计算机取证习题

Q: 计算机中的质量保障（ Quality Assurance ）主要涉及哪些内容？

A: 质量保障指一个包含很多规则的文件方面很完备的系统， 用以确保分析结果的准确性和可靠性， 包括：

同行评审报告、证据的处理、案件文书以及实验室人员的培训

Q: 在计算机取证中选择取证工具时需要注意些什么？

A: 要根据 NIST 和 NIJ 的标准，在使用前要进行验证，在更新好也要进行验证。

Q:Linux 文件系统结构中的数据位图（ Data Bitmap ）的用途是什么？试结合示例 加以说明

A: 数据位图的每一位对应着一个数据块，用 0 或者 1 表示该数据块是否空闲。如 1010 表示第一个数据块和第三个数据块不是空闲的，第二个和第四个是空闲的。

Q:ls 是 Linux 系统中常用命令，利用该命令是否能够判断一个指定目录上是否挂载有文件系统？为什么？

A: 使用 ls 命令可以查知该目录根结点 i 结点编号

Q: 什么是监管链？它由谁构建？

A: 监管链即连续的证据，是按时间顺序排列的文件或书面记录，显示仙子证据的捕获、保管、控制、传输、分析和处理托信息。由取证人员构建

Q: 专家证人和非专家证人的主要区别是什么？什么样的人能充当专家证人？

A: 专家和增人可以给出他们自己的观点， 在法律意义上能够帮助法官或者陪审团理解说明他们不熟悉的证据的人就可以充当专家证人。

Q:Segal ’ Law 揭示数字取证中的什么问题？如何面对该类问题？

A:Segal ’ Law 是说一个人有一块表就可以判断时间， 如果有两块时间不同的表就无法确定哪个时间是对的。面对该类问题，规定一个标准时间

Q: 何为数字取证中的克隆操作？为何需要克隆操作？如何进行？

A: 数字取证中的克隆操作是对硬盘的数据进行逐比特拷贝。

原因： 1.数字证据是非常不稳定的，对证据的研究、检查不能在原始证据上进行

2.硬盘有可能会崩溃，因此要多克隆以作为后备

3.一旦误操作有机会重新开始

方法：需要一个取证意义上干净的硬盘；从原电脑中移出原硬盘；将原硬盘和克隆设备或其他电脑连接；应用取证镜像工具来克隆

Q: 通常很多已被删除的信息依然可以由 Mactime 工具展示出来，这样查到的已删除文件和未删除文件有什么不同？如何定位已删除文件在文件系统中所处的文件位置？

A: 已删除的文件不再有路径名，只能显示其 i 结点编号。可以根据该文件的 i 结点编号查找文件系统中与之相邻或相近的 i 结点编号，因为文件创建时 i 结点的编号是按次序排列的，因此该文件的目录位置极有可能和 i 结点编号与之最接近的文件相同。

