**1、说明在Python中常用的注释方式包括哪些？**

答：①单行注释：行首# ②多行注释：三个单引号或三个双引号包括要注释的内容

③编码注释：#coding=utf-8或#coding=gbk ④平台注释：#！usr/bin/python **2、说明在Python中单引号、双引号和三引号之间的区别。**

答：①单引号和双引号通常用于单行字符串的表示，也可通过使用\n换行后表示多行字符串 ②三单引号和三双引号通常用于表示多行字符串以及多行注释，表示多行时无需使用任何多余字符。 ③使用单引号表示的字符串中可以直接使用双引号而不必进行转义，使用双引号表示的字符同理；三引号中可直接使用单引号和双引号而无需使用反斜杠转转义，三引号表示的字符串中可以输出#后面的内容。 **3、说明在Python中的代码a,b=b,a实现了什么功能。** 答**：**a,b数值互换 **4、Python提供了哪两种基本的循环结构。**  答：For，while **5、Python中的常用可迭代对象包括哪些？**

答：①序列，包括列表、元组、字典、集合及range

②迭代器对象 ③生成器对象 ④文件对象 **6、Python2.7的标准库hashlib中包含的hash算法包括哪些？**

答：MD5，SHA1，SHA256，SHA512。 **？7、在Python编程中，常见的结构化输出文件格式包括哪些。** 答：Csv,xml,html,json **8、在Python编程中，变量名区分英文字母的大小写，基于值的内存管理方式，使用缩进来体现代码之间的逻辑关系。（√）  
9、Python中的lambda函数也就是指匿名函数，通常是在需要一个函数，但是又不想去命名一个函数的场合下使用。（√）  
10、在Python中如果需要处理文件路径，可以使用（ OS ）模块中的对象和方法。  
11、在Python中的字符串和元组属于不可变序列，列表、字典、集合属于可变序列。（√）  
12、在Python中集合数据类型的所有元素不允许重复。（√）  
13、在Python中如何创建只包含一个元素的元组？** 答：tuple1=(a, ) **14、在Python中字典数据类型的“值”允许重复，“键”不可以重复。（√）  
15、说明Python用什么方法操作Excel文件。**

答：依靠第三方模块库xlrd、xlwt、xlutils和pyExcelerator等。

Xlrd主要用于读取Excel文件，xlwt主要用来写Excel文件，xlutils结合xlrd可以达到修改Excel文件的目的，openpyxl可以对Excel文件进行读写操作。 **16、说明Python中的异常处理机制except的用法。**

答：①except：#捕获所有异常

except：<异常名>：#捕获指定异常

except：<异常名1，异常名2）：#捕获异常1或异常2

except：<异常名>，<数据>：#捕获指定异常及其附加的数据

except：<异常名1，异常名2>：<数据>：#捕获异常名1或异常名2及附加的数据库

②一般使用try：……except：……进行异常处理，try子句中的代码块放置可能出现异常的语句，except子句中的代码块处理异常。

Try：

try块 #被监控的语句

except Exception[as reason]：

except块 #处理异常的语句

③try：……except：……else结构 ④try：……except：……finally结构

⑤try：……except：……except：……else：……finally……结构 **17、在Python中一切都是对象，Python3.x的汉字编码默认使用UTF-8。在Python中使用对象不需要提前声明。内置函数help()，dir()的作用。**

答：①help（obj）返回对象obj的帮助信息（查看函数或模块用途的详细说明）

②dir（obj）返回指定对象或模块obj的成员列表，如果不带参数则返回当前作用域内所有标识符（获取当前模块的属性列表）。 **18、常见的U盘文件系统类型包括哪些？** 答：FAT32、FAT16、exFat、NTFS **19、常见的证据镜像文件格式有哪些？** 答：E01、aff、dd、vmdk、gho **20、在取证中单向哈希函数的主要用途包括哪些。**

答：证据保全、搜索、黑名单、白名单、变化检测。 **21、常见的硬盘接口类型有哪些。** 答：IDE、SCSI、SATA、SAS。 **22、硬盘在存储数据之前，一般需经过低级格式化，分区和高级格式化这三个步骤之后才能使用，其作用是在物理硬盘上建立一定的数据逻辑结构。（√）  
23、传统硬盘由很多盘片组成，每个盘片被划分为若干个同心圆，称为柱面。（√）  
24、Rainbow是什么，有何用处？**

答：彩虹表，用于加密散列函数逆运算的预先计算好的表，为破解密码的散列值而准备（用于破解哈希函数，哈希值和消息对应）。 **25、UTC是什么时间？时间分析中纪元是什么？不同操作系统中纪元的值是什么？**

