**案情介绍：**

A文化公司与B电影公司为了偷逃税，签订了“阴阳合同”， 一份对内，一份对外，得知税务部门即将到某文化公司检查时，该公司财务王某将代表双方真实意思表示的合同烧毁，合同的电子档删除，并格式化了存储该合同电子档的分区。

**根据以上案情，回答下面的题目：（多选题）**

**1、关于该案，应该在什么位置或环境中查找代表双方真实意思表示的合同数据？**

A、王某的手机中

B、王某的办公电脑中

C、B电影公司财务室的办公电脑中

D、A公司负责人的电脑中

**2、以下哪些做法，能够比较快速定位到代表代表双方真实意思表示的合同数据?**

A、设置关键字，进行搜索，包括“合同”、“真实”、“金额”

B、设置关键字，进行搜索，包括“A文化公司”、“B电影公司”、“合同”

C、设置关键字，进行搜索，包括“甲方”、“乙方”、“权利”、“义务”

D、以上都可以

**第一题：ABCD**

解析：税务人员有权检查与公司经营有关的文件，在上述四个答案中提到的电子设备中均可能存在代表双方真实意思表示的合同。

**第二题：BC**

解析：合同中通常包括“甲方”、“乙方”、“权利”、“义务”、“合同”等词，而“A文化公司”、“B电影公司”分别是甲方和乙方，因此这两个词也有较大可能出现在合同中。

**本周题目**

**案情一：**某高速公路发生了一起严重的多车连环相撞交通事故，事故现场惨烈，多车辆已被撞毁，面目全非。现事故调查员要对肇事车辆（大型车辆）进行汽车电子数据取证，用于辅助判断该肇事车辆司机是否存在超速、疲劳驾驶等行为。

**根据以上案情，回答下列问题：**

**1、【单选题】以下哪些因素属于分析交通事故过程、认定事故事实、判定事故原因的重要因素？**

A.车速

B.驾驶行为

C.车辆状况

D.以上都是

**2、【多选题】一般情况下，在交通事故现场调查中可以对哪些线索进行搜集？**

A.ECU和TCU

B.驾驶司机的手机

C.周边监控视频

D.行车导航

**3、【单选题】对肇事车辆的行驶记录仪进行电子数据取证，获取到\_\_\_\_\_\_\_\_\_\_可以较为直观地判断肇事车辆司机是否存在疲劳驾驶的行为。**

A.行驶速度记录信息

B.位置记录信息

C.记录仪供电信息

D.超时驾驶信息

**4、【多选题】一般情况下，可以通过\_\_\_\_\_\_\_\_\_\_方法分析肇事车辆的行驶速度？**

A.现场轨迹测量

B.视频图像分析

C.现场目击

D.提取车辆行驶速度记录信息

**第一题：D**

解析：车速、驾驶行为、车辆状况是分析交通事故过程、认定事故事实、判定事故原因的重要因素。

**第二题：ABCD**

解析：通过对汽车ECU和TCU进行取证可以提取到故障号等信息，可以推断汽车驾驶行为，故A正确；对驾驶司机手机进行取证可能可以获取到汽车的位置等信息，故B正确；调取周边监控视频是常用的交通事故鉴定手段，故C正确；行车导航可以获取车辆的行驶记录，可能存在一些线索，故D正确。

**第三题：D**

解析：车辆超时驾驶信息记录司机的驾驶时长，通过对其进行取证可以用来判断司机是否存在疲劳驾驶行为。

**第四题：ABD**

解析：现场轨迹测量和视频图像分析是传统的分析车辆行驶速度的手段，提取车辆的行驶速度记录，也可以助于分析车辆行驶速度，故ABD正确；通过现场目击一般难以准确的判断车速，故C错误。

## 本周题目

**案情介绍：**

某单位网站被非法通过上传webshell获得了站点控制权限，修改了主站点的首页，并获得了网站数据库数据。 办案人员针对服务器进行了勘验，并将服务器中的相关数据进行了证据提取及固定。

