处理。

（五）裁判员须知

1.裁判员执裁前应参加培训，了解比赛任务及其要求、考核的知识与技能，认真学习评分标准，理解评分表各评价内容和标准。不参加培训的裁判员，取消执裁资格。

2.裁判员执裁期间，统一佩戴裁判员标识，举止文明礼貌，接受参赛人员的监督。

3.遵守执裁纪律，履行裁判职责，执行竞赛规则，信守裁判承诺书的各项承诺。服从赛项专家组和裁判长的领导。按照分工开展工作，始终坚守工作岗位，不得擅自离岗。

4.裁判员有维护赛场秩序、执行赛场纪律的责任，也有保证参赛选手安全的责任。时刻注意参赛选手操作安全的问题，制止违反安全操作的行为，防止安全事故的出现。

5.裁判员不得有任何影响参赛选手比赛的行为，不得向参赛选手暗示或解答与竞赛有关的问题，不得指导、帮助选手完成比赛任务。

6.公平公正的对待每一位参赛选手，不能有亲近与疏远、热情与冷淡差别。

7.赛场中选手出现的所有问题如：违反赛场纪律、违反安全操作规程、提前离开赛场等，都应在赛场记录表上记录，并要求学生签工位号确认。

8.严格执行竞赛项目评分标准，做到公平、公正、真实、准确，杜绝随意打分；对评分表的理解和宽严尺度把握有分歧时，请示裁判长解决。严禁利用工作之便，弄虚作假、徇私舞弊。

9.竞赛期间，因裁判人员工作不负责任，造成竞赛程序无法继续进行或评判结果不真实的情况，由赛项组委会视情节轻重，给予通报批评或停止裁判资格，并通知其所在单位做出相应处理。

十五、申诉与仲裁

（一）各参赛队对不符合赛项规程规定的设备、工具、材料、计算机软硬件、竞赛执裁、赛场管理及工作人员的不规范行为等，可向赛项仲裁组提出申诉。

（二）申诉主体为参赛队领队。

（三）申诉启动时，参赛队以该队领队签字同意的书面报告的形式递交赛项仲裁组。报告应对申诉事件的现象、发生时间、涉及人员、申诉依据等进行充分、实事求是的叙述。非书面申诉不予受理。

（四）提出申诉应在赛项比赛结束后 2 小时内提出。超过 2 小时不予受理。

（五）赛项仲裁组在接到申诉报告后的 2 小时内组织复议，并及时将复议结果以书面形式告知申诉方。申诉方对复议结果仍有异议，可由领队向大赛仲裁工

作组提出申诉。大赛仲裁工作组的仲裁结果为最终结果。

（六）申诉方不得以任何理由拒绝接收仲裁结果；不得以任何理由采取过激行为扰乱赛场秩序。仲裁结果由申诉人签收，不能代收；如在约定时间和地点申诉人离开，视为自行放弃申诉。

