**电子数据取证试题**

说明：考试时间100分钟，满分100分，答案写在答题纸上。

1. **单选题（共10题，每题2分，共计20分）**
2. 硬盘作为最常见的计算机存储介质，近几年从容量到性能都有了很大的提高，以下哪种硬盘的理论传输速率最慢？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. SCSI | 1. IDE | 1. SAS | 1. SATA |

1. 以下哪种规格是市场上最常见的笔记本硬盘？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. 3.5英寸 | 1. 1.8英寸 | 1. 2.5英寸 | 1. 1英寸 |

1. 以下哪种规格不是SCSI硬盘的针脚数？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. 50 | 1. 68 | 1. 72 | 1. 80 |

1. 下列哪种接口的存储设备是不支持热插拔的？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. USB接口 | 1. E-SATA接口 | 1. SATA接口 | 1. IDE接口 |

1. 下列哪个选项是无法计算哈希值的？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. 硬盘 | 1. 分区 | 1. 文件 | 1. 文件夹 |

1. 下列文件系统中，哪个是Windows 7系统不支持的？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. exFat | 1. NTFS | 1. HFS | 1. FAT32 |

1. 下列有关文件的各类时间属性，操作系统是一定不记录的？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. 创建时间 | 1. 修改时间 | 1. 访问时间 | 1. 删除时间 |

1. 下列哪种不是常见的司法取证中的硬盘镜像格式？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Gho | 1. AFF | 1. S01 | 1. 001 |

1. 系统日志中某些内容可能对取证有重要意义，比如“事件日志服务启动”通常被视为计算机开机的标志，该事件所对应的事件编号为：

|  |  |  |  |
| --- | --- | --- | --- |
| 1. 5005 | 1. 5006 | 1. 6005 | 1. 6006 |

1. Encase Forensic是业界文明的司法取证软件，它是下面哪家公司开发的？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Guidance | 1. GetData | 1. AccessData | 1. PanSafe |

1. **多选题（共10题，每题3分，共计30分）**
2. 通常Windows系统中涉及文件的3个时间属性，M代表Modify，表示最后修改时间；A代表Access，表示最后访问时间；C代表Create，表示创建时间；下列解释错误的是？
3. M始终要晚于C
4. M、A、C在Linux系统中也适用
5. M、A、C时间是不能被任何工具修改的，因此是可信的
6. 文件的M、A、C时间一旦发生变化，文件的哈希值随之改变
7. 下列关于对位复制的说法中，不正确的是？
8. 为了确保目标盘与源盘的一致性，一定要找到与源盘品牌、型号、容量均一致的目标盘进行复制
9. 为了确保司法取证的有效性，一定要验证目标盘与源盘哈希值的一致性
10. 为了确保目标盘与源盘的一致性，目标盘的硬盘接口一定要与源盘一致
11. 当目标盘容量大于源盘时，一定要计算目标盘整盘的哈希值，用于与源盘的哈希值进行比对一致性
12. 下列关于现场勘验过操作的说法中，不正确的是？
13. DD文件是最常用的镜像格式，因为该格式是原始镜像，而且支持高压缩。
14. 为了固定运行着的计算机的桌面状态，首先应该按键盘的PrtSc键进行截图。
15. 对于关机状态下的计算机进行固定时，优先采取对硬盘盘体进行开盘操作的方式。
16. 对于关机状态下又无法拆卸硬盘的计算机，应该开机直接查看系统里的数据。
17. 下列文件系统中，哪些是Windows的文件系统？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. HFS/HFS+ | 1. EXT2/3/4 | 1. NTFS | 1. FAT16/32 |

1. 下列关于对位复制和创建镜像的说法中，错误的是？
2. 一般情况下，对位复制时，目标盘容量要等于源盘容量
3. 制作DD镜像时，能够将500G源盘的完整DD镜像生成到500G的目标盘中
4. 一般情况下，源盘生成的E01镜像，占用的空间小于同一块盘生成的DD镜像
5. 用专门的镜像哈希计算工具，计算的同一块硬盘的DD和E01镜像哈希值是相同的
6. 当一块硬盘被连接到计算机上时，Windows系统已经为其分配盘符，但双击该盘符提示是否需要格式化磁盘，可能存在的原因是？
7. 该分区格式为EXT4，Windows系统无法识别
8. 该分区已损坏，Windows无法识别
9. 该硬盘是一块从未使用过的全新的硬盘
10. 该分区被病毒感染，导致分区表丢失
11. 下面关于文件头的说法中，不正确的是？
12. 各种类型文件的文件头长度不一定相同
13. JPG格式文件的文件头存在细小差异
14. 相比文件头，文件扩展名更可信，因此文件扩展名常用于判断文件类型
15. 在Windows系统中，修改文件扩展名的同时，该文件的文件头也随之变化
16. 下列哪些类型是Windows7系统中常见的日志类型？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Application | 1. Security | 1. System | 1. Local |