答：协调统一时间（协调世界时），在全球大部分国家作为官方时间源的基础。一个纪元被定义为一个显著的事件，标志着一段时期的开始。

大多数系统的纪元开始于1970年1月1日。 UNIX系统：1970年1月1日0时

Windows系统：1601年1月1日0时 Macintosh系统：1904年1月1日0时 **26、如何调查计算机打印了哪些文件？**

答：通过后台打印文件分析来证明使用者试图打印了哪些数据，调查打印历史记录。①文件恢复（.SPL,.SHD）恢复方式为签名恢复、关键字恢复等 ②获取打印内容：使用自动化的软件或Encase手工恢复。

**27、调查Prefetch的方法是什么，取证意义在哪里？  
28、写出调查以62开头的19位银行卡号的GREP表达式，写出搜索.SPL文件中的EMF头的GREP表达式** 答：①[^#]62##[- ,]####[- ,] ####[- ,] ####[- ,]###[^#] ②\x01.{40,40}EMF

**29、Windows 7系统的注册表文件在什么路径？分别是哪几个文件？如何调查操作系统的网络连接使用过的IP地址。**

答：\User\用户名，Default、SAM、Security、Software、System

调查IP地址:用Encase添加证据文件，找到与网络适配器有关的文件HKLM\System\CurrentControlset\Services\TCPip\Parameters\Interfaces\GUID  
**30、在Windows 系统中带有SPL，SHD扩展名的文件是什么文件？**

答:后台打印文件，是在打印机打印页面时用于在硬盘上存储打印文稿的临时文件。  
**31、有哪三种类型的预读取文件？**

答：引导轨迹预读取文件、应用程序预读取文件、宿主应用程序预读取文件。  
**32、Unicode编码范围在0000—007F之间的字符，编码成为UTF-8后为1字节，  
Unicode编码范围在0080—07FF之间的字符，编码成为UTF-8后为2字节，  
Unicode编码范围在0800—FFFF之间的字符，编码成为UTF-8后为3字节，**

**33、什么是Base64编码？**

答：按照RFC2045的定义，Base64被定义为：Base64内容传送编码被设计用来把任意序列的8位字节描述为一种不易被人直接识别的形式。它是将要传送的信息转化为64个ASCII字符（"A”-“Z”,”a”-“z”,”0”-“9”,”+”,”/”）组成的字符串的编码方式。

它的原理是将字符流顺序放入一个24位的缓冲区，先来的占高位，缺字符的地方补0，然后将缓冲区截断成为4个部分，每次取出6位，按照其值选择中的字符作为编码后的输出，直到全部输入数据均完成转换，即为Base64编码。

**34、什么是大端（big endian）和小端（Little endian）？** 答：大端和小端是字节的顺序，对多字节编码，在传输和处理过程中先处理高字节的叫大端，反之叫小端。  
**35、TXT文件头的EFBBBF，FFFE，FEFF各代表什么字符编码？**

答：EFBBBF：UTF-8 FFFE：UTF-16，Little-endian FEFF：UTF-16，Big-endian  
**36、解释GB2312。**

答：GB2312是国家标准总局发布的信息交换用汉字编码字符集，是一种汉字编码方案。它表示约7445个简体汉字，使用2个连续的字节表示一个汉字。为与ASCII码区分，规定这2个字节的最高位为1，高字节从A1到F7，低字节从A1到FE，保持与ASCII码的兼容。

**※37、什么是文件签名？文件签名有什么作用？Encase的文件签名验证有哪四种结果？**

答：文件签名是文件头的一段十六进制数据，能标志一个文件的真实文件类型。

①match:扩展名与文件签名所指类型一致

②直接给出文件类型:扩展名已知，文件签名是其他文件扩展的值

③Unknow:文件签名库中未收录 ④Bad signature:文件头和文件扩展名不匹配

**APP作业**

一、**综合作业**

※1. 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；下列哪个解释是正确的？ （ **在FAT32格式的分区中，A中仅包含日期，不包含时间 ）。**

※2.Windows7系统不支持的文件系统（ **HFS** ）。 ※3.MacOS的文件系统是（ **HFS/HFS+** ）。

※**4. 文件后缀名的说法中，不正确的是（可以通过改变文件的后缀名修改文件的类型）。**

※5. NTFS文件系统具有的功能（**支持长文件名、压缩文件和目录、支持超过4GB的大文件** ）。

6. 在Windows XP操作系统中，扩展名为.url的文件可以引导浏览器访问指定的网站，它通常位于的文件夹是（ ）文件夹 。

7. IE浏览器的Temporary Internet Files 文件夹包含的信息有（ **访问过的Web页面文件（在随后的加速可能会利用到）、Web邮件残留物、作用类似于数据库，用于管理缓存文件的index.dat文件** ）。

8. 电子邮箱的（ **注册资料、邮件内容、容量大小、登录记录** ）都保存在邮件服务器中。

9.使用IE访问网站，网站能够获得访问者端的一系列信息，包括（ ）。

10.文件系统需记录（ ）。

11.文件属性包括（ **创建时间、访问时间、修改时间，物理大小，文件名称，所在物理位置** ）。

12.Windows事件日志中，常见的日志类型有（ **系统日志、应用程序日志、安全日志** ）。

**16. 在默认设置的Windows XP系统中，将一个.TXT文件从移动硬盘（NTFS文件系统）复制到系统的C盘（NTFS文件系统）的桌面文件夹，并修改了此文件的文件名、扩展名。请问此文件的三个时间属性，以及哈希值，哪些会改变，如何改变？**