（七）申诉方可随时提出放弃申诉。

十六、竞赛观摩

本赛项将会设观摩区，使用大屏幕实时显示信息安全攻防对战的进度状况。

十七、竞赛直播

在大赛组委会统一安排下进行。

参赛队进行比赛时，如有关记者需要摄像，应该以不妨碍选手比赛为原则，即不进入比赛核心区，采取中远距离、短时间摄像，不得进行有声采访。

十八、其他

1.参赛选手及相关工作人员，由赛项承办院校统一安排食宿，费用自理。

2.本技术文件的最终解释权归大赛组织委员会。

（赛题部分内容因涉及隐私和安全暂不公开，待比赛时予以公开。）

2023 年安徽省职业院校技能大赛
高职组“司法技术”赛项样题

模块一：司法技术技能素养模块

一、 单选题（总共 100 小题，每题 1 分，计 100 分）

1. 观察 DFO 显现的手印所使用的光源区域是（ ）。

A. 蓝绿光　　B. 紫外线

C. 红外线　　D. 红光

2. 白灰墙上的汗潜指纹最合适的显现方法为（ ）。

A. 粉末显现法　　B. 化学显现法

C. 静电吸附法　　D. 碘熏法

3. 在中国人中，约有（ ）的指头花纹具有三个系统，约有（ ）的指头花纹只具有两个系统。

A. 95%　5%　　B. 90%　10%

C. 98%　2%　　D. 97. 5%　2. 5%

4. 以下粉末中，属于荧光粉末的是（ ）。

A. 铝粉　　B. 磁性粉

C. 8-羟基喹啉　　D. 氧化铁

5. 以下显现方法中，可用于显现血潜手印的是（ ）。

A. 四甲基联苯胺显现法　　B. 硝酸银显现法

C. 物理显影液显现法　　D. 502 显现法

6. 三角的形态结构较为复杂，可从不同的角度进行分类：按三角的内部结构的不同可将三角分为：空心三角、 （ ）、 夹线三角。

A. 隔线三角　　B. 点眼三角

C. 棒线三角　　D. 点棒三角

7. 花纹中心由两条以上起点方向相对的螺型线相对绞绕旋转组成的斗型花纹为（　）。

A. 螺型斗　　B. 曲型斗

C. 绞型斗　　D. 双曲斗

8. 全自动枪支是指扣住（　）可连续发射的枪支。

A. 击锤　B. 板机　C. 枪机　D. 击针

9. 12 号猎枪的口径是指用一磅铅制成（　）个同样大小的园形弹丸。

A. 18　B. 10　C. 12　D. 14

10. 抛壳挺的部位是在枪支的（　）部位上。

A. 枪机　B. 机匣　C. 握把　D. 弹匣

11. 硝化甘油火药是用硝化甘油. 硝化二乙二醇溶解于（　）并胶化而成的火药。

A. 酒精　B. 醇醚溶剂　C. 硝化棉　D. 甲醇

12. 由于击针簧的弹力作用，使击针撞击子弹（　），形成了弹壳底火上的击针痕迹。

A. 弹底窝　B. 火帽　C. 底火　D. 底缘

13. 打击痕迹是行为人用所持工具快速运动形成的（　）在被破坏的客体上所形成的痕迹。

A. 运动速度　B. 冲击作用　C. 凹陷痕迹　D. 线形痕迹

14. 在工具痕迹分析中，需要确定犯罪过程中留下的痕迹与（　）其他人所留下的痕迹。

A. 作案工具　B. 发案前和发案后　C. 自然痕迹　D. 动物啃咬

15. 对可能留下现场痕迹的工具，进行观察检验的叫（　）。

A. 作案工具　B. 检验嫌疑工具　C. 工具样本　D. 种类认定

16. 鞋在穿着过程中形成的损伤特征（如塑料底鞋烫伤特征）应是（　）。

A. 种类特征　B. 个别特征　C. 细小特征　D. 特定特征

17. 人的足骨（单足）共有（　）。

A. 28 块　B. 26 块　C. 24 块　D. 30 块

18. 一个正常人的每只足的趾骨为（　）。

A. 16 块　B. 14 块　C. 12 块　D. 10 块

19. 对于留在纸张. 床单等上的反差微弱的尘土足迹，可以采用（　）配制的溶液显现加强。

A. 硫氰酸钾　B. 硝酸银　C. 茚三酮　D. 碘

20. 在现场发现一种足迹，足迹不均匀，边沿不完整，前掌和后跟重压面窄而不圆滑，足弓较高，该种足迹应是（　）所留。

A. 胖人　B. 中等身材　C. 瘦人　D. 特胖的人

21. 不适合用“转移法”保护物证的现场是（　）。

A. 火案现场

B. 流水中的现场

C. 铁路线、公路干线上的现场

D. 室内现场

22. 调查取证的根本任务是查明案情和揭露、证实犯罪（　）。

A. 查缉又犯罪嫌疑人 B. 汇报案情　C. 分析案情　D. 汇报领导

23. 以下不属于现场绘图类型的是（　）。

A. 现场方位图 B. 现场全貌图 C. 现场局部图 D. 现场重点图

24. 在下列刑事现场摄影的步骤中，描述错误的是：（　）。

A. 先拍原始的，后拍移动的

B. 先拍易破坏消失的，后拍不易破坏消失的

C. 先拍上部，后拍地面

D. 先拍易，后拍难

25. 现场勘查的实施主体是（ ）。

A. 监狱民警 B. 侦查人员 C. 公安民警 D. 检察机关

26. 专案侦办期间实行（ ），必要时可将重大犯罪嫌疑人押往异地关押及审讯。

A. 直接领导 B. 条块领导 C. 垂直领导 D. 分管领导

27. 以下刑事摄影设备，属于常用工具的是：（ ）。

A. 近拍装置 B. 比例尺 C. 滤色镜 D. 摄像机

28. 犯罪现场构成要素中的核心要素是（ ）。

A. 时间要素 B. 犯罪行为要素

C. 空间要素 D. 现场物质形态变化要素

29. 关于现场复验下列说法错误的是（ ）。

A. 现场复验因由负责勘验工作的侦查人员负责

B. 现场复验人员要有特定的业务技能要求

C. 现场复验结果作为最终办案依据使用

D. 现场复验必须做好记录

30. 下列选项中,不属于爆炸案件犯罪嫌疑人应该具备的作案条件是( )。

A. 有机会接触炸药 B. 有在矿山工作的经历

C. 熟悉电路知识 D. 会制造和使用枪支

31. 分析犯罪嫌疑人的社会身份与职业，主要从（ ）方面进行分析。

A. 现场有无伪装 B. 逃离方式

C. 现场遗留物 D. 有无犯罪前科

32. 下列属于抛尸现场痕迹物证的是（ ）。

A. 有被害人的鞋印 B. 有交通工具痕迹

C. 有搏斗痕迹 D. 有大量喷溅血迹

33. 对特别重大、复杂案件现场进行保护时，需要设立新闻中心，以接待众

多的媒体记者。新闻中心应该设在（　）。

A. 区域性保护区　　B. 一般性保护区

C. 核心保护区　　D. 外围性性保护区

34. 关于楼房内室内现场的保护措施错误的是（　）。

A. 在案发的分户门或窗外设岗看守

B. 可暂时封闭整个单元