**根据以上案情，回答下列问题：**

**1、[多选题]办案人员对被非法登录的服务器现场进行勘验，可以从以下哪几个方面入手？**

A、服务器web日志

B、服务器系统安全日志

C、单位网络入口防火墙

D、站点管理员

**2、[多选题]以下哪些信息能为证据提取及固定提供帮助？**

A、站点管理员创建过的帐号信息

B、服务器RAID阵列类型

C、服务器发现异常的时间

D、服务器放置的位置

**3、[多选题]通过对服务器证据镜像分析，可以发现以下哪些信息？**

A、服务器站点架构

B、连通该服务器的远程桌面IP地址

C、站点数据库类型

D、上传webshell的IP地址

**4、[多选题]分析该服务器镜像，主要想通过它找到以下哪些信息？**

A、是谁非法登录了该服务器

B、什么时候非法登录了该服务器

C、服务器权限如何被突破的

D、数据库通过什么方式被盗取的

**第一题：ABCD**

解析：办案人员可通过服务器中各类系统日志及web日志进行分析，前提条件是该服务器有开启以上日志的记录功能，单位网络入口防火墙日志信息也是检查的目标之一，同时，可以通过询问管理员，更直接获取相关线索。

**第二题：ABC**

解析：询问站点管理员创建过的帐号，可以对比哪些是异常出现的帐号，服务器RAID阵列类型、发现异常时间都可以为办案人员分析过程提供方向，服务器放置的位置与是否被非法登录没有关系，但服务器所在的网络拓补结构是排查的方式之一。

**第三题：ACD**

解析：由于该服务器是被非法通过上传webshell获得的站点控制权限，因此在web日志中很可能留下上传webshell的IP地址，也可以分析出服务器的站点架构和数据库类型，但获取站点操作权限不代表也不一定要获取远程桌面的权限，才能盗取数据库。

**第四题：ABCD**

解析：此类案例主要需要找出登录者，作案时间线，登录方式、登录目的、造成的后果等，通过这些方向，都有可能发现非法登录的蛛丝马迹，并最大限度还原登录过程。

## 本周题目

**案情介绍：**

某办案单位接到报警信息，xxx用户发现自己电脑中的办公文件全被加密了，并且受到索要财物的信息，现对受害人的计算机进行勘察，初步判定被恶意程序攻击。

**根据以上案情，回答下列问题：**

**1、[多选题]恶意程序可能存在的位置在哪？**

A、桌面

B、应用程序菜单

C、回收站中

D、C:\Windows\System32

**2、[多选题]可疑程序可能是如何实现自启动的？**

A、修改注册表

B、服务

C、计划任务

D、开机自启

**第一题：CD**

解析：通常恶意程序都会隐藏自身，所以a,b都不可能；恶意程序通常还有一个特征就是自删除，同样也是隐藏自身，所以选择cd

**第二题：ABC**

解析：恶意程序的启动方式通常为3种，就是ABC这三个，开机自启其实是依赖于abc这三个原理，这里问的是如何实现，所以选择abc

## 本周题目

**案情介绍：**

某涉密单位客户反映，在其内网中，有服务器疑似被黑客控制，发现夜间CPU资源占用率极高，疑似被写入了挖矿程序，办案人员针对服务器进行了勘验，并进行溯源分析。

**根据以上案情，回答下列问题：**

**1、[多选题]针对该类型案件，通常需要查找分析哪些方向？**

A、控制服务器的动机是什么，做了什么？

B、怎么控制服务器的，数据传输通道在哪？

C、通过什么方式突破网络安全防护机制？

D、谁实施了控制，控制的源头在哪？

**2、[多选题]以下哪些方法可以调查控制者的进入方式？**

A、查找系统日志及各类应用程序日志

B、通过仿真调查，进行抓包

C、通过netstat命令，查找异常IP及PID

D、通过启动的服务信息进行异常程序文件定位

**3、[多选题]通常在被控制的挖矿肉机中，会发现以下哪些信息？**

A、矿池地址

B、用户钱包地址

C、FTP服务器存储目录

D、挖矿服务器链接

**第一题：ABCD**

解析：该类型案件的调查原则与思路，通常可通过3W1H方式进行调查：即WHO，WHAT，WHEN，HAO，同时也需要了解其网络拓扑是怎么样的、需求是啥、发生了什么事、用户用了什么系统、系统版本多少、病毒库版本多少、多少主机中了、主机是普通PC还是服务器、服务器是做什么的等等。

**第二题：ABCD**

解析：调查控制者的进入方式，可通过静态分析和动态取证两种方式同时进行，静态分析通常指分析被控制机的系统日志及各类应用程序日志，过滤案发时段被删除的文件、查找各种异常访问情况等，而动态分析指通过被控制机系统运行后，进行网络抓包、系统进程与服务分析等方式，进行异常信息的发现与提取。