**18.什么是E01文件？**

**答：**Encase使用的默认证据（镜像文件）文件格式（的后缀）。

**19.什么是Windows操作系统注册表？**

答：操作系统注册表记录了用户安装在计算机上的软件和每个程序的相互关联信息，它包括了计算机的硬件配置，包括自动配置的设备和已有的各种设备的说明、状态属性以及各种状态信息和数据。通过它可以控制硬件、软件、用户环境和操作系统界面的数据信息文件。

**20.什么是Unicode编码？**

**二、复习备考题-单选**

1.常见的司法取证中的硬盘镜像格式有（ **Gho、AFF、E01** ）。

**2.下列关于对位复制和创建镜像的说法中，哪个是错误的？（ D ）**

A.一般情况下，对位复制时，目标盘容量要求大于等于源盘容量

B.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

C.一般情况下，源盘生成压缩的E01镜像，占用的空间小于同一块盘生成的DD镜像

**D.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**

※3. 在Windows 7操作系统中，注册表文件NTUser.dat通常保存（ **\User\用户名** ）中。

4. 当正常关闭一台计算机后，通常情况下（ **内存中存放的数据、运行的进程、当前的网络链接、当前的登录用户** ）会丢失。

※5.（ **IDE接口** ）存储设备不支持热插拔。 6.（ **文件夹** ）无法计算哈希值。

？7.理论传输速度最快的存储设备接口是（ USB3.0 ）。 SATA3.0

8.常见的Linux操作系统（ **CentOS、红旗、Ubuntu** ）。

**9. 下列关于EFS加密的说法中，不正确的是？（ EFS加密后的文件必须输入密码才能打开 ）。**

10.常见的虚拟机软件（ **VMware、Virtual PC、VirtualBox** ）。

11.用户的活动信息有（ **USB使用记录、最近打开的文件、最近运行的程序** ）。

12.易失性数据有（ **内存数据、当前系统进程、运行的服务** ）。

**13. 关于制作硬盘复制件的原因中，（制作复制件的同时，不能够修复部分物理损坏的源盘）。**

14.智能手机操作系统有（ **Android、Windows Mobile、iOS** ）。

15.关键词搜索时的繁体字编码方案是（ **Big5** ）。

16．下列关于文件大小和文件占用空间大小的说法中，正确的是（**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 ）。**

17．Windows7系统虚拟内存对应的文件是（ **pagefile.sys** ）。

18. .pst文件是（ **Outlook** ）邮件客户端的本地文件夹。

**19. 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，不可能存在的原因是？（该硬盘是一块从未使用过的全新的硬盘）。20. 下面关于文件哈希值的说法，哪种是错误的?（ D ）**

A.两个内容完全一样的文件，其哈希值相同

B.哈希值具有单向不可逆性，不能通过修改哈希值还原文件的内容

C.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

**D.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**

21. Encase Forensic是业界文明的司法取证软件，它是（ **Guidance Software** ）公司开发的。

22. 操作系统的用户使用痕迹（artifacts）可以定义为（ **与特定用户使用偏好有关的信息、关于计算机通用设置的信息、计算机上存储的用户活动的信息、用来简化用户操作体验的信息**  ）。

23. 当在EnCase中创建一个新的案例时，案例选项对话框提示用户输入的信息包括（ **案件的名字、查员的名字、缺省的输出文件保存路径、缺省的临时文件保存路径** ）。

