首届“盘古石杯”全国电子数据取证大赛

容器密码

加密容器密码：usy1UN2Mmgram&^d?0E5r9myrk!cmJGr

公告：

- 2023-05-06 13:40:13

  赛程公告

  所有参赛选手，移动智能终端取证第18题、第20题、第21题不用参考(答题格式2000-01-01)，以实际题目对应答案提交，第19题(答案格式:2000-01-01 13:36:25)

- 2023-05-06 11:24:15

  赛程公告

  所有参赛选手，移动智能终端取证第12题为选择题，A：18043618705 B：19212175391 C:19212159177 D:18200532661 注意答案必须大写 如：A

- 2023-05-06 11:23:54

  赛程公告

  所有参赛选手，计算机取证第3题为选择题，A：掠夺攻略.docx B：工资表.xlsx C:刷单秘籍.docx D:脚本.docx 注意答案必须大写 如：A

- 2023-05-06 11:23:31

  赛程公告

  所有参赛选手，计算机取证第2题为选择题，A：Edge B:Internet Explorer C:Google Chrome D:360浏览器 注意答案必须大写，如：A

- 2023-05-06 10:12:01

  赛程公告

  所有参赛选手，移动智能终端取证第12题为选择题，A：18043618705 B：19212175391 C:19212159177 D:18200532661

- 2023-05-06 10:11:45

赛程公告

所有参赛选手，计算机取证第3题为选择题，A：掠夺攻略.docx B：工资表.xlsx C:刷单秘籍.docx D:脚本.docx

- 2023-05-06 09:25:24

  赛程公告

  加密容器密码：usy1UN2Mmgram&^d?0E5r9myrk!cmJGr

- 2023-05-06 07:41:27

  赛程公告

  1、全程录屏 所有参赛队员使用的电脑，都需要进行录屏操作（如有的选手使用两台电脑答题，那么需要上交两个录屏）。录屏软件不做要求，录屏文件要能够清晰查看解题思路，严禁后期处理。比赛过程中间录屏可以间断一次，保存录屏文件。除此之外录屏过程必须完整，不能间断。如发生特殊情况，致使录屏间断，请及时在QQ群里跟工作人员沟通，录屏间断，未与工作人员沟通的，后边不接受任何的解释，取消成绩。赛后请保存录屏文件7天以上，以供审核人员随时抽查。

- 2023-05-06 07:41:15

  赛程公告

  2、答题要求 每题都要求上传题目的操作核心步骤截图，所有截图按照题号放在自行创建的word文件中，考试结束一小时后立即将该文件发送到组委会提供的邮箱内（liucong01@qianxin.com，lvxuesong@qianxin.com，wangxiaoming02@qianxin.com）。 以上截图均为电脑全屏截图，必须包含系统任务栏。没有解题思路的成绩无效。

- 2023-05-06 07:41:02

  赛程公告

  3、成绩计算 三人协作团队共同答题。

Android程序分析

1.涉案应用刷刷樂的签名序列号是(答案格式：123ca12a)(★☆☆☆☆)

2.涉案应用刷刷樂是否包含读取短信权限(答案格式：是/否)(★★☆☆☆)

3.涉案应用刷刷樂打包封装的调证ID值是(答案格式：123ca12a)(★★☆☆☆)

4.涉案应用刷刷樂服务器地址域名是(答案格式：axa.baidun.com)(★★★☆☆)

5.涉案应用刷刷樂是否存在录音行为(答案格式：是/否)(★★★☆☆)

6.涉案应用未来资产的包名是(答案格式：axa.baidun.com)(★☆☆☆☆)

7.涉案应用未来资产的语音识别服务的调证key值是(答案格式：1ca2jc)(★★☆☆☆)

8.涉案应用未来资产的服务器地址域名是(答案格式：axa.baidun.com)(★★★☆☆)

9.涉案应用未来资产的打包封装的调证ID值是是(答案格式：axa.baidun.com)(★★☆☆☆)

移动智能终端取证

1.根据容恨寒的安卓手机分析，手机的蓝牙物理地址是(答案格式：B9:8B:35:8B:03:52)(★☆☆☆☆)

2.根据容恨寒的安卓手机分析，SIM卡的ICCID是(答案格式：80891103212348510720)(★☆☆☆☆)