**第三题：ABD**

解析：因为是被控制的挖矿肉机，所以在肉机中通常可以找出矿池地址，用户钱包地址，挖矿服务器链接，端口转发工具等，但回传的信息不会以FTP服务器的形式收集。

**本周题目**

**案情介绍：**

某公司在某猫平台和某狗商城分别开设了某旗舰店和某保健品专营店，作为其进口系列食品的网络销售平台。为了更快打开市场，当事人以一年562000元的费用雇请上海某电商有限公司对其经营的两个网店中的系列进口产品进行了“刷单”及推广，用多次虚假的交易来提高网店内相关产品的销量显示，用一些虚假的评论诱导消费者误以为其产品质量很好。截止案发时，上海某电子商务有限公司对当事人所经营的两个网店中销售的37种系列进口产品共刷单4975笔。

**根据以上案情，回答问题：**

【多选题】“刷单”行为较为隐藏，如何取出此类行为的证据是办案难点。在本案的调查过程中，办案人员主要可以从哪些方面收集证据（ ）

A、检查当事人经营网店系列进口食品销售数据，并截图保存

B、对当事人的购进销售票据进行检查

C、审查当事人账目

D、前往刷单公司进行检查印证

## 上周答案

**答案：ABCD**

解析：选项A主要收集当事人所经营网店内系列进口食品的销量及评论显示数据；选项B如发现实际销售数据与显示的销售数据不符，借此挖掘出当事人“刷单”的违法行为；选项C可反映当事人是否雇请上海某电子商务有限公司对其所经营网店进行网络宣传推广并制造虚假交易量等；选项D可帮助形成证据链，证实当事人“刷单”制造虚假销售量及虚假评论的事实。

## 本周题目

**案情介绍：**

公安机关接群众举报：[http://www.xxxgirls.com](https://link.zhihu.com/?target=http%3A//www.xxxgirls.com)（情色天地）为一淫秽色情网站，这个网站上含有大量的淫秽电影和图片，而且还在网站上发展会员，谋取利润。经过大量线索排查，最终在犯罪嫌疑人的住所将其抓获，并当场收缴用于建设、维护网站的电脑一台，以及租用的云存储及云应用服务器组。

**根据以上案情，回答问题：**

**1、[多选题]对嫌疑人住所进行现场勘查时，需要获取以下哪些信息？**

A、远程控制云服务器组的权限

B、淫秽文件获取与上传通道

C、建设、维护该网站的操作情况

D、[http://www.xxxgirls.com](https://link.zhihu.com/?target=http%3A//www.xxxgirls.com)站点程序源代码

**2、[多选题]对云服务器数据的证据固定可以通过以下哪些方式进行？**

A、在适当时机冻结云服务器

B、通过远程电子数据固定的方法与流程进行证据固定

C、通过调证手续，对服务器中数据进行调证提取

D、通过黑客解析云服务器，提取固定证据

**3、[多选题]以下哪些信息，决定嫌疑人的量刑程度？**

A、上传淫秽电影和图片的数量

B、淫秽电影和图片是采用本地服务器还是云服务器进行存储

C、嫌疑人建设、维护网站的主观意愿

D、网站发展会员产生的收益

**第一题：ABCD**

解析：通过前期线索排查，发现该站点由嫌疑人维护，并租用了云存储及云应用服务器组，因此在现场勘查中，需要获取云服务器组的控制权限，同时，需要询问嫌疑人是通过哪些通道获取淫秽电影和图片并上传到服务器中的；因该嫌疑人是站点的建设与维护人员，所以在嫌疑人的电脑中，一般可以获取到该站点的源代码及建设、维护该网站的操作痕迹以及相关的日志信息等。

**第二题：ABC**

解析：该云服务器中电子数据的提取固定需要通过合法方式进行，如通过黑客解析等方式会失去证据效力，合法方式包括数据冻结、合法调证、远程固定获取等。

**第二题：ACD**

解析：淫秽文件的数量、嫌疑人传播的主观意愿、传播过程中产生的收益，都是该类型案件的量刑依据，但存储方式是证明淫秽文件存在的客观事实，决定的是案件性质，而非量刑程度。