24. NTFS分区下的元文件有（ **$MFT、$Boot、$Secure ）**。

25.适用于RAR文件的密码破解方法有（ **暴力破解、掩码破解、字典破解** ）。

三、复习备考题-综合

1.ASCII中非打印字符“07”代表（ **响铃** ）。

**2. 下列关于文件头说法错误的是（ C ）**

A．文件头位于一个文件开始的部分。 B．文件头是一般是一串十进制字符。

**C．文件头的内容决定了操作系统能否识别该文件并用相应的程序打开或运行该文件。**

D．文件头数据如果被改动过，即使文件的扩展名不变，也很可能导致文件无法打开。

3. 嫌疑人将多个JPEG图片的文件的扩展名改为其他名称，需要通过( **文件签名分析** )才能找到这些文件 。

**4. 以下关于文件删除的说法中，不正确的是：（ C ）**

A文件目录项的首字节改变为十六进制值E5 B文件数据所占的簇被更新为未分配状态

**C文件数据被填充为00h。** D文件的数据仍然保留在原位置。

5.常见的文件系统格式有（ **FAT32、NTFS、HFS** ）。

6.硬盘数据存储和磁盘管理的最基本单元是（ **扇区** ）。

**7. 以下关于硬盘的逻辑结构说法不正确的是（ C ）**

A每个盘片有两个面，这两个面都是用来存储数据的

B随着读写磁头沿着盘片半径方向上下移动，每个盘片被划分成若干个同心圆磁道

**C磁道被划分成若干个段，每个段称为一个扇区。扇区的编号是按0,1，„„顺序进行的**

D硬盘柱面、磁道、扇区的划分表面上是看不到任何物理痕迹的

8. 关于关键词搜索，（ **通过正则表达可以实现关键词模糊匹配和批量搜索** ）。

9. 磁盘在格式化时被划分成许多同心圆，这些同心圆轨迹就叫做（ **磁道** ）。

**10. 下列有关硬盘镜像文件制作说法不正确的是（ D ）。**

A.取证过程中常用的硬盘镜像文件格式包括.DD/.AFF/.E01/.img/.vmdk/.gho等格式。

B. 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。 C.制作镜像的过程中一定要计算哈希值，用以确保和追溯嫌疑盘及其镜像文件中数据的原始性 **D.同一块硬盘制作出的任何格式镜像文件的哈希值一定是相同的。**

**11. 关于硬盘复制，错误的是 ( B )。**

A硬盘复制过程中不应该改变源盘中的数据 **B硬盘复制过程中要先对源盘进行格式化**

C硬盘复制前先接入硬盘再打开电源开关 D硬盘复制机不需要再接外接只读锁

**12. 金山WPS 2010版本以及Microsoft Office 系列办公软件中的默认字符编码格式是**（ **Unicode** ）。 **13.常见的硬盘接口类型有（ IDE、SATA、SCSI、SAS** ）。

14．在windows操作系统中，打开本地注册表的命令是regedit和（ **regedt32** ）。

15. 一台计算机主机采用静态地址IP接入网络后，其IP地址通常记录在（ **注册表** ）中，MAC地址通常记录在（ **网卡** ）中，在系统运行时读入内存。

16. 磁盘上数据能够读写的最小单位是（ **扇区** ），文件读写（或分配）的最小单位是（ **簇** ）。

17.NTFS文件系统默认簇的大小为8K字节。（×）

18. 中文版本的Office软件以GB-2312编码保存文件内容。（×）

19. 在Windows中，命令dxdiag可以检查网络IP地址。（×）

20. exFAT 是一种磁盘接口标准。（×） **21. EFS只能在NTFS卷上使用。（√）**

22.当设置好时间同步服务器后，计算机系统的时间就与（**计算机所设定时区**）同步。**23.Windows系统的链接文件（或快捷方式）文件后缀是什么？对其分析的取证意义是什么？**

答：.lnk，对其取证可以找出最近的操作行为，每一个lnk文件都有自己的创建、修改和访问时间，可对这些时间进行分析。

**24.请写出Encase中用来搜索中国电信公司手机号的GREP表达式。**

答：[^#]?1[358]#########[^#]

**25.列举四种常见的操作系统。**  答：Windows、Linux、MacOS、Unix

**26.列举三种智能手机用到的操作系统。**  答：Android、Windows Mobile、iOS

**27.什么是硬盘只读锁？** 答：硬盘只读锁是一种使接入的硬盘只能处于读状态的设备，用于在电子取证中保护原盘数据不被错误操作删改。

**28.什么是文件系统（File system）？**

答：文件系统是操作系统用于明确存储设备或分区上的文件的方法和数据结构，即在存储设备上组织文件的方法。

**四、编程**

**1.编写Python程序，生成包含1000个0-100之间的随机整数，然后统计每个元素出现的次数。**

import random  
a\_list =[]  
for i in range(1,1001,1):  
   b = random.random()  
   b = b\*10000//100  
   a\_list.append(b)  
a\_zidian = {}  
print(a)  
for j in range(1,101,1):  
   c = int(a\_list[j])  
   if (c in a\_zidian):  
       a\_zidian[c] = a\_zidian[c]+1  
   else:

       a\_zidian[c] = 1  
print(a\_zidian)

**2.编写一段程序，要求用户输入1个列表，2个整数。然后以整数作为下标，输出列表中介于2个下标之间的元素构成的子列表。例如输入的列表是[1,2,3,4,5,6,7,8,9]，整数是2，5。那么输出是[3,4,5,6]**

ist1 = input("请输入一个列表：")

list1 = eval(list1)

start,end = eval(input("请输入两个数："))

print(list1[start:end])