C. 通往案发房间的楼梯可以不封闭

D. 在一楼单元门口设岗看守

35. 关于对犯罪嫌疑人的人身检查，错误的是（　）。

A. 犯罪嫌疑人若拒绝检查，不可以强制检查

B. 检查犯罪嫌疑人，必先搜身，注意安全

C. 人身检查应当有见证人在场

D. 检查女性的身体，应当由女侦查人员进行，或者在女侦查人员主持下由医师进行检查

36. 某些室外现场。如拦路抢劫、强奸（预先踩点、窥视）等案件的受害人能明确指出案发地点的，或杀人案件所在部位十分明显的现场，应采取哪种顺序进行勘验（　）。

A. 从中心向外围勘验　　B. 从外围向中心勘验

C. 从现场进出口处勘验　　D. 沿着犯罪嫌疑人活动的路线进行勘验

37. 产品质量鉴定属于（　）。

A. 认定种属的鉴定　　B. 确定事实有无的鉴定

C. 认定事实真伪的鉴定　　D. 确定事实因果关系的鉴定

38. 完善以宪法为核心的中国特色社会主义法律体系，要求推进科学立法和民主立法。下列哪一做法没有体现这一要求？（　）。

A. 在《大气污染防治法》修改中，立法部门就处罚幅度听取政府部门和专家学者的意见

B. 在《种子法》修改中，全国人大农委调研组赴基层调研，征求果农、种子企业的意见

C. 甲市人大常委会在某社区建立了立法联系点，推进立法精细化

D. 乙市人大常委会在环境保护地方性法规制定中发挥主导作用，表决通过后直接由其公布施行

39. 以下有关时间的说法错误的是（ ）。

A. 具有与所申请从事的司法鉴定业务相关的专业执业资格或者高等院校相关专业本科以上学历，从事相关工作三年以上的，可申请从事司法鉴定业务

B. 具有与所申请从事的司法鉴定业务相关工作十年以上经历，具有较强的专业技能的，可申请从事司法鉴定业务

C. 省级人民政府司法行政部门可以对鉴定人或鉴定机构给予停止从事司法鉴定业务三个月以上一年以下的处罚

D. 《全国人民代表大会常务委员会关于司法鉴定管理问题的决定》自 2005 年 10 月 1 日起施行。

40. 下列各项中，属于司法会计鉴定对象的是（ ）。

A. 原始凭证内容真实性的辨认问题

B. 记帐凭证中有关会计分录的制作与否真实、对的和合理的辨认问题

C. 原始凭证中签名的真伪问题

D. 原始凭证中与否波及法律惩罚的问题

41. 在一盗窃案件现场发现的下列物证中，属于化学物证的是（ ）。

A. 汗液手印　　B. 玻璃渣　　C. 足迹　　D. 撬痕

42. “注意的局限性”是属于笔迹基本属性中（ ）。

A. 反映性 B. 自身同一性 C. 总体特殊性 D. 系列性

43. “羣”字属于（ ）。

A. 错别字特征　　B. 写法特征

C. 运笔特征　　D. 笔顺特征

44. 下列不属于喷墨式打印机打印特点的是（ ）。

A. 墨迹由小圆点组成　　B. 无冲击

C. 墨迹有洇散　　D. 有挤墨现象

45. 在复印文件中测量到重复性斑痕之间的距离为 282.6mm,可计算得出该复印机的感光鼓直径为（ ）。

A. 30　　B. 60　　C. 80　　D. 90

46. 平板印刷的主要特点是（ ）。

A. 文字线条有露白现象

B. 文字线条有毛刺

C. 文字线条有冲击压痕

D. 文字线条有挤墨现象

47. 一般情况下司法鉴定机构应当自司法鉴定委托书（ ）之日起 30 个工作日内完成鉴定。

A. 递交　　B. 受理　　C. 批准　　D. 生效

48. 下列不属于办公设备机制文件的是（ ）。

A. 打印文件

B. 传真文件

C. 静电复印文件

D. 凸版印刷文件

49. 下列不能使用 502 熏显法显现的是（ ）。

A. 灯泡上的汗液手印

B. 塑料瓶上的汗液手印

C. 窗户上的灰尘手印

D. 衣服上的油脂手印

50. 根据指纹内部花纹和三角的基本形态，指纹可分为（ ）。

A. 弓型纹、箕型纹、斗型纹、帐型纹

B. 弓型纹、箕型纹、斗型纹、弧型纹

C. 弓型纹、箕型纹、斗型纹、混杂型纹

D. 弓型纹、箕型纹、混杂型纹、帐型纹

51. EPON 常用接入模式包括 ONU 子卡模式和以下哪种模式（ ）。

A. WLAN B. 3G 接入 C. SFP 光口 D. 外置 ONU

52. 下面对国家秘密定级和范围的描述中，哪项不符合《保守国家秘密法》要求（ ）。

A. 国家秘密及其密级的具体范围，由国家保密工作部门分别会同外交、公安、国家安全和其他中央有关机关规定

B. 各级国家机关、单位对所产生的国家秘密事项，应当按照国家秘密及其密级具体范围的规定确定密级

C. 对是否属于国家机密和属于何种密级不明确的事项，可由各单位自行参考国家要求确定和定级，然后报国家保密工作部门确定

D. 对是否属于国家秘密和属于何种密级不明确的事项。由国家保密工作部门，省、自治区、直辖市的保密工作部门。省、自治区政府所在地的市和经国务院批准的较大的市的保密工作部门或者国家保密工作部门审定的机关确定

53. 在可信计算机系统评估准则（TCSEC）中，下列哪一项是满足强制保护要求的最低级别（ ）。

A. C2 B. C1 C. B2 D. B1

54. 以下不属于安全防范手段的是（ ）。

A. 人防 B. 事防 C. 物防 D. 技防

55. 以下行为不属于违反国家保密规定的行为（ ）。

A. 将涉密计算机、涉密存储设备接入互联网及其他公共信息网络

B. 通过普通邮政等无保密措施的渠道传递国家秘密载体

C. 在私人交往中涉及国家秘密

D. 以不正当手段获取商业秘密

56. 以下哪一项不是信息系统集成项目的特点（ ）。

A. 信息系统集成项目要以满足客户和用户的需求为根本出发点

B. 系统集成就是选择最好的产品和技术，开发相应的软件和硬件，将其集成到信息系统的过程

C. 信息系统集成项目的指导方法是“总体规划、分步实施”

D. 信息系统集成包含技术，管理和商务等方面，是一项综合性的系统工程

57. 为防范网络欺诈确保交易安全，网银系统首先要求用户安全登录，然后使用“智能卡+短信认证”模式进行网上转账等交易。在此场景中用到下列哪些鉴别方法（ ）。

A. 实体“所知”以及实体“所有”的鉴别方法

B. 实体“所有”以及实体“特征”的鉴别方法

C. 实体“所知”以及实体“特征”的鉴别方法

D. 实体“所有”以及实体“行为”的鉴别方法

58. 实体身份鉴别一般依据以下三种基本情况或这三种情况的组合：实体所知的鉴别方法、实体所有的鉴别方法和基于实体特征的鉴别方法。下面选项中属于实体特征的鉴别方法是（ ）。