## 本周题目

**案情介绍：**

黑客TANK想入侵某公司网络，窃取机密信息。为了提升效率，您认为他需要做的第一步工作会是（①）；第二步应该是（②）；在成功入侵该公司网络主机并取得主机的控制权后，他会做的工作是（③）；在获取到机密信息后，最后需要做的工作应该是（④）。

**请根据您的理解，以此将以下的选项，填入到案例中相应的空格：**

A、查找所需的攻击工具，并利用这些工具获得攻击目标的控制权

B、消灭踪迹，消除所有入侵脚印，以免被管理员发现

C、信息收集，通过扫描工具获取被攻击目标的IP地址，开放端口或安装软件版本等信息

D、继续渗透网络，直至获取机密数据

**第一题：CADB**

解析：本题主要考察黑客攻击的基本知识及流程，以通过此了解到入侵取证的整体思路。典型的黑客攻击的步骤如下：

1、信息收集（通过扫描工具获取被攻击目标的IP地址，开放端口或安装软件版本等信息）

2、根据收集到的相关信息，去查找对应的攻击工具；

3、利用查找到的攻击工具获得被攻击目标的控制权；

4、在被攻破的机器中安装后门程序，方便后续再次利用；

5、继续渗透网络，直至获取机密数据；

6、消灭踪迹，消除所有入侵脚印，以免被管理员发现。

## 本周题目

**案情介绍：**

公安机关在网上巡查过程中发现冒充教育部的一个网站，让一些假毕业证、假文凭、假证书用户交纳一定的费用，就可以在该网站注册认证。经过大量线索排查，最终将制作网站的犯罪嫌疑人在家中抓获，并当场收缴用于建设、维护网站和提供web服务的电脑一台。

**根据以上案情，回答问题：**

**1、[多选题]对嫌疑人住所进行现场勘查时，发现现场计算机处于关机状态，该如何处理？**

A、现场打开计算机电源，并拷贝取证工具到该计算机进行现场取证，第一时间获取关键证据

B、现场直接扣押封存该计算机

C、现场拆卸封存计算机硬盘，并详细记录该计算机及硬盘的品牌型号及唯一序列号等相关信息

D、现场计算机无需处理

**2、[多选题]以下哪些内容，可以证明嫌疑人通过该计算机建设、维护网站和提供web服务？**

A、与需要进行假证书认证的用户聊天沟通的即时通讯记录

B、计算机中布署的冒充教育部网站的整站系统信息

C、计算机中涉及新增的假证书的数据库记录

D、计算机中访问的日志记录

**第一题：C**

解析：拷贝取证工具到该计算机进行现场取证会破坏覆盖存储介质中大量的删除数据，不能这样操作；现场直接扣押封存该计算机表面上没有错，但没有记录计算机中存储硬盘的品牌型号及唯一序列号等相关信息，现场扣押封存记录不完善，对于现场是否应该对关机状态计算机进行开机，在详细记录了《电子数据现场提取笔录》且检材持有人和见证人签字的情况下，可以开机处理，如检材持有人和见证人无法签字或拒绝签字，可在全程录像的基础上，进行电子数据现场勘查及固定。

**第二题：ABCD**

解析：嫌疑人的即时通讯、邮件、计算机中的整站系统、数据库记录、访问日志等都属于证据信息。

## 本周题目

**案情介绍：**

近年来无人机成为电子消费行业的新宠，由此带来的意外事故或安全管控问题也越来越突出。近日，某大型活动现场，根据安保要求，现场工作人员查获一架正在禁飞区域上空飞行的无人机（D JI Phantom3），并找到了该无人机的操纵者，现在取证人员需要对现场查获的无人机、手机进行取证固定。

**根据以上案情，回答问题：**

**1、[多选题]无人机的数据源在哪儿？**

A、内置存储

B、外置存储卡

C、无人机的操作端APP

D、无人机服务商云端

**2、[多选题]如何确认无人机的飞行轨迹？**

A、无人机自带的飞行记录器里（Flight Data Recorder）

B、无人机手机端的APP-D JI GO

C、此款无人机飞行轨迹保存在以 “飞行日期”和“飞行时间”命名的TXT日志里，如“DJIGlightRecord\_2019-08-16\_[09-04-00].txt”