Q:Linux 的 ext3/4 的文件自通日志保存在一个文件中，该文件有大量时间信息，但该文件不会出现在目录列表中，如何访问该文件以便从中获取时间信息？

A: 因为不在目录中显示，所以不能通过名字找到，可以通过 tune2fs 明星显示日志文件的保存位置， i 节点编号等信息，然后通过在这些信息去找到它

Q: 如果数字取证中嫌疑人经常使用浏览器访问互联网，那么以互联网行为为主线，可以从哪些方面获取相关证据信息，这些信息又能证明什么？

A：1.cookies，cookies一般保存在 index。Dat 里面，包括 URL 信息访问日期时间，用户名等信息

2.临时文件（网页缓存），会显示如“最近一次访问的时间”在 TIF 中

3.历史记录，分成按日期、星期、月份，在 index.dat显示访问的 URL 和时间

4.注册表， ntuser.dat文件中，有近期访问的 URL，键的名称按时间顺序排列。

一、 填空题（每空 1 分，共 32 分）

1、计算机证据的来源有（ ）、（ ）、（ ）

2、存储设备与服务器的连接方式通常有（ ）、（ ）、（ ）

3、向一块硬盘写入数据之前 ,首先需要将其分区和格式化 ,这个过程一般可以分为（ ）、（ ）、（ ）三个步骤，安装文件系统是其中的（ ）

4、硬盘分区可以分为（ ）（ ）、（ ），分区操作所做的事情是对（ ）进行修改。

5、操作系统启动扇区位于（ ），它包括（ ）和（ ）

6、NTFS 将其数据一般存放在（ ）

7、对称加密技术的典型算法为（ ），非对称加密技术的典型算法为（ ）

8、信息隐藏技术主要分为（ ）和（ ）

9、（ ）与（ ）是电子签名法要解决的首要问题。

10、（ ）是计算机取证的核心和关键

11、（ ）功能十分强大，能够对 FAT 和 NTFS 分区中的文件删除、格式化分区进行数据恢复，也能够对没有文件系统结构信息即 FAT 表和目录区被破坏后的数据进行恢复。

12、为了确保取证工具输出的完整性， 当电子文件被转移或传输的过程中计算 （ ）是十分必要的。

13、Windows 操作系统维护三个相互独立的日志文件（ ）（ ）（ ）

14、在计算机上维护有关应用程序， 安全性系统事件的日志， 可以使用 （ ）查看并管理事件日志。

15、自从 WIN95 操作系统开始（ ）就成为了 Windows 及其所支持的应用程序的中心配置数据库。

二 选择题（每空 2 分，共 20 分）

1、WinXP 主要的文件系统是（ ）

A.FAT-16 B.NTFS C.FAT32 D.FAT-12

2、当关闭计算机时，主要丢失的是什么信息？

A. RAM 中的数据 B. 正在运行的进程

C. 当前的网络连接 D. 全选

3、FAT 表的定义是

A 包括主引导记录区和逻辑分区

B 正在运行的系统在分区上读取并定位数据的时候产生

C 包括文件名和文件属性的表

D 由文件名、被删除的文件的名字以及文件的属性构成的表

4、以下哪一项是关于分区表的描述

A 位于 0 柱面， 0 磁道， 1 扇区

B 位于主引导记录区

C 用于追踪硬盘驱动器上的分区

D 以上所有的

5、哪个选项 FAT 文件系统中分割文件的路径？

A FAT 表

B 目录结构

C 卷引导记录区

D 主控文件表
6、NTFS 文件系统具有以下什么特点？
A 支持长文件名
B 支持文件加密管理功能
C 对文件也是以目录形式来组织的
D 全选
7、FAT 记录（ ）而目录项记录着（ ）
A 文件的名字 文件的大小
B 文件的起始簇 文件的最后一个簇（ EOF）
C 文件的最后一个簇（ EOF）文件的起始簇
D 文件的大小 文件的分割
8、 Encase 软件是如何恢复一个删除的文件的
A 在 FAT 表中读取被删除文件的名字并根据其起始簇号和逻辑大小寻找文件
B 在目录项中读取被删除的文件的名字并在未分配的簇中寻找文件的名字
C 从目录项中获得被删文件的起始簇号和大小以获得数据的起始地址和所需簇的数量
D 在 FAT 表中获取被删除文件的起始簇号和大小寻找文件以获得数据的起始地址和所需簇的数量
9、驱动上数据可以被写入的最小区域是（ ），驱动上文件被写入的最小区域是（ ）
A BIT BYTE B 扇区 簇 C 卷 驱动 D 内存 磁盘
10、主引导记录区的分区表为物理驱动器准备了几个逻辑分区（）
A 1 B 2 C 4 D 24
三、名词解释（每小题 4 分，共 20 分）
1、计算机取证
2、文件系统
3、数据恢复
4、电子数据鉴定
5、自由空间、闲散空间
四、简答题（每小题 4 分，共 28 分）
1、列举几例有关计算机的犯罪
2、计算机取证的基本原则
3、FAT 文件系统中第一个扇区是引导（启动）扇区。请对 FAT 引导扇区做一个详细的描述
4、法律执行过程模型的内容
5、列举易失性系统信息有哪些
6、计算机取证的技术有哪六大类？
7、对 EnCase软件的功能做一个简单介绍
三、简答题
1. 在计算机取证的过程中，不管发生了什么紧急情况，调查者都必须遵循的原则是什么？
答：①不要改变原始记录
②不要在作为证据的计算机上执行无关的程序
③不要给犯罪者销毁证据的机会
④详细记录所有的取证活动
⑤妥善保存取得的物证
2. 当 Windows 系统受到入侵攻击，而需要对系统进行取证分析的操作会引起易失性数据。主要的易失性数据包括哪些？
答：①系统日期和时间 ②当前运行的活动进程
③当前的网络连接 ④当前打开的端口