A. 将登录口令设置为出生日期

B. 通过询问和核对用户的个人隐私信息来鉴别

C. 使用系统定制的、在本系统专用的 IC 卡进行鉴别

D. 通过扫墙和识别用户的脸部信息来鉴别

59. 《智能建筑工程质量验收规范》明确提出验收应按（ ）顺序进行。

A. 先产品，后系统，先子系统，后系统集成

B. 先产品，后系统，先系统集成，后子系统

C. 先系统，后产品，先子系统，后系统集成

D. 先系统，后产品，先系统集成，后子系统

60. 以下关于信息安全工程说法正确的是（ ）。

A. 信息化建设中系统功能的实现是最重要的

B. 信息化建设可以先实施系统，而后对系统进行安全加固

C. 信息化建设中在规划阶段合理规划信息安全，在建设阶段要同步实施信息安全建设

D. 信息化建设没有必要涉及信息安全建设

61. 我们常说的摄像机镜头分成 C/CS 型号,其中 C 型号镜头距 CC|D 靶面距离为多少（ ）。

A.12.5 毫米　　B.15.5 毫米

C.17.5 毫米　　D.14.5 毫米

62. 按照 GB50311 国家标准规定,水平双绞线电缆最长不宜超过多少米（ ）。

A.50 米　　B.150 米　　C.90 米　　D.100 米

63. 出入口管理涵盖着门禁、停车（库）场、楼宇（可视）对讲等业务领域，是（ ）系统的重要组成部分。

A. 技防

B. 人防

C. 安全管理

D. 安全防范

64. （ ）通过辨识目标物品的管理、化学等特性，形成特征信息，如金属物质识别、磁性物质识别、爆炸物质识别、放射性物质识别、特殊化学物质识别等。

A. 物品特征识别

B. 物品编码识别

C. 眼底纹识别

D. 人脸识别

65. 报警系统紧急报警、入侵报警及防破坏报警响应时间应不大于（ ）。

A. 2s　　B. 5s　　C. 3s　　D. 4s

66. 被动红外探测器属于（ ）。

A. 点控制型探测器

B. 空间控制型探测器

C. 面控制型探测器

D. 线控制型探测器

67. 光缆是一种高速度、高频宽、（ ）、远距离的信号传输介质。

A. 高消耗

B. 低消耗

C. 低衰减

D. 高衰减

68. 出入口控制系统应（ ），并应能与电子巡查、入侵报警、视频安防监控等系统联动。

A. 能独立运行

B. 保持在线运行

C. 依托于建筑智能化系统运行

D. 本地化运行

69. 一卡通系统可以集成的安防子系统主要有：门禁、（ ）、访客和考勤管理系统。

A. 录像　　B. 抓拍　　C. 巡更　　D. 报警

70. 下列关于广角镜头的描述正确的是（ ）。

A. 焦距越小，视野越小

B. 焦距越大，视野越小

C. 焦距越小，视野越广

D. 焦距越小，视野越大

71. 加密技术的三个重要方法是（ ）。

A.数据加工、变换、验证

B.封装、变换、身份验证

C.封装、变换、验证

D.变换、校验、数据拼接

72.“能够确保敏感或机密的信息传输和存储不遭受未授权的浏览，甚至可以做到不暴露保密通信的事实。”属于信息安全的（ ）。

A.可用性　　B.完整性

C.非否认性　　D.机密性

73.能够保证信息系统的操作者或者信息的处理者不能否认其行为或处理结果,这可以防止参与某次操作或通信的乙方事后否认该事件曾发生过，这属于信息安全的（ ）。

A.可用性　　B.完整性

C.非否认性　　D.机密性

74.未被授权的实体通过窃听、截收、人员疏忽等方式得到信息的形式属于信息安全威胁的哪一种？（ ）

A.信息泄露　　B.篡改

C.间谍行为　　D.重放

75.计算机病毒具有的特征是（ ）。

A.隐蔽性　　B.传染性

C.破坏性　　D.以上都是

76.在学校或单位如果发现自己的计算机感染了病毒，应首先采取什么措施（ ）。

A.断开网络　　B.告知领导

C.杀毒　　D.重启

77.主要用于加密机制的协议是（ ）。

A.HTTP　　B.FTP

C.TELNET　　D.SSL

78.根据《信息安全等级保护管理办法》，（　）关规范和标准督促、检查、指导本行业、本部门或本地区信息系统运营、使用单位的信息安全等级保护工作。

A.公安机关　　B.国家保密工作部门

C.国家密码管理部门　　D.信息系统的主管部门

79.新建（　）信息系统，应当在投入运行后（　），由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

A.第一级以上30日内　　B.第二级以上60日内

C.第一级以上60日内　　D.第二级以上30日内

80.信息系统建设完成后，（　）的信息系统的运营使用单位应当选择符合国家规定的测评机构进行测评合格方可投入使用。

A.二级以上　　B.三级以上

C.四级以上　　D.五级以上

81．关键信息基础设施的安全保护等级应不低于等保（　）。

A. 第一级

B. 第二级

C. 第三级

D. 第四级

82．网络安全等级保护基本要求安全管理中心层面，集中管控要求，三级系统审计记录的留存时间至少（　）。

A. 一个月 B. 二个月 C. 三个月 D. 六个月

83．等保2.0中，不属于双因子鉴别的是（　）。

A. 口令+验证码

B. 口令+人脸识别

C. 口令+令牌

D. 口令+指纹

84．会话侦听与劫持技术属于（　）技术。

A. 密码分析还原

B. 协议漏洞渗透

C. 应用漏洞分析与渗透

D. DOS 攻击

85．凡是基于网络应用的程序都离不开（　）。

A. Socket　　B. Winsock C. 注册表　D. MFC 编程

86．只备份上次备份以后有变化的数据，属于数据备份类型的（　）。

A. 完全备份

B. 增量备份

C. 拆分备份

D. 按需备份

87．Hash 函数的输入长度是（　）。

A. 512bit　　B. 128bit　　C. 任意长度　　D. 160bit

88．以下关于 DOS 攻击的描述，哪句话是正确的？（　）

A. 不需要侵入受攻击的系统

B. 以窃取目标系统上的机密信息为目的

C. 导致目标系统无法处理正常用户的请求

D. 如果目标系统没有漏洞，远程攻击就不可能成功

89．下列不属于系统安全的技术是（　）。

A. 防火墙　B. 加密狗　C. 认证　D. 防病毒

90．不属于安全策略所涉及的方面是（　）。

A. 物理安全策略

B. 访问控制策略

C. 信息加密策略

D. 防火墙策略

91．SQL 杀手蠕虫病毒发作的特征是（　）。

A. 攻击手机网络

B. 攻击个人 PC 终端

C. 破坏 PC 游戏程序

D. 大量消耗网络带宽

92. 计算机信息系统安全保护等级根据计算机信息系统在国家安全、经济建设、社会生活中的（ ），计算机信息系统受到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的（ ）等因素确定。

A. 经济价值 经济损失

B. 重要程度 危害程度

C. 经济价值 危害程度

D. 重要程度 经济损失

93. 通过发送大量的欺骗包，每个包可能被几百个主机接收到，成倍的响应涌到目标系统，占据系统所有的资源获知导致系统崩溃或挂起。这种攻击属于以下哪种拒绝服务攻击（ ）。

A. SYN 湮没 B. Teardrop C. IP 地址欺骗 D. Smurf

94. 攻击者截获并记录了从 A 到 B 的数据，然后又从早些时候所截获的数据中提取出信息重新发往 B 称为（ ）。

A. 中间人攻击

B. 口令猜测器和字典攻击

C. 强力攻击

D. 重放攻击

95. 实现从 IP 地址到以太网 MAC 地址转换的命令为（ ）。

A. ping B. ifconfig C. arp D. traceroute

96. 在数据库的安全性控制中，授权的数据对象的（ ），授权予系统就越灵活。

A. 范围越小

B. 约束越细致

C. 范围越大

D. 约束范围大

97. 侵犯知识产权，黑客行为等信息道德与信息安全失范行为是从以下哪

个角度出发来定义（ ）。

A. 信息获取角度

B. 信息处理角度

C. 信息传播角度

D. 以上都不是

98. 如果一个信息系统，主要对象为涉及国家安全、社会秩序和公共利益的重要信息系统,其业务信息安全性或业务服务保证性受到破坏后，会对国家安全、社会秩序和公共利益造成严重损害；本级系统依照国家管理规范和技术标准进行自主保护，信息安全监管职能部门对其进行强制监督、检查。这应当属于等级保护的（ ）。