D、无人机飞行轨迹日志因为是TXT格式，所以可直接双击打开查看

## 上周答案

**第一题：ABCD**

**第二题：ABC**

解析：D不对，这个不是我们常见的TXT文本，它是经过编码的，需要进行格式转换才能看到里面的飞行记录数据；或者把飞行数据数据转换成KML或GPX格式文件，再使用Google Earth进行飞行记录数据查看。目前DC-4501可实现这类数据的直接解析查看，解析完成的数据包括飞行里程、飞行时间、高度、直线距离、水平速度、经纬度等飞行轨迹信息。

## 本周题目

**案情介绍：**

2019年3月初，某地网安部门接到某公司报案称，有人在该地利用计算机“外挂”从事某平台游戏“刷币”活动。经查，辛某等人使用“外挂”程序刷取腾讯公司某平台游戏金币出售而获利，累计涉案价值300余万元。

**根据以上案情，回答问题：**

**1、[多选题]可以采用以下哪些方法对“外挂”程序的功能进行分析？**

A、逆向分析代码

B、分析程序联网通信的行为内容

C、在测试环境中运行

D、使用动态分析工具进行分析

**2、[多选题]如何证实辛某使用“外挂”程序刷取了游戏金币？**

A、分析服务器日志，发现“金币”经济行为异常的账号

B、落地登录异常账号的地点

C、确认登录异常账号者的真实身份

D、发现使用“外挂”的痕迹

## 上周答案

**第一题：ABCD**

解析：程序功能分析包括了静态分析和动态分析，逆向分析属于静态分析，其他都属于动态分析。

**第二题：ABCD**

解析：要确认犯罪行为，要解决以下几个事件的关联性：

账号“金币行为异常”——辛某使用该账号——辛某使用外挂

## 本周题目

**案情介绍：**

某地市场监管部门接到群众举报，称某公司在网页上发布违法信息并在微信群及朋友圈内传播。但当执法部门收到举报时该链接已显示被微信官方屏蔽无法打开。

**根据以上案情，回答问题：**

**1、[多选题]当执法部门收到群众举报，正确的固证办法有哪些？**

A、直接使用经过司法认可的第三方存证工具进行网页存证

B、找到涉嫌违法单位后，到现场进行固证

C、在办案人员单位电脑上按照网络在线提取的流程对涉案网页截图固证

D、在办案人员手机上进行截图

**2、[多选题]因该链接已经被微信官方屏蔽，导致手机上无法访问，请问有哪些适合的固证方式？**

A、将网页地址在办案人员单位的浏览器上尝试打开看是否能访问；若访问成功，按照网络在线提取流程进行固证

B、发协查函到腾讯相关部门进行调证

C、寻求违法信息发布站点管理员协助

D、无法固证

## 上周答案

**第一题：AC**

解析：正确的固证方法应为第一时间直接使用第三方存证工具或者严格按照网络在线提取流程进行涉案网页截图固证，若等到违法单位内进行查证，有可能涉案单位已经将相关网页删除，这样对取证来说会增加很多难度。

**第二题：ABC**

解析：题干所示涉案网页有可能在微信公众号平台上发布也有可能在其他第三方服务器网站上发布然后通过微信公众号平台进行发布传播。因此该涉案网页有可能存在于两个位置，一是腾讯微信公众号平台，二是第三方网页平台。因此选项A是用来判断网页到底存放于什么位置，选项B是直接寻求腾讯协助，选项C是寻求第三方网页平台协助。

## 本周题目

**案情介绍：**

电话类电信网络诈骗通常是指嫌疑人利用电话、VOIP网络电话等远程语音通信方式联系目标人（被诈骗人），虚拟事实制造骗局，诱使目标人向嫌疑人使用的账户转账汇款的行为。此类案件案件虽然作案骗术种类繁多，但都是通过电话等远程语音沟通方式进行联系。在发案阶段应首先询问报案人的被骗账户信息，第一时间进行止付操作；其次围绕被骗人提供的信息及其使用的电子设备开展工作，梳理通信流、资金流。