1. 手机中常用的简体中文编码格式不包括？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Big5 | 1. UTF-16 | 1. Unicode BE | 1. UTF-7 |

1. 下面哪些密码破解方法可以用于RAR文件？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. 彩虹表破解 | 1. 暴力破解 | 1. 掩码破解 | 1. 字典破解 |

1. **不定项选择题（共10题，每题3分，共计30分）**
2. 下列不是NTFS分区下的元文件的是？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. $MFT | 1. $Boot | 1. $FAT | 1. $Secure |

1. 下列属于Windows 7系统中虚拟内存对应的文件是？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. hiberfil.sys | 1. pagefile.sys | 1. virtualmem.sys | 1. config.sys |

1. 下列关于文件大小和文件占用空间大小的说法中，不正确的是？
2. 文件大小和文件占用空间大小总是不一致的
3. 文件占用空间大小总是大于文件的实际大小
4. 文件大小总是文件占用扇区大小的整数倍
5. 文件占用空间大小与文件实际大小之间的差额通常被称为文件松弛区（Slack）
6. 下面哪些操作系统不属于智能手机操作系统？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Linux | 1. Windows 8 | 1. Mac OS | 1. MTK |

1. 下面哪些文件不是Windows的注册表文件？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. Regedit | 1. Sam | 1. System | 1. Security |

1. 下面哪种类型的数据不属于易失性数据？

|  |  |  |  |
| --- | --- | --- | --- |
| 1. 内存 | 1. 未分配簇 | 1. 运行的服务 | 1. 未打开的图片 |

1. 下列关于安卓手机取证说法错误的是？
2. 安卓手机大部分的关键数据都记录在data区内
3. Data区无法随意访问，需要最高用户权限的授权（root权限）
4. 通过解析备份文件也可以完成对data区的取证
5. 通过一些第三方软件，可以将QQ、微信等主流社交软件的聊天记录储存位置指定在SD卡
6. 下列关于制作硬盘复制件的说法中，不正确的是？
7. 降低直接在源盘检验带来的源盘损坏的风险。
8. 防止误操作等原因造成的硬盘数据篡改。
9. 对于某些传输速率低的硬盘，复制件采用高速率硬盘能有效提高后续取证效率。
10. 制作复制件的同时，能够修复部分物理损坏的源盘。
11. 下列文件后缀名的说法中，不正确的是？
12. 文件的后缀名显示与否是Windows系统中可以设置的。
13. 文件的后缀名一般来说为3-4个位长度。
14. 可以通过改变文件的后缀名修改文件的类型。
15. 所有文件都有文件后缀名。
16. 下列关于iPhone取证说法错误的是？
17. iPhone数据恢复一定要越狱
18. iPhone的DFU模式通常用于刷机和越狱
19. iPhone4的4位屏幕密码可以破解
20. iPhone只有越狱了才能进行密码破解
21. **判断题（共10题，每题1分，共计10分）**
22. 手机取证时一般将手机调成飞信模式再进行取证。
23. 计算机仿真取证技术可以很大程度上弥补传统静态取证证据获取能力的不足。
24. 手机的备份文件中不会记录IMEI号。
25. 开机状态下Windows的用户密码信息是以明文形式保存在注册表中的。
26. 安卓手机都可以通过备份进行获取。
27. 现场勘验时可以通过PE工具直接清除windows密码后进行开机取证。
28. 对手机取证时应保证待检测手机的数据、信号畅通，以便及时接受到最新的证据。
29. iPhone手机微信中获取的语音文件属于证据形式中的声像资料，而不是电子数据。
30. 在进行硬盘克隆（对位复制）前必须对目标盘进行擦除。
31. Aff与E01格式支持镜像压缩，可根据实际需求选择压缩比，减少文件占用的空间与镜像制作的时间。
32. **简答题（共2题，每题5分，共计10分）**
33. 简述硬盘克隆（对位复制）与镜像的异同。
34. 简述有屏幕密码的安卓手机应该如何取证。