⑤当前打开的套接字上的应用程序　　⑥当前登录用户

3.Windows　系统中初始响应指的是什么？现场数据收集的主要步骤包括哪些？

答：1. 初始响应指的是收集受害者机器上的易失性数据,
并据此进行取证分析的过程

2. 现场数据收集包括一下　3 步：

①打开一个可信的命令解释程序

②数据收集的准备工作

③开始收集易失性数据

4. 描述你知道的证据获取技术包括哪些？

答：① 对计算机系统和文件的安全获取技术；

② 避免对原始介质进行任何破坏和干扰；

③ 对数据和软件的安全搜集技术；

④ 对磁盘或其它存储介质的安全无损伤备份技术；

⑤ 对已删除文件的恢复、重建技术；

⑥ 对磁盘空间、未分配空间和自由空间中包含的信息的发掘技术；

⑦ 对交换文件、缓存文件、临时文件中包含的信息的复原技术；

⑧ 计算机在某一特定时刻活动内存中的数据的搜集技术；

⑨ 网络流动数据的获取技术等

5. 基本过程模型有哪些步骤？

答：①保证安全并进行隔离；

②对现场信息进行记录；

③全面查找证据；

④对证据进行提取和打包；

⑤维护证据监督链

6. 电子证据与传统证据的区别有哪些？

答：①计算机数据无时无刻不在改变；

②计算机数据不是肉眼直接可见的，必须借助适当的工具；

③搜集计算机数据的过程，可能会对原始数据造成很严重的修改,
因为打开文件、打印文件等一般都不是原子操作；

④电子证据问题是由于技术发展引起的,
因为计算机和电信技术的发展非常迅猛,
所以取证步骤和程序也必须不断调整以适应技术的进步。

7. Windows　系统取证方法的主要流程是什么？

答：6 大流程：

①取容易丢失的信息

②冻结硬件

③申请取证

④取证分析

⑤分析报告

⑥文件归档

8. 日志分析有哪些？包括什么内容？

答：①操作系统日志分析；

②防火墙日志分析；

③IDS 软件日志分析；

④应用软件日志分析

9. Windows 2000/XP　安全管理的常用方法有哪些？（至少写出　6 个）

答：①创建 2 个管理员账户
②使用 NTFS分区
③使用安全密码
④设置屏保密码
⑤创建一个陷门帐号
⑥把 administrator 账号改名

四、综合题

1. Windows 系统下取证方法的主要流程是什么？我们文件数据一般的隐藏术有哪些 , 谈谈你的看法？

答：6 大流程：
①取容易丢失的信息
②冻结硬件
③申请取证
④取证分析
⑤分析报告
⑥文件归档

文件数据一般的隐藏术
①操作系统本身自带功能
②利用 FAT簇大小
③利用 slack 簇
④利用更高级的工具

2. 阐述事件响应过程模型执行步骤及其工作内容？

答：①攻击预防阶段 : 事先进行相关培训，并准备好所需的数字取证设备。
②事件侦测阶段 : 识别可疑事件。
③初始响应阶段 : 证实攻击事件已经发生，须尽快收集易丢失的证据
④响应策略匹配 : 依据现有的经验确定响应策略。
⑤备份 : 产生系统备份
⑥调查 : 调查系统以便识别攻击者身份、攻击手段及攻击过程。
⑦安全方案实施 : 对被侦察的系统进行安全隔离。
⑧网络监控 : 监视网络以便识别攻击。
⑨恢复 : 将系统恢复到初始状态，并合理设置安全设施。
⑩报告 : 记录相应的步骤及补救的方法。
11. 补充 : 对响应过程及方法进行回顾审查，并进行适当的调整