A. 强制保护级

B. 监督保护级

C. 指导保护级

D. 自主保护级

99. RSA 算法基于的数学难题是（ ）。

A. 大整数因子分解的困难性

B. 离散对数问题

C. 椭圆曲线问题

D. 费马大定理

100. 以下哪个协议不属于 TCP/IP 模型中网络层（ ）。

A. ICMP B. RARP C. IGMP D. RIP

二、 多选题（总共 60 小题，每题 2 分，计 120 分）

101.犯罪现场的无色潜在手印由于其载体物面性质和手印物质不同,所采取的观察方法亦不同，大体有（ ）。

A.透射光观察法 B.反射光观察法

C.“哈气”方法 D.借助特种光源进行观察

102．茚三酮显现手印时的操作方法有（ ）。

A.涂液法 B.浸泡法

C.喷雾法　　D.蒸显法

103.以下那些因素会影响手印显现化学反应（　）。

A.酸碱度的影响　　B.试剂和溶剂的影响

C.溶液浓度的影响　　D.温度湿度的影响

104.在手掌及脚掌面上的真皮层由（　）组成。

A.乳头层　　B.生发层

C.透明层　　D.网状层

105.静电吸附是提取足迹的有效方法，它可以提取（　）。

A.木板地上的尘土足迹　　B.木板地上的血足迹

C.纺织物上的尘土足　　D.纺织物上的血足迹

106.下列（　）可以成为文件检验对象。

A.文字　　B.符号　　C.语言　　D.图形

107.按照笔迹样本的形成来划分，笔迹样本可分为（　）。

A.案前样本　　B.平时样本　　C.案后样本　　D.实验样本

108.套摹的方式有（　）。

A.复印套摹　　B.重叠套摹　　C.复写套摹　　D.抑压套摹

109.常见损毁文件主要有（　）。

A.烧毁文件　　B.断离文件　　C.折叠文件　　D.浸泡粘连文件

110.个人的语音特征具有（　）三大基本属性。

A.稳定性　　B.共同性　　C.同一性　　D.特殊性

111. 公安部打击犯罪新机制有（　）。

A. 科学指挥、合成作战

B. 现场必勘、专业研判

C. 分类侦查、准确办案

D. 迅速分析，快速出警

112. 犯罪现场的要素有哪些（　）。

A. 犯罪行为要素

B. 时空要素

C. 物质形态变化要素

D. 人的要素

113. 现场保护的“相关人员” 包括哪些人（ ）。

A. 保卫处干部

B. 治保积极分子

C. 相关单位

D. 个人

114. 实地勘验对象有哪些（ ）。

A. 犯罪场所

B. 物品

C. 现场痕迹

D. 人身、尸体

115. 形成工具痕迹所必须具备的基本要素有（ ）。

A. 造型客体

B. 附着物质

C. 作用力

D. 承受客体

116. 提取足迹的常用方法（ ）。

A. 照相法

B. 原物提取法

C. 制模法

D. 静电复印法

117. 司法鉴定意见书出具后，发现有下列（ ）情形之一的，司法鉴定机构可以进行补正。

A. 图像、谱图、表格不清晰的

B. 签名、盖章或者编号不符合制作要求的

C. 结论有重大错误的

D. 文字表达有瑕疵或者错别字，但不影响司法鉴定意见的

118. 下列各项中，属于爆炸物证的有（　）。

A. 被炸者人体组织

B. 炸药微粒

C. 烟痕

D. 焦土

E. 现场足迹

119. 异体写法包括（　）方面的内容。

A. 异体字

B. 繁体字

C. 俗简化字

D. 用简化字

120. 实地勘验的一般步骤（　）。

A. 个体勘验

B. 局部观察

C. 整体巡视

D. 细致观察

121. 下列司法鉴定的检验方法中，属于物理学方法的有（　）。

A. 红外线检验法

B. 金相显微镜检验法

C. DNA 指纹技术

D. 显微结晶反应分析法

E. 容量法

122. 下列属于化学物证提取方法的有（　）。

A. 拍照法

B. 用吸尘器吸取

C. 用透明胶带粘取

D. 连同载体一起提取

E. 用镊子或竹片等工具直接提取

123. 下列各项属于不受理鉴定的条件有（ ）。

A. 直接指派鉴定人的委托

B. 鉴定资料不具备鉴定条件

C. 跨部门和跨地区的委托

D. 鉴定机构无力解决的问题

124. 下列各项中，常见的伪造文书手法有（ ）。

A. 复印法

B. 雕刻制版法

C. 涂抹掩盖法

D. 照相制版法

125. 在犯罪现场勘查中，见证人的权利和义务包括（ ）。

A. 有权对现场上发现、提取的痕迹、物品进行观察

B. 如果见证人认为勘查人员在实地勘验中有不正确的行为，可以要求停止勘验，并可要求把自己的意见记录在现场勘查笔录中

C. 勘查结束后，见证人应按要求在勘查笔录上签字或盖章

D. 严格保密，不得泄露所见证的情况

126. 动态勘验包含哪些内容（ ）。

A. 进一步发现不易看到的痕迹、物品或物质

B. 研究痕迹形成的原因、方式及与犯罪活动的关系

C. 显现并提取有关的痕迹、物品

D. 对物品的结构特征与形态变化进行的观察、记录和检查

127. 现场勘查要求有哪些（ ）。

A. 及时、全面

B. 细致、客观

C. 科学、合法

D. 安全

128. 见证人的义务有哪些（ ）。

A. 不得随意离开、走动，触摸相关痕迹、物证

B. 证明笔录中的一切记载是客观、真实的

C. 证明提取的痕迹、物证都是来源于现场，生物样本来源于相关人员

D. 根据审判的需要出庭作证

129. 下列各项中，实行司法官授权鉴定制度的国家有（ ）。

A. 法国

B. 加拿大

C. 德国

D. 英国

E. 俄罗斯

130. 下列各项中，体现个人语音习惯特性的有（ ）。

A. 音色

B. 音强

C. 音阶

D. 音长

E. 音高

131. 关于摄像机的描述，正确的是（ ）。

A. 摄像机的传感器尺寸越大，感光面积越大，成像效果越好

B. 720p 及以上分辨率的摄像机为高清摄像机

C. 4CIF、D1 分辨率的摄像机为标清摄像机

D. 网络摄像机可直接接入到 TCP/IP 的数字化网络中

132. 12mm 焦距的镜头相比 6mm 焦距的镜头具有以下哪些特点（ ）。