3.根据容恨寒的安卓手机分析，团队内部沟通的聊天工具程序名称是(答案格式：微信)(★☆☆☆☆)

4.根据容恨寒的安卓手机分析，团队内部沟通容恨寒收到的最后一条聊天信息内容是(答案格式：好的)(★★★☆☆)

5.根据容恨寒的安卓手机分析，收到的刷单.rar的MD5值是(答案格式：202cb962ac59075b964b07152d234b70)(★★☆☆☆)

6.根据容恨寒的安卓手机分析，收到的刷单.rar的解压密码是(答案格式：abcdg@1234@hd)(★★★☆☆)

7.根据容恨寒的安卓手机分析，发送刷单.rar的用户的手机号是(答案格式：15137321234)(★★★★☆)

8.根据容恨寒的安卓手机分析，发送多个报表的用户来自哪个部门(答案格式：理财部)(★★★★★)

9.根据容恨寒的安卓手机分析，MAC的开机密码是(答案格式：asdcz)(★☆☆☆☆)

10.根据容恨寒的安卓手机分析，苹果手机的备份密码前4位是(答案格式：1234)(★☆☆☆☆)

11.根据魏文茵苹果手机分析，IMEI号是？(答案格式:239471000325479)(★☆☆☆☆)

12.根据魏文茵苹果手机分析，可能使用过的电话号码不包括？(答案格式:13527821339)(★☆☆☆☆)

13.根据臧觅风的安卓手机分析，微信ID是(答案格式：wxid_av7b3jbaaht123)(★☆☆☆☆)

14.根据臧觅风的安卓手机分析，在哪里使用过交友软件(答案格式：杭州)(★★★☆☆)

15.根据臧觅风的安卓手机分析，嫌疑人从哪个用户购买的源码，请给出出售源码方的账号(答案格式：1234524229)(★☆☆☆☆)

16.根据臧觅风的安卓手机分析，购买源码花了多少BTC？(答案格式：1.21)(★☆☆☆☆)

17.根据臧觅风的安卓手机分析，接收源码的邮箱是(答案格式：asdasd666@hotmail.com)(★☆☆☆☆)

18.嫌疑人容恨寒苹果手机的IMEI是?(答案格式:2000-01-01)(★★☆☆☆)

19.嫌疑人容恨寒苹果手机最后备份时间是?(答案格式:2000-01-01)(★★☆☆☆)

20.嫌疑人容恨寒苹果手机“易信”的唯一标识符（UUID）？(答案格式:2000-01-01)(★★★★☆)

21.嫌疑人容恨寒苹果手机微信ID是?(答案格式:2000-01-01)(★☆☆☆☆)

计算机取证

1.嫌疑人魏文茵计算机的操作系统版本?(答案格式:Windows 7 Ultimate 8603)(★☆☆☆☆)

2.嫌疑人魏文茵计算机默认的浏览器是?(答案格式:Internet Explorer)(★☆☆☆☆)

3.嫌疑人魏文茵计算机中以下那个文档不是嫌疑人最近打开过的文档?(答案格式:D)(★☆☆☆☆)

4.嫌疑人魏文茵计算机中存在几个加密分区?(答案格式:3个)(★★☆☆☆)

5.嫌疑人魏文茵计算机中安装了哪个第三方加密容器?(答案格式:VeraCrypt))(★☆☆☆☆)

6.接上题，嫌疑人魏文茵计算机中加密容器加密后的容器文件路径？(答案格式:C:\xxx\xxx)(★★☆☆☆)

7.嫌疑人魏文茵计算机中磁盘分区BitLocker加密恢复秘钥为?(答案格式: 000000-000000-000000-000000-000000-000000-000000-000000))(★★★☆☆)

8.嫌疑人魏文茵计算机中BitLocker加密分区中“攻略.docx”文档里涉及多少种诈骗方式?(答案格式:11)(★☆☆☆☆)

9.投资理财团伙“华中组”目前诈骗收益大约多少?(答案格式:10万)(★★☆☆☆)

10.通过对嫌疑人魏文茵计算机内存分析，print.exe的PID是？(答案格式:123)(★★☆☆☆)