3. 简述硬盘的结构与数据组织，写出一般文件的删除与恢复方法？

答：①硬盘的结构主要分为物理结构和逻辑结构,
它的工作原理主要利用电、磁转换实现的,
硬盘的物理结构只要包括：盘片、磁头、盘片主轴、控制电机、
磁头控制器、数据转化器、接口、缓存等几个部分。在逻辑结构中,
因为硬盘有很多的盘片组成，每个盘片被划分为若干个同心圆,
称为磁道，所有的盘片都固定在一个旋转抽上，这个轴即盘片主轴,
硬盘上的数据按照其不同的特点和作用大致可分为 5 部分：
MBR区、 DBR区、 FAT区、 DIR 区和 DATA区。其中， MBR区由分区软件创建,
而 DBR区、 DBR区、 FAT区、 DIR 区和 DATA区由高级格式化程序创建。
②删除方法平时使用的！！
③windows 系统操作中，文件的删除分为逻辑删除和物理删除,
逻辑删除就是以上提到文件删除到回收站,
而物理删除是相当于清完回收站，这时 windows 设法还原,
需要工具，工作原理就是利用硬盘灯数据组织在内存中重建数据。

4. 在 Windows 系统下的文件删除与恢复的操作是什么？
答：和 3 答题②③一致

5. 计算机取证模型有哪些？分别阐述其特点？
答：计算机取证模型包括：
①基本过程模型；
②事件响应模型；
③法律执行过程
④过程抽象模型
⑤多维计算机取证

一、选择题（每小题 2 分，共 20 分）
1、以下有关 EasyRecovery的说法不正确的是（）
A. EasyRecovery在恢复数据时并不向硬盘写任何东西，而是在内存中镜像文件的 FAT 表和目录区。
B. 使用该软件时一定要注意将恢复出来的数据保存在其他的硬盘空间内。
C. 该软件能够对 FAT 和 NTFS 分区中的文件删除、格式化分区进行数据恢复。
D. 它主要是对数据进行硬件恢复。
2、以下不属于在数据恢复中需要使用的软件的是（ ）。
A. PC3000 B. FinalData C. Encase D. FixRAR
3、以下不属于电子证据特点的是（）
A. 电子证据的脆弱性 B. 电子证据的隐蔽性
C. 电子证据的不可挽救性 D.电子证据对系统的依赖性
4、以下不属于计算机取证过程中分析过程的是（）
A. 协议分析 B. 镜像技术 C. 数据挖掘 D. 过程还原
5、以下属于计算机取证技术的发展趋势的是（）
A. 动态取证技术 B. 计算机取证挖掘算法和柔性挖掘技术
C. 取证工具和过程的标准化 D. 以上都是
6、以下关于硬盘的逻辑结构说法不正确的是（）
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痕迹的。
7、以下不属于文件系统的是（）。
A. LINUX B.NTFS C. FAT32 D.EXT2
8、以下不属于数据分析技术的是（）。
A. 对已删除文件的恢复、重建技术 B. 关键字搜索技术
C. 日志分析 D. 特殊类型文件分析
9、以下（）命令可以用来测试本地主机的网络连接是否通畅。
A. traceroute B. ping C. ipconfig D. pslist
10、在大多数黑客案件中， 嗅探工具常被用来捕捉通过网络的流量以重建诸如上网和访问网络文件等功能，以下（）是这类工具。
A. FTK B. sniffer pro C. Quick View Plus D.NTI-DOC
二、填空题（每空 2 分，共 40 分）
1、当执行删除文件操作时， 系统做了两方面的工作： 一是将目录区中该文件的第一个字符改为 “ E6H ”来表示该文件已经被删除；二是将文件所占的文件簇在（ ）中对应表项值全部置“ 0 ”。 文