A. 12mm 的镜头监控距离更近

B. 12mm 的镜头监视范围更窄

C. 12mm 的镜头监控距离更远

D. 12mm 的镜头监视范围更宽

133. 典型的视频安防监控系统主要由（ ）组成。

A. 显示及记录部分

B. 传输部分

C. 控制部分

D. 摄像部分

134. 下列关于镜头与景深关系的描述正确的是（ ）。

A. 长焦镜头景深小

B. 长焦镜头景深大

C. 广角镜头景深小

D. 广角镜头景深大

135. 门禁系统进出识别方式分为以下（ ）。

A. 密码识别

B. 卡片识别

C. 生物识别

D. 二维码识别

136. 视频监控系统的设计来源于需求，需求是多种多样、千变万化的，但是都可以归纳为五个设计要素，包括（ ）。

A. 传输设计

B. 前端设计

C. 控制设计

D. 显示设计

137. 以下系统中属于安防系统的包括（ ）。

A. 电子考场系统

B. 视频监控系统

C. 考勤门禁系统

D. 楼宇对讲系统

138. 下列关于解码能力换算正确的是（ ）。

A. 1080P@60hz=2*720P@60hz

B. 1080P@30hz=4*4CIF

C. 1080P@60hz=2*1080P@30hz

D. 1080P@60hz=9*D1

139. 防盗报警系统的设备一般分为以下（ ）。

A. 前端控制器

B. 前端探测器

C. 后端探测器

D. 报警控制器

140. 视频存储系统有哪些（ ）。

A. 高可靠性

B. 可扩展性

C. 高码流

D. 高性能

141. 下面哪种是跨站脚本的攻击形式（ ）。

A. 盗取 Cookie

B. 钓鱼

C. 操纵受害者的浏览器

D. 蠕虫攻击

142. 数据在 Internet 上传输面临的威胁有（ ）。

A. 中间人攻击

B. 篡改攻击

C. 窃听攻击

D. 以上都不是

143. 下列关于基于网络的入侵检测系统说法不正确的是：（ ）。

A. 可以提供实时的网络检测行为

B. 可以处理加密后的数据

C. 可以同时保护多台网络主机

D. 影响被保护主机的性能

144. 针对入侵检测系统描述正确的是：（ ）。

A. 入侵检测系统可以通过网络和计算机动态地搜集大量关键信息资料,并能及时分析和判断整个系统环境的目前状态

B. 入侵检测系统一旦发现有违反安全政策的行为或系统存在被攻击的痕迹等,可以实施阻断操作

C. 入侵检测系统包括用于入侵检测的所有软硬件系统

D. 入侵检测系统可以与防火墙、交换机进行联动,成为防火墙的得力

“助手”,更好、更准确的控制外域间的访问

145. 下列哪些选项属于误用入侵检测技术？（ ）

A. 统计检测

B. 基于状态转移的入侵检测

C. 基于专家系统的入侵检测

D. 基于神经网络的入侵检测

146. 移动用户常用的 VPN 接入方式是（ ）。

A. L2TP

B. IPSEC+IKE 野蛮模式

C. GRE+IPSEC

D. L2TP+IPSEC

147. 关于 IP 报文头的 TTL 字段，以下说法正确的有（ ）。

A. TTL 主要是为了防止 IP 报文在网络中的循环转发,浪费网络宽带

B. 在正常情况下,路由器不应该从接口收到 TTL=0 的 IP 报文

C. TTL 的最大可能值是 65535

D. IP 报文每经过一个网络设备,包括 Hub、LanSwitch 和路由器，TTL 值都会被减去一定的数值

148. 利用 Metasploit 进行缓冲区溢出渗透的基本步骤包括（ ）。

A. 选择利用的漏洞类型

B. 选择 meterpreter 或者 shell 类型的 payload

C. 设置渗透目标 IP、本机 IP 地址和监听端口号

D. 选择合适的目标类型

149. 下列哪些选项属于木马程序？（ ）

A. X—Scan

B. 流光

C. Rootkit

D. 冰河

150. IPSec 可以提供哪些安全服务（ ）。

A. 数据机密性

B. 数据完整性

C. 数据来源认证

D. 防重放攻击

151. 一个 IP 报文在网络传送途中被分片，生成了 3 个新的 IP 包，则以下说法正确的是（ ）。

A. 这 3 个 IP 包有相同的标识(Identification)字段

B. 这 3 个 IP 包有相同的标志(MF、DF)字段

C. 这 3 个 IP 包有相同的目的地址字段

D. 这 3 个 IP 包有相同的报文总长度(2 字节)字段

E. 这 3 个 IP 包有相同的偏移字段

152. PKI 能够执行的功能是（ ）和 （ ）。

A. 鉴别计算机消息的始发者

B. 确认计算机的物理位置

C. 保守消息的机密

D. 确认用户具有的安全性特权

153. VPN 按照组网应用分类,主要有哪几种类型？（ ）

A. AccessVPN

B. ExtranetVPN

C. IntranetVPN

D. ClientinitiatedVPN

154. 网络嗅探的检测方法有？（ ）

A. ping 检测

B. ARP 检测网络嗅探

C. DNS 检测网络嗅探

D. 根据网络和主机响应时间检测网络嗅探

155. 下面那些方法可以检测恶意 ICMP 流量？（ ）

A. 检测同一来源 ICMP 数据包的数量

B. 注意那些 ICMP 数据包中 payload 大于 64 比特的数据包

C. 寻找那些响应数据包中 payload 跟请求数据包不一致的 ICMP 数据包

D. 检查 ICMP 数据包的协议标签

156. 下面哪些选项属于黑客经常利用的漏洞？（ ）

A. 拒绝服务攻击漏洞

B. 缓冲区溢出

C. 远程命令执行漏洞

D. 脚本执行漏洞

157. SSL 远程接入方式包括（ ）。

A. Web 接入

B. TCP 接入

C. IP 接入

D. 手工接入

158. 源代码泄露可能让攻击者分析出哪些其它漏洞？（ ）