11.根据臧觅风的计算机分析，请给出技术人员计算机“zang.E01”的SHA-1?(答案格式:7B2DC1741AE00D7776F64064CDA321037563A769)(★☆☆☆☆)

12.根据臧觅风的计算机分析，请给出该技术人员计算机“zang.E01”的总扇区数？(答案格式:100,000,000)(★★☆☆☆)

13.根据臧觅风的计算机分析，以下那个文件不是技术人员通过浏览器下载的？(答案格式:A)(★☆☆☆☆)

A.WeChatSetup.exe

B.aDrive.exe

C.Potato_Desktop2.37.zip

D.BaiduNetdisk_7.27.0.5.exe

14.根据臧觅风的计算机分析，请给出该技术人员邮件附件“好东西.zip”解压密码？(答案格式:abc123)(★★★★★)

15.根据臧觅风的计算机分析，该技术人员电脑内曾通过远程管理工具连接过服务器“master.k8s.com”,请给出连接的端口号？(答案格式:22)(★★☆☆☆)

16.根据臧觅风的计算机分析，接上题，请给出服务器的密码？(答案格式:password(★★★★☆)

17.根据臧觅风的计算机分析，据该技术人员交代，其电脑内有个保存各种密码的txt文件，请找出该文件，计算其MD5值？(答案格式:7B2DC1741AE00D7776F64064CDA321037563A769)(★★★★★)

18.根据臧觅风的计算机分析，该技术人员曾使用过加密容器反取证技术，请给出该容器挂载的盘符？(答案格式:A)(★☆☆☆☆)

19.根据臧觅风的计算机分析，请给出该技术人员电脑内keePass的Master Password？(答案格式:password12#)(★★★★☆)

20.根据臧觅风的计算机分析，请给出该技术人员所使用的爬虫工具名称？(答案格式:xxx)(★★☆☆☆)

21.根据臧觅风的计算机分析，接上题，该技术人员通过该采集器一共采集了多少条人员信息数据？(答案格式:10,000)(★★★★★)

22.根据臧觅风的计算机分析，以下那个不是该技术人员通过爬虫工具采集的数据？(答案格式:A)(★☆☆☆☆)

A.中国证券投资基金业协人员信息

B.仓山区市场监督管理局行政执法人员信息

C.清平镇卫生院基本公共卫生服务

D.仓山区市场监督管理局行政执法人员信息

23.根据臧觅风的计算机分析，该嫌疑人曾浏览过“阿里云WebDAV”，请给出该“阿里云WebDAV”端口号？(答案格式:2211)(★★☆☆☆)

24.根据臧觅风的计算机分析，请给出该技术人员电脑内代理软件所使用的端口号？(答案格式:2211)(★★☆☆☆)

25.根据臧觅风的计算机分析，接上题，请给出该代理软件内订阅链接的token？(答案格式:abc1234df334...)(★★☆☆☆)

26.根据臧觅风的计算机分析，请给出该技术人员电脑内用于内部通联工具的地址和端口？(答案格式:www.baidu.com:1122)(★★★☆☆)

27.根据臧觅风的计算机分析，请给出该电脑内存镜像创建的时间（北京时间）？(答案格式:2023-05-06 14:00:00)(★☆☆☆☆)

28.根据臧觅风的计算机分析，以下那个不是“chrone.exe”的动态链接库？(答案格式:A)(★★★★☆)

A.ntdll.dll

B.iertutil.dll

C.wow64cpu.dll

D.wow64win.dll

29.根据臧觅风的计算机分析，请给出“\REGISTRY\MACHINE\SYSTEM”在内存镜像中的虚拟地址是多少？(答案格式:0xxxxx123...)(★★☆☆☆)

30.根据臧觅风的计算机分析，据嫌疑人交代，其电脑上曾存打开过一个名为“账号信息.docx”的文档，请给出该文档的最后访问时间（北京时间）？(答案格式:2023-05-06 14:00:00)(★★★★☆)

31.根据臧觅风的计算机分析，接上题，请给出该文档的存储路径？(答案格式:C:\xxx\xxx)(★★★☆☆)

32.嫌疑人容恨寒苹果电脑的系统版本名称是？(答案格式:注意大小写)(★☆☆☆☆)