件分配表
2、计算机对硬盘的读写是以（　）为基本单位的；（）是数据存储和磁盘管理的最基本单位。　　扇区、簇
3、硬盘上的数据按照其不同的特点和作用大致可分为　　5 部分：主引导扇区、操作系统引导扇区、文件分配表、目录区和数据区。其中（）包括硬盘主引导记录　　MBR 和硬盘分区表 DPT；将（）中起始单元的和 FAT 表结合分析可以知道文件在硬盘中的具体位置和大小。　　主引导扇区、目录区
4、操作系统启动分为　5 个阶段：预引导阶段、引导阶段、加载内核阶段、初始化内核阶段和登录。其中（）阶段彩色的　Windows XP 的 logo 以及进度条显示在屏幕中央。　初始化内核阶段
5、Windows 的系统的主要日志有应用程序日志、系统日志和（）。　　安全日志
6、加密算法主要分为对称加密算法和非对称加密算法，其中（）加密算法又称为公钥加密算法，其公钥与私钥是不同的。　非对称
7、（）是一种不可逆的加密算法，它可以说是文件的数字指纹任何文件经过该算法都得到一个　　128 位独一无二的数字，如果该文件被修改过该值也将改变，以此来校验这个文件是否被篡改。　　（）MD5
8、Windows 操作系统下常用的数据包截获技术主要有两种方式：　（ ）和内核层数据包截取技术。　用户层数据包截取技术
9、（）是指“ 通过对行为、安全日志或审计数据或其它网络上可以获得的信息进行操作，检测到对系统的闯入或闯入的企图 ”。　入侵检测
10、没有分配给任何卷的可用磁盘空间称为未分配空间，　　分配给文件的最后一个簇中会有未被当前文件占用的剩余空间，这部分空间一般被称为（）。　　slack 空间
11、在电子证据取证过程中，为了保全证据通常使用数字签名和数字时间戳技术，其中（）用于验证传送对象的完整性以及传送者的身份。　　数字签名
12、Internet Explore 的访问历史记录关联了三种类型的文件夹：　cache、cookies 和 history，其中（）目录主要将访问的网站内容保存在本地，以便用户下一次登录时不必再次下载同样的图形和网页文件。这些目录的共同特点是都具有（）文件，从根本上说针对　　IE 历史记录的分析和取证就是针对该文件。 cache index.dat　14
13、（）是 Windows 系统存储关于计算机配置信息的数据库，是　　Windows 操作系统的核心。（）可以用来显示注册表的逻辑视图。　注册表、注册表编辑器
14、电子邮件是通过　SMTP 和（）协议来进行收发的。　POP3
15、网络证据调查取证要点有时间、（）、日志、准备现场调查工具。　　网络拓扑
16、路由器按功能可以分为（）、企业级路由器和接入级路由器。　　骨干级路由器
17、（）是从大量的、不完全的、有噪声的、模糊的、随机的数据中，提取隐含在其中的、人们事先不知道的、但又是潜在有用的信息和知识的过程。　　数据挖掘
三、判断题（每小题　2 分，共 20 分）
1、对于误删除，错误格式化，硬盘主引导记录、分区表或目录分配表损坏但又没有用其他数据覆盖这些形式的数据，恢复一般都有效。（）对
2、数字引动设备主要包括　PDA、移动硬盘、手机等。（）错
3、数据库系统、网络服务器、防火墙都提供了日志功能。（）对
4、恶意代码是一种程序，它通过把代码在不被察觉的情况下镶嵌到另一段程序中，从而达到破坏被感染电脑数据。计算机病毒、特洛伊木马、计算机蠕虫等都属于恶意代码。（）对
5、证物的完整性验证和和数字时间戳都是通过计算哈希值来实现的。（）对
6、encase不具备关键字查找功能。（）错
7、在进行现场勘查的过程中，如果操作系统正在批量下载信息或杀毒，我们不应该立即终止这些操作。（）错
8、在提取易失性信息的过程中可以使用目标系统上的程序实施提取。（）错
9、计算机证物应存储在正常室温的环境下，避免遭受湿气、磁力、灰尘、烟雾、水及油的影响。（）对
10、在 linux 系统中可以使用　kill 命令杀死某个进程。（）对