A. SQL 注入

B. 命令执行

C. 文件上传

D. XSS

159. 在 RHEL5 系统中，以下（ ）操作将在分区/dev/sdb7 上创建 EXT3 文件系统。

A. mkfs -t ext3 /dev/sdb7

B. mkfs.ext3 /dev/sdb7

C. fdisk -t ext3 /dev/sdb7

D. format /dev/sdb7 -t ext3

160. HTTP 协议攻击有哪些？（ ）

A. 跨站脚本攻击

B. SQL 注入攻击

C. DNS 劫持

D. 命令注入攻击

三、判断题（总共 40 题，每题 2 分，计 80 分）

161. 碘熏法显现出的手印可直接提取保存。（ ）

162. 文件检验属于技术侦查与司法鉴定手段。（ ）

163. 笔迹的本质是个人书写习惯的表现形式。（ ）

164. 印章，又称图章，是用于在文件上形成印文以表示文件签署的一种特殊文具。（ ）

165. 中国古代，就书面文字材料称作“文书” 。（ ）

166. 检材在涉及文件物证的案件中是确定案件性质的必不可少的。（ ）

167. 随意伪装笔迹具有整体熟练程度降低的基本特点。（ ）

168. 摹仿笔迹主要包括临摹、套摹与凭记忆摹仿三种基本类型。（ ）

169. 证件是用来证明地位和权力的文件。（ ）

170. 汉语方言总的特点为北方各方言差异大，南方各方言差异小。（ ）

171. 立体手印模型的凸凹形态与手掌上纹线的凸凹形态是相反的。（ ）

172. 中心有一根以上的大头闭口箕型线，其中心腔内有一根以上突向箕口的弧形线（与引向箕口的纹线相接触）所组成的形似囊袋状的花纹形态称为闭口箕型纹。（ ）

173. 小微粒悬浮液试用于显现潮湿的渗透性和非渗透性客体表面的手印。（ ）

174. 磁性粉中主粉起显色作用，配粉起媒介、运载和稀释作用。（ ）

175. 文件包括书报、稿件、照片、发票。（ ）

176. 笔迹检验的任务之一是判断物证笔迹与嫌疑人笔迹是否为同一人所写。（ ）

177. 笔迹检验的主要目的在于识别书写人的社会属性与自然属性。（ ）

178. 文件检验的基本方法包括种类识别与同一认定。（ ）

179. 污损文件:受人为或是自然条件变化损毁,影响其内容可读性的文件。（ ）

180. 变造文件就是使用印刷手段伪装的文件。（ ）

181. 主动探测与被动探测的根本差别是：探测装置是否向空间发出某种能量。（ ）

182. 电锤的缺点是照动大，对周边构筑物有一定程度的破坏作用。（ ）

183. 当连续 2 次在现场识读装置实施误操作时，系统应能发出报警信号。（ ）

184. 锁具类产品主要指机械防盗锁，也包括电子锁、汽车防资锁等。（ ）

185. 探测器的电源线路及报警信号传输线路被破坏时，报警控制器均应发出报警信号。（ ）

186. 一般情况下，线径越细，衰减越大，容量越小，传输距离越近。（ ）

187. 门禁控制器与前端连接设备的线缆敷设结构形式是点到点星形结构。（ ）

188. 可视对讲门口机的安装高度应为 1m。（ ）

189. 视频监控系统只能由系统管理软件进行功能设置。（ ）

190. 集成就是将各种技术集中在一起。（ ）

191. 我国规定安全电压是工顿有效值不超过 60 伏。（ ）

192. 出入口控制系统中使用的设备必须符合国家法律法规和现行强制性标准的要求，并经法定机构检验或认证合格。（ ）

193. 安全防范技术由于其特殊性，不适合于其它领域。（ ）

194. 质量标准是对竣工后需要进行检测检查的内容和要求进行规定。（ ）

195. 线径的确定一般需要通过计算完成，经验丰富的工程师也可以取经验值。（ ）

196. 基尔霍夫电压定律可以根据能量守恒定律推导出来，当单位正电荷从任何一点沿-闭合路径移动回到原点，电场对它作的功，其能量增加。（ ）

197. 高空作业用升降装置(包括梯子)一定要由作业人员自己操作或看护。（ ）

198. 施工项目安全生产第一责任人是安全员。（ ）

199. 视频监控系统应尽可能长的存贮图像信息。（ ）

200. 监控立杆的防腐处理应采用绕生料带。（ ）

模块二：物证检验与数字取证技能模块

物证鉴定技术

任务 3. 手印鉴定技术应用（200 分）

案件任务书

件 景	某法院受理一起民间借贷纠纷，原告王平月要求被告张三还款，李四作为担保人承担连带责任。王月平向法院提交的主要证据为《借款合同》及转账记录等，王平月称《借款合同》落款“张三”签名处指印及内容“叁（三)”处指印为张三手指捺印，落款“李四”签名处指印及内容“责任”字迹处指印为李四手指捺印。张三及李四对《借款合同》的真实性提出异议，否认本人捺印。为查清案件事实，法院送检委托指印鉴定。具体事项如下： 1.《借款合同》上内容“叁（三)”处指印（检材指印-1）是否为张三手指捺印； 2.《借款合同》上落款“张三”签名处指印是否为张三手指捺印； 3.《借款合同》上落款“李四”签名处指印是否为李四手指捺印。 注：送检的《借款合同》上的指印已确认为手指蘸取印泥直接捺印形成，无需质疑其形成过程及形成方式。
检 材 料	**检材**：借款人为“张三”、借款期限为“2020 年 3 月 7 日至 2021 年 3 月 7 日”的《借款合同》扫描图片 1 张，《借款合同》落款“张三”签名处指印下称“检材指印-1”,《借款合同》内容“叁（三)”处指印下称“检材指印-2”,《借款合同》落款“李四”签名处指印下称“检材指印-3”。 （见“送检材料”文件夹中名为“检材.jpg”的图像文件)。
务 要 求	1.指印分析：分析本案检材指印-1、检材指印-2、检材指印-3 的指位、基本纹型、鉴定条件； 2.指印细节特征寻找：寻找并确定检材指印-1、检材指印-2、检材指印-3 上的指印细节特征，并标识名称。
意 事 项	1.参赛小组应尽可能全面地进行检验和分析，必要时可附图表等支撑材料。 2.成绩评价依赖于参赛小组反馈的信息，信息不充分将会影响最终的评审结果。 3.任务所需附件内容请从竞赛平台下载。