33.嫌疑人容恨寒苹果电脑操作系统安装日期是？(答案格式:2000-01-01)(★★☆☆☆)

34.嫌疑人容恨寒苹果电脑的内核版本是？(答案格式:xxxxx 11.0.4，注意大小写)(★☆☆☆☆)

35.嫌疑人容恨寒苹果电脑有多少正在运行的后台程序？(答案格式:20)(★★☆☆☆)

36.嫌疑人容恨寒苹果电脑最后一次关机时间（GMT）？(答案格式:2000-01-01 01:00:09)(★★☆☆☆)

37.嫌疑人容恨寒苹果电脑执行过多少次查询主机名称命令？(答案格式:20)(★★★☆☆)

38.从嫌疑人容恨寒苹果电脑中找出“陆文杰”提现金额是？(答案格式:20)(★★★★☆)

39.从嫌疑人容恨寒苹果电脑中找出嫌疑人容恨寒上午上班时长是？(答案格式:8小时)(★★★★☆)

40.从嫌疑人容恨寒苹果电脑中找出“万便”的邮箱是？(答案格式:xxx@xxx.xx)(★★★★☆)

41.通过分析得出嫌疑人容恨寒小孩的年龄是？(答案格式:10岁)(★★★☆☆)

二进制文件分析

1.根据魏文茵的计算机分析，恶意程序加了什么类型的壳(答案：asdcz)(★★☆☆☆)

2.根据魏文茵的计算机分析，恶意程序调用了几个dll(答案：1)(★★★☆☆)

3.根据魏文茵的计算机分析，恶意程序中send函数被多少个函数调用(答案：1)(★★★☆☆)

4.根据魏文茵的计算机分析，恶意程序远控端ip(答案：120.1.2.3)(★★☆☆☆)

5.根据魏文茵的计算机分析，恶意程序远控端端口(答案：123)(★★☆☆☆)

6.根据魏文茵的计算机分析，恶意程序用到是tcp还是udp(★★★☆☆)

A.tcp

B.udp

7.根据魏文茵的计算机分析，恶意程序能执行几条命令(答案：123)(★★★★☆)

8.根据魏文茵的计算机分析，恶意程序加密电脑文件对应是哪个命令(答案：1a)(★★★☆☆)

9.(多选题)根据魏文茵的计算机分析，恶意程序加密哪些后缀文件(★★★☆☆)

A.docx

B.xlsx

C.pdf

D.doc

10.根据魏文茵的计算机分析，编写该程序电脑的用户名是(答案：12345)(★★★★★)

11.嫌疑人魏文茵计算机中“工资表.xlsx”中，发放工资总金额为：(答案格式:12345))(★★★★★)

暗网取证

1.臧觅风电脑使用暗网浏览器版本是？(答案格式：10.0.0)(★☆☆☆☆)

2.臧觅风电脑使用的暗网浏览器历史记录中最多浏览内容是？(答案格式：制作)(★★☆☆☆)

3.臧觅风电脑使用的暗网网浏览器书签“社工库”添加的时间是？(答案格式：2000-01-01 01:00:09)(★★★★☆)

4.臧觅风电脑使用的暗网浏览器第一次使用时间是？(答案格式：2000-01-01 01:00:09)(★★★☆☆)

5.臧觅风电脑使用的暗网浏览器扩展应用中“ftp.js”文件的md5值是？(答案格式：字母小写)(★★★★★)

物联取证

1.请给出该软路由管理的IP地址？(答案格式:192.168.1.1)(★☆☆☆☆)

2.请给出该软路由管理员的密码？(答案格式:admin123!@#)(★★★☆☆)

3.请给出阿里云WebDAV的token？(答案格式:bac123sasdew3212...)(★★☆☆☆)

4.请给出该软路由所用机场订阅的token？(答案格式:bac123sasdew3212...)(★★☆☆☆)

5.请给出该软路由数据卷的UUID？(答案格式:8adn28hd-00c0c0c0...)(★★☆☆☆)

6.请给出该软路由的共享路径？(答案格式:/home/data)(★★☆☆☆)

服务器取证

1.请给出IM服务器的当前Build版本？(答案格式:11111)(★☆☆☆☆)

2.请给出IM聊天服务的启动密码？(答案格式:3w.Baidu.com)(★★★★★)