四、简答题（每小题　5 分，共 20 分）

1、简述数据恢复的方法。

2、请简单介绍什么是司法鉴定？电子证据鉴定的专门司法机构有哪些？

3、根据电子证据易破坏性的特点，确保电子证据可信、准确、完整并符合相关的法律法规，国际计算机证据组织就计算机取证提出了哪些原则？

4、请简述计算机取证的流程。

一：填空题

1：计算机取证模型包括：基本过程模型；事件响应模型；执法过程模型；过程抽象模型

2：在证据收集过程中必须收集的易失证据主要有：系统日期和时间；当前运行的活动目录；当前的网络连接；当前打开的端口；当前打开的套接字上的应用程序；当前登录用户

3：目前的计算机翻反取证技术主要有：删除技术；隐藏技术

4：在 windows 工作模式下显示系统的基本信息包括：用户；网络环境；系统进程；系统硬件环境

5：隐藏术通常通过两种方法对数据进行保护：使数据不可见，隐藏起所有属性；对数据加密

6：在 MACtimes中的 Mtime 指文件的最后修改事件；　Atimes 指：文件最后访问时间按；　Ctimes 指：文件的最后创建时间

7：防止密码被破译的措施：强壮的加密算法；动态的会话密钥；良好的密码使用管理制度

8：目前主要的数据分析技术包括：文件属性分析技术；文件数字摘要分析技术；日志分析技术；数据分析技术

9 ：安全管理主要包括三个方面：技术安全管理；法律法规安全管理；网络安全管理

10：计算机信息系统安全管理的三个原则：多人负责原则；任期有限原则；职责分离原则

11：信息系统安全包括：身份认证；访问控制；数据保密；数据完整性；不可否认性

12：任何材料要成为证据，均需具备三性：客观相；关联性；合法性

13：计算机取证是指对能够为法庭接受的，　足够可靠和有说服性的存在于计算机和相关外设中的电子证据的确认；保护；提取和归档的过程

14：DES是对称密钥加密算法，　DES算法大致可以分为四个部分：初始置换；迭代过程；子密钥生成；逆置换

15：目前反取证技术分为：擦出技术；隐藏技术；加密技术

16：网络安全管理的隐患有：安全机制；安全工具；安全漏洞和系统后门

二．判断

1. 取证的目的是为了据此找出入侵者（或入侵的机器），并解释入侵的过程。（　　F　　）

2. 网络入侵取证系统中，日志文件是可以很轻易被人修改的，　但是这种修改是很容易被发现的。（ F　）

3. 硬盘由很多盘片组成，每个盘片被划分为若干个同心圆，称为磁道。（　　T　　）

4. 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。（　　T　　）

5. 初始响应在数据收集过程中，能将收集到的证据写回到被入侵机器的硬盘上。（　　T　　）

6. 数据遭受物理损坏后，失效的数据彻底无法使用。（　　F　　）

7. 数据备份是指将计算机硬盘上的原始数据复制到可移动媒体上，如磁带，光盘等。　（　T　　）

8. 计算机反取证就是删除或者隐藏入侵证据使取证工作失效。（　　T　　）

9. 用数字加密技术对数据进行保护主要有两种方式：保密和证明数据的完整性。（　　F　　）

10.Windows 文件删除分为逻辑删除和物理删除两种。（　T　　）

11. 防火墙本身具有较强的抗攻击能力，它是提供信息安全服务，实现网络和信息安全的基础设施。（　T　　）

12. 安全机制分为两类，一类是与安全服务有关；另一类与管理功能有关。（　　T　　）

13. 数据流加密是指把数据划分为定长的数据块，　再分别加密。数据块加密是指加密后的密文前部分，

用来参与报文后面部分的加密。　　（　F　　）
14. 让一台计算机能辨别某个特定的文件系统的过程称为装载文件系统。（　　T　　）