网络取证技术

任务 4. 内存取证 M（100 分）

案件任务书

A 监狱某服务器系统感染恶意程序，导致系统关键文件被破坏，信息被窃取。请分析 A 集团提供的系统镜像，找到恶意程序及破坏系统的证据信息。

本任务素材清单：操作系统镜像、内存镜像。

请根据赛题环境及任务要求提交正确答案。

1.对内存文件进行取证分析，将攻击者攻击服务器所使用的端口号作为 flag 值提交，提交格式：端口号 1+端口号 n...；（提示：服务器下载内存文件 data.mem）

2.对内存文件进行取证分析，找打攻击者存放的可执行木马，将木马文件的绝对路径以及运行的 PID 作为 flag 值提交，提交格式：路径+PID；

3.对内存文件进行取证分析，找出系统的可疑账号，将可疑账户作为 flag 值提交;

4.对内存文件进行取证分析，找出遭受攻击的服务版本号，将版本号作为 flag 值提交；

5.对内存文件进行取证分析，找出黑客上传的恶意文件，将上传的恶意文件名称以及时间作为 flag 值提交，提交格式：2021:22:44:23+文件名；

6.对内存文件进行取证分析，找到后门账号，将此账号的密码作为 flag 值提交。

说明：

1、本体 writeup 文件名夹命名：GWXX-4.zip（XX 为工位号）；

2、文件名夹保存在物理机桌面，并同步提交与竞赛平台。

任务 5. FTP 流量分析（100 分）

案件任务书

近日 B 监狱截取到了一份可疑的流量包，推测是内部的间谍向外部发送的信息,现已经将流量包提取出，请你协助并找出隐写的信息。

注意：服务器 IP 在答题平台显示，如 IP 不显示，请尝试刷新页面。

1.访问靶机找到隐藏的流量包文件，计算文件 MD5 值作为 FLAG 提交；

2.统计流量包中基于 TCP 协议的应用层协议，将所有用到的协议作为 FLAG（形式：[协议名字一,协议名字二]）提交；

3.分析流量包，将通过 FTP 下载文件的第一个包的序号作为 FLAG 提交；

4.分析流量包，将使用显示过滤器过滤 ftp - data 为下载为文件的过滤表达提交；

5.分析流量包，将找到通过 FTP 传输的文件名作为 FLAG 提交；

6.分析通过 FTP 传输的文件，将文件的类型作为 FLAG 提交；

7.分析最后找到的文件，将文件中的 FLAG 信息提交。

说明：

1、本体 writeup 文件名夹命名：GWXX-5.zip（XX 为工位号）；

2、文件名夹保存在物理机桌面，并同步提交与竞赛平台。

模块三：监所安防和信息系统运维技能

监所信息管理系统安全攻防

任务 6. Linux 系统安全运营（100 分）

C 市检察院运维过程中发现一重要服务器疑似存在安全风险，为处理服务器的安全风险，现指派你作为本次任务的负责人完成该服务器的渗透测试，请按照答题卡要求完成任务。

1.分析系统异常流量，找出异常的账户并删除，将此账户第一次创建后登录系统的时间作为 flag 值提交，提交格式：00:00:00；

2.对系统账户进行加固，将 root 账户的密码与加密方式作为 flag 值提交，提交格式：密码-加密方式；

3.对系统进行故障排查，切换 root 账户，为了防止其他用户再次登录创建相应文件，将操作用到的全部命令作为 flag 值提交

4.对当前系统的服务进行排查，将系统开机自启动的服务数量作为 flag 值提交

5.分析系统的任务，找出恶意后门，将后门文件中隐藏的内容作为 flag 值提交，提交格式：隐藏内容+端口号

6.对目标系统后门进行排查，对相应服务进行加固，将加固的配置命令作为 flag 值提交

7.对目标系统进行安全加固，为历史命令添加执行时间，将需要添加的环境变量名称以及修改后刷新 shell 环境所使用的命令作为 flag 值提交，提交格式：变量名称+命令。

说明：

1、本体 writeup 文件名夹命名：GWXX-6.zip（XX 为工位号）；

2、文件名夹保存在物理机桌面，并同步提交与竞赛平台。

任务 7. FTP 配置评估（100 分）

一、A 市监狱系统为提高网络服务器的安全性，现拟从以下几个方面对网络服务器进行加固。

1.通过分析 FTP 服务器的配置，将除 ftp001 用户以外的用户都锁定在用户主目录下，将需要修改的配置项作为 flag 值提交，如涉及到多项内容，中间用/分隔，提交格式：flag{***/***}；

2.通过分析 FTP 服务器的配置，禁止匿名用户创建目录，将需要修改的配置项作为 flag 值提交，如涉及到多项内容，中间用/分隔，提交格式：flag{***/***}；

3.通过分析 FTP 服务器的配置，配置用户的家目录为/var/www/html，将需要修改的配置项作为 flag 值提交，如涉及到多项内容，中间用/分隔，提交格式：flag{***/***}；

4.通过分析 FTP 服务器的配置,启用/etc/hosts.permit 和/etc/hosts.deny 文件，将需要修改的配置项作为 flag 值提交，如涉及到多项内容，中间用/分隔，提交格式：flag{***/***}；

5.通过分析 FTP 服务器的配置，拒绝所有 user_list 中的用户登入，将需要修改的配置项作为 flag 值提交，如涉及到多项内容，中间用/分隔，提交格式：flag{***/***}；

6.通过分析 FTP 服务器的配置，启用主动模式，将需要修改的配置项作为 flag 值提交，如涉及到多项内容，中间用/分隔，提交格式：flag{***/***}；

7.通过分析 FTP 服务器的配置,将禁止访问 FTP 的用户列表默认文件名作为 flag 值提交，如涉及到多项内容，中间用/分隔，提交格式：flag{***/***}。

二、说明：

1、所有 flag 信息提交格式为 flag{xxxx}；

2、本体 writeup 文件名夹命名：GWXX-7.zip（XX 为工位号）；

3、文件名夹保存在物理机桌面，并同步提交与竞赛平台。