**根据以上案情，回答问题：**

**1、[多选题]针对诈骗案的电子数据勘查取证，在发案阶段对通信流方面需要发现、固定以下哪些证据、线索？**

A、被骗事主与嫌疑人的通话记录、通话录音文件

B、嫌疑人使用的电话

C、被骗事主与嫌疑人的通话次数、通话时间、通话时长，时间精确到秒，以备查询信令使用

D、嫌疑人与被骗事主通过其他途径沟通产生的数据，如其他社交软件联系聊天记录、短信发送的信息、网址、二维码等

**2、[多选题]在发案阶段，获取资金流信息应包括以下方面？**

A、被骗事主银行卡（或第三方支付）账户、转账时间、转账地点、转账金额、转账方式

B、收款方的银行（或第三方支付）账户、开户人

C、开展调查收款方开户人名下的其他账户信息，拓展涉案银行卡资金流线索

D、其他与事主转账资金有关的信息，如网银转账IP，登录MAC地址信息等

\*注：我们将于下期公布本期问题的答案及解析，千万不要错过哟~

## 上周答案

**第一题：ABCD**

解析：以上全是在发案阶段对通信流方面需要发现、固定的证据、线索范畴。

**第二题：ABCD**

解析：以上全是在发案阶段对资金流方面需要发现、固定的证据、线索范畴。

## 本周题目

**案情介绍：**

某单位接到一个手机受检，初步勘验后发现没有直接分析到线索，进一步检查后发现有个文件保险箱的工具。

**根据以上案情，回答问题：**

**1、[多选题]使用文件保险箱通常可以做什么？**

A、加密图片

B、加密音视频

C、加密文件

D、加密微信聊天记录

**2、[多选题]目前没有掌握文件保险箱的密码（经测试该软件有密码次数验证），如何进一步获取？**

A、直接暴力破解

B、联网修改密码

C、逆向分析得知密码

D、询问送检人

## 上周答案

**第一题：ABC**

解析：微信聊天记录存储于Data下，此目录普通用户无法操作。

**第二题：BCD**

解析：

A选项有密码次数验证，尝试5次有软件锁定；

B选项如果可以点击忘记密码，可以通过短信验证修改密码；

C选项如果单机验证密码，可以逆向文件保险箱，破解密码；

D选项最简单的就是询问密码。

## 本周题目

**案情介绍：**

某省有人反映某单位招聘考试网站的学生成绩在网站被公开销售，于是公安机关派出调查人员对其调查取证，还原了整个攻击泄露过程。在这个过程中还发现了网站存在的安全漏洞，并于事后及时修复了漏洞，对网站进行了全面的安全检测，提高了网站的安全性。

**根据以上案情，回答问题：**

**1、[多选题]调查人员可以通过哪些方法来获取服务器的日志信息？**

A、从日志所在路径，直接提取日志文件数据

B、通过删除文件快速恢复，提取被直接删除的日志文件

C、通过签名恢复，恢复文件元数据已被破坏的日志文件

D、通过关键词搜索，恢复文件内容已被破坏的日志文件碎片

**2、[单选题]在日志文件提取的信息中，经常看到一些状态代码，下列说法不正确的是？**

A、200 表示访问成功

B、301 表示永久重定向

C、404 表示页面没有权限

D、500 表示内部服务器错误

## 上周答案

**第一题：ABCD**

解析：针对于服务器日志的提取，可以从类似于Windows操作系统恢复文件的方式：直接提取文件，快速恢复，签名恢复，关键词搜索等方法来提取日志信息。

**第二题：C**

解析：因为404是表示网页无法打开。所以选C

## 本周题目

**案情介绍：**

某日，某地公安机关接到群众报警称，某品牌手机经常无故弹出大屏广告，微信无故关注陌生公众号且手机频繁卡死、重启等，怀疑手机受到人为控制，请求公安机关调查。经初步调查后确认该案件系一起经典的非法控制案件。受害人手机在出厂前即被预先植入后门，待手机联网激活后，该后门程序立即通过网络连接中控服务器，下载安装用于非法弹送广告和非法控制用户微信的恶意程序对用户手机实施非法控制。

**根据以上案情，回答问题：**

**1、[多选题]本案中，嫌疑人以亚马逊AWS服务器为中控，推送恶意程序，控制大量手机非法弹送广告和关注微信公众号，对于本案中以下哪些是案件调查的关键？**

A、找到数据库服务器

B、固定恶意程序

C、固定非法广告资源

D、摸清服务器架构

**2、[多选题]本案中，大量的关键数据如接口服务器备份日志、恶意程序、非法广告资源等均存放于AWS的S3存储桶进行分布式存储，对于此类存储的数据取证有哪些难点？**

A、无法通过调证形式进行调取

B、文件不能批量下载

C、进行网络在线提取费时费力

D、无法对文件夹进行下载

https://www.zhihu.com/column/c\_1155491953624780800