3.请给出该聊天服务器所用的PHP版本？(答案格式:7.2.5)(★★★★☆)

4.请给出该服务器所用的数据库类型及版本？(答案格式:mysql 5.7.1)(★★★★★)

5.请给出该服务器MySQL数据库root账号的密码？(答案格式:3w.baidu.com)(★★★★★)

6.请给该IM服务器内当前企业所使用的数据库？(答案格式:admin_admin)(★★★★☆)

7.请给出该组织“usdtreclub”内共有多少个部门（不含分区）？(答案格式:1)(★★★☆☆)

8.客户端消息传输采用哪种加密形式？(答案格式:A)(★★☆☆☆)

A.AES128

B.AES256

C.DES

D.Base64

9.以下那个不是此系统提供的应用？(答案格式:A)(★★☆☆☆)

A.云盘

B.审批

C.会议

D.考勤

10.请给出“ 2023-04-11 21:48:14”登录成功此系统的用户设备MAC地址？(答案格式:08-AA-33-DF-1A)(★★★☆☆)

11.请给出用户“卢正文”的手机号码？(答案格式:13888888888)(★★★★☆)

集群服务器取证

1.请给出集群master节点的内核版本？(答案格式:2.6.0-104.e11.x86_64)(★☆☆☆☆)

2.请给出该集群的pod网络？(答案格式:192.168.0.0/24)(★★★★☆)

3.请给出该集群所用的网络插件？(答案格式:abcd)(★★☆☆☆)

4.默认ns除外，本集群共有多少个ns？(答案格式:1)(★★★☆☆)

5.请给出该集群的集群IP？(答案格式:192.168.0.0)(★★☆☆☆)

6.请给出该ns为“licai”svc为“php-svc”的访问类型？(答案格式:Abc)(★★☆☆☆)

7.请给出ns为“shuadan”下的的PHP版本？(答案格式:1.1)(★★★★★)

8.请给出本机集群所使用的私有仓库地址？(答案格式:192.168.0.0)(★★★★☆)

9.接上题，请给出登录该私有仓库所用的token？(答案格式:bae213ionada21...)(★★★★★)

10.请给出“licaisite”持久化存储的大小？(答案格式:10G)(★★☆☆☆)

11.接上题，请给出对应的存储持久化声明名称？(答案格式:abc-abc)(★★★☆☆)

12.请给出集群内部署网站所使用数据库的IP地址和端口号？(答案格式:192.168.0.0:8080)(★★★☆☆)

13.请给出网站“vip.kefu.com”所使用的端口号？(答案格式:8080)(★★☆☆☆)

14.请给出网站“vip.shuadan.com”连接数据库所使用的账号和密码？(答案格式root/password)(★★★★★)

15.请给出调证数据库的版本号？(答案格式5.7.1)(★★★★★)

16.请给出刷单网站客服域名？(答案格式:http://www.baidu.com:8080/login.html)(★★★★★)

17.请给出理财客服系统用户“admin”共有多少个会话窗口？(答案格式:123)(★★★★★)

18.刷单客服是嵌套在刷单源码下那个文件内，请给出该文件在网站源码内的目录和文件名？(答案格式:www.baidu.com:8080/login.html)(★★★★★)

19.请统计出刷单网站后台累计提现成功的金额？(答案格式:1000)(★☆☆☆☆)

20.请给出受害人上级的电话号码？(答案格式:13888888888)(★★★☆☆)

21.请给出刷单网站受害人加款的时间（北京时间）？(答案格式:2023-05-06 14:00:00)(★★★☆☆)

22.该理财网站曾经被挂马，请给出上传木马者的IP？(答案格式:192.168.10.10)(★★★☆☆)

23.接上题，请找到此木马，计算该木马的md5？(答案格式:123dadgadad332...)(★★★☆☆)

24.请统计该投资理财平台累计交易额为多少亿？(答案格式:1.8)(★★☆☆☆)

25.请给出该虚拟币投资平台内用户“李国斌”的银行卡号？(答案格式:622222222222222)(★★★☆☆)

26.分析该虚拟币投资平台财务明细表，用户“13912345678”共支出多少钱（cnc），结果保留两位小数?(答案格式:10000.00)(★★★★★)